**Europa-Parlamentet**
2019-2024

*Mødedokument*

**A9-0341/2021**

7.12.2021

# ***I
# BETÆNKNING

om 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Økonomi- og Valutaudvalget

Ordfører: Billy Kelleher

## *Tegnforklaring*

| | |
|---|---|
| * | Høringsprocedure |
| *** | Godkendelsesprocedure |
| ***I | Almindelig lovgivningsprocedure (førstebehandling) |
| ***II | Almindelig lovgivningsprocedure (andenbehandling) |
| ***III | Almindelig lovgivningsprocedure (tredjebehandling) |

(Proceduren afhænger af, hvilket retsgrundlag der er valgt i udkastet til retsakt)

## *Ændringsforslag til et udkast til retsakt*

**Ændringsforslag fra Europa-Parlamentet opstillet i to kolonner**

Tekst, der udgår, er markeret med ***fede typer og kursiv*** i venstre kolonne.
Tekst, der udskiftes, er markeret med ***fede typer og kursiv*** i begge kolonner.
Ny tekst er markeret med ***fede typer og kursiv*** i højre kolonne.

Den første og den anden linje i informationsblokken til hvert ændringsforslag angiver den relevante passage i det pågældende udkast til retsakt. Hvis et ændringsforslag angår en eksisterende retsakt, som udkastet til retsakt har til formål at ændre, indeholder informationsblokken tillige en tredje og en fjerde linje, hvori det er anført, hvilken eksisterende retsakt og hvilken bestemmelse heri der er berørt.

**Ændringsforslag fra Europa-Parlamentet i form af en konsolideret tekst**

Ny tekst er markeret med ***fede typer og kursiv***. Tekst, som er bortfaldet, markeres med symbolet ▌ eller med overstregning. Ved udskiftninger markeres den nye tekst med ***fede typer og kursiv***, og den udskiftede tekst slettes eller overstreges.
Som en undtagelse bliver rent tekniske justeringer, der er foretaget af de berørte tjenestegrene med henblik på udarbejdelsen af den endelige tekst, ikke markeret.

**INDHOLD**

**Side**

FORSLAG TIL EUROPA-PARLAMENTETS LOVGIVNINGSMÆSSIGE BESLUTNING 5

PROCEDURE I KORRESPONDERENDE UDVALG .....98

ENDELIG AFSTEMNING VED NAVNEOPRÅB I KORRESPONDERENDE UDVALG .....100

DA

## FORSLAG TIL EUROPA-PARLAMENTETS LOVGIVNINGSMÆSSIGE BESLUTNING

**om 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 (COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))**

**(Almindelig lovgivningsprocedure: førstebehandling)**

*Europa-Parlamentet*,

– der henviser til Kommissionens forslag til Europa-Parlamentet og Rådet (COM(2020)0595),

– der henviser til artikel 294, stk. 2, og artikel 114 i traktaten om Den Europæiske Unions funktionsmåde, på grundlag af hvilke Kommissionen har forelagt forslaget for Europa-Parlamentet (C9-0304/2020),

– der henviser til artikel 294, stk. 3, i traktaten om Den Europæiske Unions funktionsmåde,

– der henviser til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg af 24. februar 2021[1],

– der henviser til forretningsordenens artikel 59,

– der henviser til betænkning fra Økonomi- og Valutaudvalget (A9-0341/2021),

1. vedtager nedenstående holdning ved førstebehandling;

2. anmoder om fornyet forelæggelse, hvis Kommissionen agter at ændre sit forslag i væsentlig grad eller erstatte det med en anden tekst;

2. pålægger sin formand at sende Parlamentets holdning til Rådet og Kommissionen samt til de nationale parlamenter.

[1] EUT C 155 af 30.4.2021, s. 38.

**Ændringsforslag 1**

EUROPA-PARLAMENTETS ÆNDRINGSFORSLAG*

til Kommissionens forslag

---

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[2],

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[3],

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 ▌digital modstandsdygtighed ***mangler stadig at blive*** indbygget i deres

---

*Ændringsforslag: Ny eller ændret tekst er markeret med fede typer og kursiv; udgået tekst er markeret med symbolet ▌.

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

3 EUT C 155 af 30.4.2021, s. 38.

operationelle rammer ***i tilstrækkeligt omfang***.

(2) Brugen af IKT har i de seneste årtier 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 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, ▌skadesbehandling og back office-funktioner. ***Forsikringsbranchen er også blevet forvandlet af brugen af IKT, fra fremkomsten af digitale forsikringsformidlere, der anvender InsurTech, til digital tegning af forsikring og distribution af kontrakter.*** Finans er ikke alene blevet stort set digital i hele sektoren, men digitaliseringen 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[4], 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[5] til hele det finansielle system, uhindret af geografiske grænser. Alvorlige brud på IKT-sikkerheden i den finansielle sektor rammer ikke kun de 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 af EU's finansielle system, idet de skaber likviditetsudstrømning og et generelt tab af tilliden 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. ***Det er derfor nødvendigt at overveje IKT-risikoen i forbindelse med et stærkt forbundet globalt finansielt system, hvor sammenhængen i den internationale regulering og internationalt samarbejde mellem kompetente myndigheder på verdensplan skal prioriteres.***

(5) Til trods for målrettede politiske og lovgivningsmæssige initiativer på nationalt plan og

---

[4] 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.

[5] Ifølge den konsekvensanalyse, der ledsager gennemgangen 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 centrale modparter, børser, systematiske internalisatorer, transaktionsregistre og multilateral handelsfaciliteter) 45 kreditvurderingsbureauer og 2 500 betalingsinstitutter og e-pengeinstitutter med tilladelse. Det giver i alt ca. 21 233 enheder og omfatter ikke crowdfundingenheder, revisorer og revisionsfirmaer, udbydere af kryptoaktivtjenester og benchmarkadministratorer.

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.

(6) I Kommissionens fintechhandlingsplan fra 2018[6] 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 sikkerhedsbrud 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 af 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 til at ***håndtere IKT-risici i den finansielle sektor, beskytte det indre markeds integritet og effektivitet og fremme dets korrekte funktionsmåde styrkes***.

(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

[6] 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/2018/0109, https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A52018DC0109.

forskelle, der skyldes en påtænkt udvikling på nationalt plan, udløse yderligere hindringer for et velfungerende indre marked til skade for markedsdeltagerne 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, 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 som 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.

***(10a) Etablering og opretholdelse af tilstrækkelige netværks- og informationsinfrastruktursystemer er også en væsentlig forudsætning for en effektiv praksis for indsamling af risikodata og risikoindberetning, hvilket igen er en væsentlig forudsætning for kreditinstitutternes solide og bæredygtige risikoforvaltnings- og beslutningsprocesser. Baselkomitéen for Banktilsyn (BCBS) offentliggjorde i 2013 et sæt principper for effektiv indsamling af risikodata og risikoindberetning (BCBS 239) baseret på to overordnede principper for styring og IT-infrastruktur, som skal gennemføres inden starten af 2016. Ifølge rapporten fra Den Europæiske Centralbank (ECB) fra maj 2018 om den tematiske gennemgang om effektiv indsamling af risikodata og risikoindberetning og BCBS's statusrapport fra april 2020 var fremskridtene med gennemførelsen i banker af systemisk betydning på globalt plan utilfredsstillende og en kilde til bekymring. Med henblik på at fremme overholdelsen af og tilpasningen til internationale standarder bør Kommissionen i tæt samarbejde med ECB og efter høring af EBA og ESRB udarbejde en rapport for at vurdere samspillet mellem BCBS 239-principperne og bestemmelserne i denne forordning og, om nødvendigt, hvordan disse principper kan indarbejdes i EU-retten.***

(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 på fyldestgørende vis tackle alle de komponenter, der indgår i operationel modstandsdygtighed. 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. ***Dette initiativ har også til formål at øge bevidstheden om IKT-risici og anerkender, at IKT-hændelser og manglende operationel modstandsdygtighed kan true finansielle enheders finansielle soliditet.***

(13) Finansielle enheder bør følge den samme tilgang og de samme principbaserede regler, når de imødegår IKT-risici***, i overensstemmelse med deres størrelse, art, kompleksitet og risikoprofil***. Konsekvens bidrager til at øge tilliden til det finansielle system og bevare dets stabilitet, navnlig i tider med ***udbredt anvendelse*** 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.

***(14a) Gennemførelsen af denne forordning bør imidlertid ikke forhindre innovation med hensyn til, hvordan finansielle enheder håndterer problemer med digital operationel modstandsdygtighed under overholdelse af dens bestemmelser, eller med hensyn til de tjenester, de tilbyder, eller de tjenester, der tilbydes af eksterne udbydere af IKT-tjenester.***

(15) Foruden lovgivningen om finansielle tjenesteydelser, udgør Europa-Parlamentets og

Rådets direktiv (EU) 2016/1148[7] den nuværende overordnede ramme for cybersikkerhed på EU-plan. Blandt de syv kritiske sektorer, finder nævnte direktiv også anvendelse på tre typer af finansielle enheder, nemlig kreditinstitutter, markedspladser og centrale modparter. Eftersom 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-sikkerhed 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 ***for finansielle enheder*** en lex specialis 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 ***for at*** 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. ***Det fælles tilsynsorgan, de ledende tilsynsførende og*** de kompetente 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.

***Denne forordning bør desuden sikre, at det i direktiv (EU) 2016/1148 oprettede CSIRT-netværk får tilsendt detaljerne om større IKT-relaterede hændelser.***

(18) Dette er også vigtigt for at sikre overensstemmelse med både direktivet om europæisk kritisk infrastruktur, som i øjeblikket revideres for at styrke beskyttelsen af og modstandsdygtigheden i kritiske infrastrukturer mod ikke-cyberrelaterede trusler, ***og direktivet om kritiske enheders modstandsdygtighed***[8], med mulige konsekvenser for den finansielle sektor.

(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

---

[7] 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).

[8] 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).

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***, og både de indholdsmæssige og proceduremæssige krav, der gælder for de kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordning, bør være sammenhængende og i overensstemmelse med de krav, der gælder i henhold til direktivet***. 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 omfattende 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 ***og koncerninterne IKT-risici***. Standarden for digital operationel modstandsdygtighed i det finansielle system bør højnes, samtidig med at der skabes mulighed for en forholdsmæssigt afpasset anvendelse af krav ***under hensyntagen til deres art, omfang, kompleksitet og overordnede risikoprofil***.

(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)[9] 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 imødegåelsen af IKT-risici i tilfælde af storstilede angreb med potentielle systemiske konsekvenser til følge.

***(21a) For at mindske den administrative byrde og undgå kompleksitet og overlappende indberetningskrav for betalingstjenesteudbydere, der er omfattet af denne forordning, bør kravene om indberetning af hændelser i direktiv (EU) 2015/2366 ikke længere finde anvendelse. Kreditinstitutter, e-pengeinstitutter og betalingsinstitutter bør således i henhold til denne forordning indberette alle operationelle eller sikkerhedsmæssige betalingsrelaterede og ikkebetalingsrelaterede hændelser, der tidligere blev indberettet i henhold til direktiv (EU) 2015/2366, uanset om hændelserne er IKT-relaterede eller ej.***

(22) For at sætte kompetente myndigheder i stand til opfylde deres tilsynsmæssige roller ved at opnå et fuldstændigt overblik over IKT-relaterede hændelsers karakter, hyppighed, betydning og virkninger og for at styrke informationsudvekslingen mellem relevante

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

offentlige myndigheder, herunder retshåndhævende myndigheder og afviklingsmyndigheder, er det nødvendigt at fastlægge regler for at ***opnå en robust ordning*** for indberetning af IKT-hændelser med ▌krav, der ***afhjælper manglerne i den sektorspecifikke*** lovgivning om finansielle ***tjenesteydelser*** og fjerner 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 ▌til deres kompetente myndigheder ***gennem en enkelt strømlinet ramme som omhandlet i denne forordning***. 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 ***sommetider*** ukoordinerede nationale rammer, som på forskellig vis omhandler de samme spørgsmål. Dette fører til duplikation af omkostninger for grænseoverskridende finansielle enheder og ***kan hindre*** 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 indføre 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 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 denne type kontrakter indeholder desuden ikke tilstrækkelige garantier, som muliggør en fuldgyldig overvågning af underentrepriseforhold, og berøver dermed den finansielle enhed muligheden 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 af EU-retsakterne om finansielle tjenesteydelser er overvågningen af den kontraktlige dimension ikke fuldt ud forankret i EU-retten. 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[10], tages der i EU-retten 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 af afhængigheden af IKT-tredjeparter og foretage en tilstrækkelig overvågning af risici, der opstår som følge af koncentration 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 ***leverer*** kritiske ***tjenester*** til finansielle enheder. ***Eftersom koncernintern levering af IKT-tjenester ikke indebærer de samme risici, bør udbydere af IKT-tjenester, der er en del af den samme koncern eller institutsikringsordning, ikke defineres som kritiske tredjepartsudbydere af IKT-tjenester.***

(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 mellem 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-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

[10] 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).

databeskyttelsesregler, antitrustregler og regler om ansvar. ***Det er derfor vigtigt at styrke samarbejdsordninger og indberetningen mellem finansielle enheder og de kompetente myndigheder samt informationsudvekslingen med offentligheden med henblik på at udvikle en åben ramme for udveksling af efterretninger og en "security by design"-tilgang, hvilket er afgørende for at øge den finansielle sektors operationelle modstandsdygtighed og beredskab med hensyn til IKT-trusler. Informationsudvekslingsordninger bør altid tage behørigt hensyn til potentielle risici i forbindelse med cybersikkerhed, databeskyttelse eller kommerciel fortrolighed.***

(31) Dertil kommer, at tvivl med hensyn til typen af 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 ikke findes nogen konsekvente ordninger for informationsudveksling på EU-plan, som er skræddersyet til behovene i en integreret finansiel sektor. ***Det er derfor vigtigt at styrke disse kommunikationskanaler og få input fra ikke-tilsynsmyndigheder, når det er nødvendigt og relevant, i hele tilsynscyklussen.***

(32) Finansielle enheder bør ***også*** 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[11] samt på en måde, der garanterer fuld overholdelse af EU's databeskyttelsesregler, primært Europa-Parlamentets og Rådets forordning (EU) 2016/679[12], 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***, herunder kravene i rammen for IKT-risikostyring,*** tages hensyn til væsentlige forskelle mellem finansielle enheder med hensyn til størrelse***, art, kompleksitet og risikoprofil***. 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***, art, kompleksitet***, forretningsprofil ***og relative risikoprofil***, mens de kompetente myndigheder fortsat bør vurdere og se nærmere på tilgangen til en sådan afvejning.

---

11 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).

12 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).

(34) Da større finansielle enheder kan have adgang til flere ressourcer og hurtigt kan afsætte midler til at udvikle styringsstrukturer 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 styringsordninger. Sådanne enheder er bedre rustet til at indføre særlige 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 utidssvarende 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 ***anslåede*** omkostninger og tab, der er forårsaget af ***væsentlige*** IKT-forstyrrelser***, større IKT-relaterede hændelser,*** og resultaterne af gennemgange efter hændelser med ***sådanne*** 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 omfattende tilgang, der skal udmøntes yderligere i ledelsesorganets vedvarende 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[13] fremmer denne forordning et sæt funktioner, der gør det lettere foretage en

[13] 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;

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 de 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***, idet der tages hensyn til, hvorvidt funktionen er en kritisk eller vigtig funktion***. 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) Skønt 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. Selv om 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 opfange større IKT-relaterede hændelser. Direkte indberetning vil give finansielle tilsynsmyndigheder adgang til oplysninger om IKT-

---

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

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 de 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) Der bør forudses yderligere overvejelser vedrørende en mulig centralisering af indberetninger af IKT-relaterede hændelser ved hjælp af et fælles ▌EU-knudepunkt ***for indberetning af større IKT-relaterede hændelser***, 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 robust digital operationel modstandsdygtighed og i overensstemmelse med international standarder (f.eks. "G7 Fundamental Elements for Threat-Led Penetration Testing") bør finansielle enheder***, bortset fra mikrovirksomheder,*** 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 afprøvningen 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). Afprøvningen 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 af avancerede afprøvningskrav (f.eks. TLPT) i deres hjemland, og en sådan afprøvning 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. ***For at styrke samarbejdet med pålidelige tredjelande om finansielle enheders modstandsdygtighed bør Kommissionen og de kompetente myndigheder endvidere søge at fastlægge en ramme for gensidig anerkendelse af resultaterne af TLPT.***

***Medlemsstaterne bør udpege én enkelt offentlig myndighed, der skal være ansvarlig***

***for TLPT i den finansielle sektor på nationalt plan. Denne offentlige myndighed kan bl.a. være en national kompetent myndighed eller en offentlig myndighed, der er udpeget i overensstemmelse med artikel 8 i direktiv (EU) 2016/1148 (NIS). Denne offentlige myndighed bør være ansvarlig for at udstede attester for, at TLPT er blevet udført i overensstemmelse med kravene. Sådanne attester bør lette de kompetente myndigheders gensidige anerkendelse af afprøvning.***

***Nogle finansielle enheder har kapacitet til at udføre intern avanceret afprøvning, mens andre vil indgå kontrakter med eksterne testere fra Unionen eller fra et tredjeland. Det er således vigtigt, at alle testere er underlagt de samme klare krav. For at sikre interne testeres uafhængighed bør brugen af dem være betinget af den kompetente myndigheds godkendelse.***

***Metoden til udførelse af TLPT bør ikke være obligatorisk, men anvendelsen af den eksisterende TIBER-EU-ramme bør anses for at være i overensstemmelse med kravene om TLPT som fastsat i denne forordning.***

***Indtil denne forordning er trådt i kraft, og ESA'erne har udarbejdet og vedtaget de krævede reguleringsmæssige tekniske standarder vedrørende TLPT, bør de finansielle enheder følge de relevante EU-retningslinjer og -rammer, der gælder for efterretningsbaserede penetrationstest, da disse fortsat vil finde anvendelse, når denne forordning er trådt i kraft.***

***(44a) Ansvaret for at udføre TLPT – og for cybersikkerhedsstyring i almindelighed og forebyggelse af cyberangreb – bør forblive fuldt ud hos den finansielle enhed, og attesteringer fra myndighederne bør udelukkende være med henblik på gensidig anerkendelse og bør ikke udelukke nogen opfølgende foranstaltninger vedrørende det IKT-risikoniveau, som den finansielle enhed er udsat for, eller betragtes som en godkendelse af dens kapacitet til IKT-risikostyring og -afbødning.***

(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***, navnlig hvad angår leveringen af kritiske eller vigtige funktioner fra 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 ***arten,*** 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***, samt på om IKT-tjenesterne leveres af en koncernintern udbyder eller en tredjepartsudbyder***.

(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 at anmode om uddrag herfra på ad hoc-basis.

(48) En grundig analyse forud for kontraktindgåelsen bør understøtte og gå forud for den formelle indgåelse af kontraktlige ordninger***, samtidig med at korrigerende og afhjælpende foranstaltninger, som kan omfatte delvis eller fuldstændig*** kontraktopsigelse, som minimum bør ***træffes i tilfælde*** af en række omstændigheder, der påviser ***alvorlige*** 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 ▌. 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. ***Det fælles tilsynsorgan***, der ***udøver*** tilsyn med hver enkelt kritisk tredjepartsudbyder af IKT-tjenester***, og den ESA, der er udpeget til at udøve det daglige tilsyn*** ("ledende tilsynsførende"), bør i forbindelse med varetagelsen af tilsynsopgaver være særligt opmærksom på at få en fuldstændig forståelse af 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 af EU's finansielle system, og bør i stedet tilsikre en dialog med kritiske tredjepartsudbydere af IKT-tjenester, når en sådan risiko identificeres[14].

(50) For regelmæssigt at kunne vurdere og overvåge evnen hos tredjepartsudbydere af IKT-tjenester til at levere tjenester til den finansielle enhed på en sikker måde, 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 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, genfinding og tilbagesendelse i tilfælde af insolvens eller afvikling, i tilfælde af at tredjepartsudbyderen af IKT-tjenester afbryder sine forretningsaktiviteter***, eller at de kontraktlige ordninger opsiges,*** også betragtes

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

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***, som er relevant for de tjenesteydelser, der leveres af tredjepartsudbyderen af IKT-tjenester til finansieringsinstituttet,*** uden yderligere omkostninger eller til en forud fastsat pris. ***Accessoriske IKT-tjenester, som ikke er nødvendige for de finansielle enheders drift, er ikke omfattet af denne forordning.***

***Endvidere bør definitionen af "kritisk eller vigtig funktion" i denne forordning omfatte definitionen af "kritiske funktioner" som fastsat i artikel 2, stk. 1, nr. 35), i Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15.maj 2014***[15]***. I overensstemmelse hermed bør funktioner, der er kritiske funktioner i henhold til direktiv (EU) 2014/59, anses for at være kritiske eller vigtige funktioner i henhold til denne forordning.***

(53) ***I tilfælde af kontraktlige ordninger vedrørende kritiske eller vigtige funktioner er*** adgangsrettigheder samt retten til inspektion og revision, som udøves af den finansielle enhed eller en udpeget tredjepart, ▌ 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 ***fælles tilsynsorgan og den ledende tilsynsførende*** 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***, og bør samtidig udøve forsigtighed med ikke at forstyrre de tjenester, som leveres til andre kunder hos tredjepartsudbyderen af IKT-tjenester***. ***Den finansielle enhed og tredjepartsudbyderen af IKT-tjenester bør have mulighed for at aftale, at adgangs-, inspektions- og revisionsrettighederne kan uddelegeres til en uafhængig tredjepart.***

(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 ***interne*** løsninger, der stemmer overens med den leverede tjenestes kompleksitet. ***Endvidere bør kreditinstitutter sikre, at de relevante IKT-kontrakter er robuste og kan håndhæves fuldt ud i tilfælde af afvikling af kreditinstituttet. I overensstemmelse med afviklingsmyndighedernes forventninger***

---

[15] ***Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber og om ændring af Rådets direktiv 82/891/EØF og Europa-Parlamentets og Rådets direktiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU samt Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).***

***bør kreditinstitutterne sikre, at de relevante kontrakter om IKT-tjenester er modstandsdygtige i tilfælde af afvikling. Så længe kritiske eller vigtige IKT-funktioner fortsat udføres, bør disse finansielle enheder sikre, at kontrakterne bl.a. indeholder klausuler om, at de ikke vil blive ophævet, suspenderet eller ændret som følge af omstrukturering eller afvikling.***

(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 det 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.

***(55a) ESA'erne bør have mandat til at udarbejde gennemførelsesmæssige tekniske og reguleringsmæssige standarder, der præciserer forventningerne til politikkerne for styring af IKT-tredjepartsrisici og til kontraktmæssige krav. Indtil disse standarder træder i kraft, bør finansielle enheder følge relevante retningslinjer og andre foranstaltninger udstedt af ESA'erne og de kompetente myndigheder.***

(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 ***tilsynsrammen***. Kritiske tredjepartsudbydere af IKT-tjenester, som ikke automatisk udpeges ved anvendelsen 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 ***understøtter udførelsen af opgaverne på eurosystemniveau som*** omhandlet i artikel 127, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde, derfor bør fritages. ***Tilsvarende bør virksomheder, som er en del af en finansiel koncern, og som udelukkende leverer IKT-tjenester til finansielle enheder inden for samme finansielle koncern, ikke være underlagt mekanismen til udpegning som kritisk.***

(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. ***Kravet om at have en virksomhed, som f.eks. et datterselskab, etableret i EU under en medlemsstats ret har***

***til formål at skabe et kontaktpunkt mellem tredjepartsudbyderen af IKT-tjenester på den ene side og den ledende tilsynsførende og det fælles tilsynsorgan på den anden side og at sikre, at den ledende tilsynsførende og det fælles tilsynsorgan kan udføre deres opgaver og udøve deres tilsyns- og håndhævelsesbeføjelser i henhold til denne forordning. De tjenesteydelser fra tredjepartsudbyderen af IKT-tjenester, som der er indgået kontrakt om, behøver ikke blive udført af dennes enhed i EU.***

***(58a) På grund af de store konsekvenser, som udpegningen som kritisk kan få for tredjepartsudbydere af IKT-tjenester, bør der fastsættes en ret til forudgående høring i form af en pligt, der pålægges ESA'erne og det fælles tilsynsorgan, til at tage behørigt hensyn til yderligere oplysninger, der fremlægges af tredjepartsudbydere af IKT-tjenester i forbindelse med udpegningsprocessen.***

(59) ***Tilsynsrammen*** bør ikke berøre medlemsstaternes beføjelser til at gennemføre deres egne tilsynsbesøg 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 aktivt at udnytte 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 ***gennem det nyetablerede fælles tilsynsorgan, som*** både ***kommer med*** 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 det fælles tilsynsorgan oprettes til at føre direkte tilsyn med tredjepartsudbydere af IKT-tjenester***. ***Desuden*** bør en af ESA'erne udpeges som ledende tilsynsførende for hver af de kritiske tredjepartsudbydere af IKT-tjenester ***til at udføre og koordinere det daglige tilsyns- og undersøgelsesarbejde, fungere som fælles kontaktpunkt og sikre kontinuitet***. ***Det fælles tilsynsorgan og den ledende tilsynsførende bør arbejde gnidningsløst for at sikre et effektivt dagligt tilsyn såvel som en holistisk tilgang til beslutningstagning og henstillinger.***

(62) Ledende tilsynsførende bør have de nødvendige beføjelser til at foretage undersøgelser, inspektioner på stedet ▌ 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.

***(62a)*** Overdragelse af ***det direkte tilsyn*** til ***det fælles tilsynsorgan*** 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) ***Det fælles tilsynsorgan*** bør ▌ 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 ***det fælles tilsynsorgan*** som led i ***dets*** opgaver vedrørende tilsyn med finansielle enheder. ***Inden sådanne henstillinger færdiggøres, bør kritiske tredjepartsudbydere af IKT-tjenester få mulighed for at fremlægge oplysninger, som de med rimelighed mener, bør tages i betragtning, før henstillingen færdiggøres og fremsættes.***

***(63a) For at undgå overlapning og uoverensstemmelse med de tekniske og organisatoriske foranstaltninger, der gælder for kritiske tredjepartsudbydere af IKT-tjenester, bør de ledende tilsynsførende og det fælles tilsynsorgan tage behørigt hensyn til den ramme, der er fastlagt ved direktiv (EU) 2016/1148, under udøvelsen af deres beføjelser i overensstemmelse med tilsynsrammen i denne forordning. Før udøvelsen af disse beføjelser bør det fælles tilsynsorgan og den ledende tilsynsførende høre de relevante kompetente myndigheder, der har kompetence i henhold til direktiv (EU) 2016/1148.***

(64) Tilsynsrammen må hverken erstatte eller på nogen måde træde i stedet for 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 samarbejdsaftaler 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***, når de foretager overordnede undersøgelser eller inspektioner på stedet,*** 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[16], og høring af ESA'erne gennem gensidig informationsudveksling og levering af bistand i forbindelse med tilsynsaktiviteter. ***Selv om Den Fælles Afviklingsinstans ikke er en kompetent myndighed i henhold til denne forordning, bør den ikke desto mindre inddrages i mekanismerne for gensidig udveksling af oplysninger for enheder, som er omfattet af anvendelsesområdet for Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014[17]***.

(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[18]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(69) Eftersom denne forordning sammen med Europa-Parlamentets og Rådets direktiv (EU) 20xx/xx[19] 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.

---

16 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).

17 ***Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond og om ændring af forordning (EU) nr. 1093/2010 (EUT L 225 af 30.7.2014, s. 1).***

18 EUT L 123 af 12.5.2016, s. 1.

19 [*Indsæt venligst den fulde titel*].

***Relevante retningslinjer udstedt af eller for nuværende under udarbejdelse af ESA'erne om anvendelsen af disse forordninger og direktiver bør gennemgås og revideres som led i konsolideringsprocessen, så retsgrundlaget for kravene til IKT-risici i EU-retten udelukkende stammer fra denne forordning, dens gennemførelsesretsakter og afgørelser og henstillinger udstedt i henhold hertil vedrørende enheder, der er omfattet af anvendelsesområdet.***

***(69a)*** 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. ***Ved udarbejdelsen af udkast til reguleringsmæssige tekniske standarder bør ESA'erne tage behørigt hensyn til deres mandat i forbindelse med proportionalitetsaspekter og rådføre sig med deres respektive rådgivende udvalg om proportionalitet, især i forbindelse med anvendelsen af denne forordning på SMV'er og midcapselskaber.***

(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 ***art***, størrelse, kompleksitet ***og forretningsprofil*** 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

GENERELLE 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

– ***indberetning af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser til de kompetente enheder, der er nævnt i artikel 2, stk. 1, litra a)-c)***

– 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 tilsyn og de kompetente myndigheders håndhævelse 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.

***2a. Denne forordning berører ikke medlemsstaternes beføjelser til opretholdelse af den offentlige sikkerhed, forsvaret og den nationale sikkerhed***

*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 ***og udbydere*** af kryptoaktiver, udstedere ***og udbydere*** af aktivbaserede tokens og udstedere af signifikante aktivbaserede tokens

f) værdipapircentraler ***og operatører af værdipapirafviklingssystemer***

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***, der ikke er mikrovirksomheder, små eller mellemstore virksomheder, medmindre disse mikrovirksomheder, små eller mellemstore virksomheder udelukkende anvender organiserede automatiske salgssystemer***

o) arbejdsmarkedsrelaterede pensionskasser ***(IORP'er), der ikke forvalter pensionsordninger, som tilsammen har færre end 15 medlemmer***

p) kreditvurderingsbureauer

q) revisorer og revisionsfirmaer***, der ikke er mikrovirksomheder eller små eller mellemstore virksomheder, medmindre sådanne mikrovirksomheder eller små og mellemstore virksomheder yder revisionsvirksomhed til virksomheder, der er opført i denne artikel, med undtagelse af mikrovirksomheder, små og mellemstore virksomheder, der ikke arbejder med gevinst for øje, jf. artikel 2, stk. 3, i forordning (EU) nr. 537/2014, medmindre den kompetente myndighed beslutter, at undtagelsen ikke er gyldig***

r) administratorer af kritiske benchmarks

s) udbydere af crowdfundingtjenester

t) securitiseringsregistre

u) tredjepartsudbydere af IKT-tjenester.

***1a. Denne forordning finder, med undtagelse af afdeling II i kapitel V, også anvendelse på koncerninterne IKT-tjenesteudbydere.***

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

***2a. I denne forordning anvendes "tredjepartsudbydere af IKT-tjenester" som fælles betegnelse for tredjepartsudbydere af IKT-tjenester og koncerninterne IKT-tjenesteudbydere, dog med undtagelse af kapitel V, afdeling II.***

*Artikel 3*

Definitioner

I denne forordning forstås ved: "digital operationel modstandsdygtighed":

1) "digital operationel modstandsdygtighed": en finansiel enheds evne til at opbygge, sikre og vurdere sin operationelle integritet ▌, ved enten direkte eller indirekte, gennem anvendelse af tjenester fra tredjepartsudbydere af IKT-tjenester, at sikre ▌ det løbende udbud af tjenesteydelser og kvaliteten heraf ***til trods for de driftsforstyrrelser, der rammer den finansielle enheds IKT-funktioner***

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 hidrørende fra brugen af net- og informationssystemer ▌ som, hvis de forekommer, kan kompromittere sikkerheden i eller ramme net- og informationssystemerne, i eventuelle IKT-afhængige værktøjer eller processer, i den igangværende operation eller behandling eller i forbindelse med udbuddet af tjenester ▌

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

6) "IKT-relateret hændelse": en uforudset identificeret hændelse ***eller en række af forbundne hændelser***, som kompromitterer sikkerheden i net- og informationssystemer ▌, eller som har negative virkninger for tilgængeligheden, fortroligheden, regelmæssigheden, ***integriteten*** eller autenciteten af de finansielle tjenesteydelser, som den finansielle enhed udbyder

***6a) "operationel eller sikkerhedsbetalingsrelateret hændelse": en hændelse eller en række forbundne hændelser, som ikke har været forudset af finansielle enheder som omtalt i artikel 2, stk. 1, litra a)-c), som har eller sandsynligvis får negativ indvirkning på integriteten, tilgængeligheden, fortroligheden, autenticiteten eller kontinuiteten af betalingsrelaterede ydelser***

7) "større IKT-relateret hændelse": en IKT-relateret hændelse***, som har eller sandsynligvis får*** en ▌ stor negativ indvirkning på net- og informationssystemer, som understøtter kritiske funktioner i den finansielle enhed

***7a) "større operationel eller sikkerhedsbetalingsrelateret hændelse": en operationel eller sikkerhedsbetalingsrelateret hændelse, der opfylder de i artikel 16 fastsatte kriterier***

8) "cybertrussel": en cybertrussel som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]

***8a) "væsentlig cybertrussel": en cybertrussel, hvis karakteristika klart indikerer, at den sandsynligvis vil føre til en større IKT-relateret hændelse***

---

[20] 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).

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 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 gennem en ***cybertrussel***

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 IKT-tjenester, herunder ***en finansiel enhed, der leverer IKT-tjenester, som udgør en del af en virksomhed, der leverer et større udvalg af produkter eller tjenesteydelser***, 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[21]

***15a) "koncernintern udbyder af IKT-tjenester": en virksomhed, der indgår i en finansiel koncern og som udelukkende udbyder IKT-tjenester til finansielle virksomheder inden for samme koncern, eller til finansielle enheder, der tilhører samme institutionelle beskyttelsesordning, herunder til deres moderselskaber, datterselskaber og filialer eller andre enheder, der hører under fælles ejerskab eller kontrol***

16) "IKT-tjenester": digitale tjenester og datatjenester, der leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere ***kontinuerligt, med undtagelse af telekommunikationskontrakter***

17) "kritisk eller vigtig funktion": en ***aktivitet eller en tjeneste, som er afgørende for driften af en finansiel enhed, og som hvis den forstyrres i væsentlig grad vil forringe soliditeten eller kontinuiteten af den finansielle enheds tjenester eller aktiviteter***, eller som, hvis dens afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med

[21] 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).

dens tilladelse, eller af dens andre forpligtelser i henhold til gældende lovgivning om finansielle tjenesteydelser, ***herunder "kritiske funktioner" som defineret i artikel 2, stk. 1, nr. 35), i direktiv 2014/59/EU***

18) "kritisk tredjepartsudbyder af IKT-tjenester": en tredjepartsudbyder af IKT-tjenester, der er udpeget i overensstemmelse med artikel ***28*** og omfattet af den i artikel ***29***-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 ▌, og som har indgået kontraktlige ordninger med en finansiel enhed om levering af IKT-tjenester

20) "IKT-underleverandør med hjemsted i et tredjeland": en IKT-underleverandør, som er en juridisk person med hjemsted i et tredjeland, ▌ 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 ***den finansielle stabilitet i Unionen som helhed eller for*** en finansiel enheds evne ▌ til at varetage kritiske eller vigtige 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 forordning (EU) nr. 909/2014, artikel 3, stk. 1, nr. 20, i Europa-Parlamentets og Rådets forordning (EU) 2016/1011[22], artikel 3, stk. 1, nr. ***18***), i Europa-Parlamentets og Rådets forordning (EU) 20xx/xx[23] [MiCA], 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[24]

***23a) "et kreditinstitut, der i henhold til direktiv 2013/36/EU er undtaget fra bestemmelserne": et kreditinstitut, der, jf. artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU nyder fordel af at være undtaget fra bestemmelserne***

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

***24a) "lille og ikkeforbundet investeringsselskab": et investeringsselskab, som opfylder de***

---

22 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).

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

24 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).

***betingelser, der er fastsat i artikel 12, stk. 1, i forordning (EU) 2019/2033***

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

***25a) "betalingsinstitut undtaget ved direktiv (EU) 2015/2366": et betalingsinstitut, der nyder fordel af en undtagelse i henhold til artikel 32, stk. 1, 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[25]

***26a) "e-pengeinstitut undtaget ved direktiv 2009/110/EF": et e-pengeinstitut, der nyder fordel af en undtagelse i henhold til artikel 9 i direktiv 2009/110/EF***

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

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,

---

[25] 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).

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, ***nr. 8)***, i forordning (EU) 202x/xx [Publikationskontor: Indsæt venligst henvisning til MiCA-forordningen]

44) "tilbudsgiver med hensyn til køb af kryptoaktiver": tilbudsgiver med hensyn til køb af kryptoaktiver som fastlagt i [artikel 3, stk. 1, ***nr. 6)***, i [EUT: Indsæt venligst henvisning til MiCA-forordningen]

***44a) "tilbudsgiver" tilbudsgiver som fastlagt i [artikel 3, stk. 1, nr. XX] i [EUT: Indsæt venligst henvisning til MiCA-forordningen]***

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

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

***45a) "tilbudsgiver med hensyn til køb af aktivbaserede tokens": en tilbudsgiver med hensyn til køb af aktivbaserede betalingstokens som fastlagt i artikel 3, stk. 1, nr. [(XX)], i [EUT: Indsæt venligst henvisning til MiCA-forordningen]***

46) "tilbudsgiver med hensyn til køb af signifikante aktivbaserede tokens": en tilbudsgiver med hensyn til køb af signifikante aktivbaserede betalingstokens som fastlagt i artikel 3, stk. 1, ***nr. (XX)***, i [EUT: Indsæt venligst henvisning til MiCA-forordningen]

47) "administrator af kritiske benchmarks" en administrator af kritiske benchmarks som defineret i artikel ***3***, ***nr. 25***), i forordning ***2016/1011*** [EUT: Indsæt venligst henvisning til MiCA-forordningen]

48) "udbyder af crowdfundingtjenester": en udbyder af crowdfundingtjenester som defineret i artikel ***2, stk. 1, litra e)***, i forordning (EU) ***2020/1503*** [Publikationskontor: Indsæt venligst henvisning til crowfundingforordningen]

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

50) "mikrovirksomhed***, lille eller mellemstor virksomhed***": en finansiel enhed som defineret i artikel 2, i bilaget til henstilling 2003/361/EF

***50a) "afviklingsmyndighed": en myndighed, som er udpeget af en medlemsstat i henhold til artikel 3 i direktiv 2014/59/EU eller Den Fælles Afviklingsinstans etableret i henhold til artikel 42 i forordning (EU) nr. 806/2014.***

***Artikel 3a***

***Proportionalitetsprincippet***

*1. Finansielle enheder indfører reglerne i kapitel II, III og IV i overensstemmelse med proportionalitetsprincippet under hensyntagen til størrelsen af deres foretagende samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og transaktioner, og deres overordnede risikoprofil.*

*2. I henhold til proportionalitetsprincippet finder artikel 4-14 i denne forordning ikke anvendelse på:*

*a) små og ikke indbyrdes forbundne investeringsselskaber eller betalingsinstitutter, der er undtaget ved direktiv (EU) 2015/2366*

*b) kreditinstitutter, der er undtaget ved direktiv 2013/36/EU*

*c) udstedere af elektroniske penge, der er undtaget ved direktiv 2009/110/EF og*

*d) små arbejdsmarkedsrelaterede pensionskasser*

*3. På grundlag af den årlige rapport om gennemgangen af IKT-risikostyringsrammen, jf. artikel 5, stk. 6, og artikel 14a, stk. 2, gennemgår og evaluerer de relevante kompetente myndigheder en finansiel enheds anvendelse af proportionaliteten og afgør, om den finansielle enheds IKT-risikostyringsramme sikrer forsvarlig styring og digital operationel modstandsdygtighed og dækning af IKT-risici. De kompetente myndigheder tager i denne forbindelse hensyn til finansielle enheders størrelse, karakteren, omfanget og kompleksiteten af deres tjenesteydelser, aktiviteter og transaktioner og deres overordnede risikoprofil.*

*4. Hvis den relevante kompetente myndighed anser den finansielle enheds IKT-risikostyringsramme for at være utilstrækkelig og uforholdsmæssig, indleder den en dialog med den finansielle enhed for at afhjælpe manglerne og sikre fuld overholdelse af kapitel II.*

*5. ESA'erne udarbejder udkast til reguleringsmæssige tekniske standarder med hensyn til følgende:*

*a) fastlæggelse af, i hvilket omfang IKT-risikostyringsforpligtelser finder anvendelse på hver af de finansielle enheder, der er nævnt i stk. 1*

*b) yderligere præcisering af indholdet og formatet af den årlige rapport om gennemgangen af IKT-risikostyringsrammen, jf. stk. 3*

*c) nærmere fastlæggelse af de regler og procedurer, som de kompetente myndigheder og de finansielle enheder skal følge i den dialog, der er omhandlet i stk. 4.*

*6. ESA'erne forelægger Kommissionen udkastet til reguleringsmæssige tekniske standarder, der er omhandlet i stk. 5, senest den [Publikationskontoret: Indsæt datoen 1 år efter ikrafttrædelsesdatoen].*

*Kommissionen tillægges beføjelse til at vedtage de i denne artikels stk. 5 omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.*

KAPITEL II

IKT-RISIKOSTYRING

AFDELING I

*Artikel 4*

*Styring og organisation*

1. Finansielle enheder skal have indført en intern styringsramme og en kontrolramme, der sikrer en effektiv og forsigtig styring af alle IKT-risici, ***med henblik på at opnå en høj grad af digital operationel modstandsdygtighed.***

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

   ***aa) etablerer procedurer og politikker med henblik på at sikre opretholdelse af høje standarder for sikkerhed, fortrolighed og dataintegritet***

   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 IKT-forretningskontinuitetspolitik og IKT-katastrofeberedskabsplan, ***der kan vedtages som en særlig særskilt politik og som en integreret del af den finansielle enheds overordnede forretningskontinuitetspolitik og 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 ***relevante*** kurser i IKT-risici og -færdigheder for alt ▌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) underrettes behørigt 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) ▌ underrettes ***regelmæssigt*** om ***som minimum større*** 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 enhedens ordninger ***inden for den finansielle enhed*** vedrørende brugen af IKT-tjenester, ***navnlig dem, der er indgået aftale om med tredjepartsudbydere af IKT-tjenester***, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

4. Medlemmerne af ***den finansielle enheds*** ledelsesorgan skal ***aktivt*** holde den viden og de færdigheder, der er nødvendige for at forstå og vurdere IKT-risici og deres indvirkning på den finansielle enheds drift, ajour, ***herunder ved regelmæssigt at følge specifik uddannelse, som svarer til de IKT-risici, der styres***.

## 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 ▌.

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 ***og om deres ramme for IKT-styring, som krævet*** af de kompetente myndigheder.

4. Som led i den stk. 1 omhandlede ramme for IKT-risikostyring indfører 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, ***hvis sådanne allerede findes, og hvor det er hensigtsmæssigt, herunder vejledninger, der er udarbejdet i relevante retningslinjer af ESA'erne***, og reviderer det regelmæssigt.

5. Finansielle enheder, som ikke er mikrovirksomheder, ***overdrager ansvaret for styring af og tilsyn med IKT-relaterede risici til en kontrolfunktion og sikrer, at denne***

***kontrolfunktion er uafhængig med henblik på at undgå interessekonflikter. Finansielle enheder sikrer*** en passende ***uafhængighed af*** IKT-styringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

6. Den i 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.

***Der skal hvert år forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed.***

7. ***For så vidt angår enheder, der ikke er mikrovirksomheder***, gennemgås den stk. 1 omhandlede ramme for IKT-risikostyring regelmæssigt af IKT-revisorer, der besidder tilstrækkelig viden, faglig kompetence og ekspertise med hensyn til IKT-risici. IKT-revisionernes 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. ▌

9. Den i stk. 1 omhandlede ramme for IKT-risikostyring skal omfatte en strategi for digital ***operationel*** 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-arkitekturen*** 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 effektiviteten af forebyggende foranstaltninger

   g) ***identificere*** den centrale afhængighed af IKT-tredjepartstjenesteudbydere og ***præcisere exitstrategier i forbindelse med sådanne vigtige afhængighedsforhold***

h) gennemføre afprøvning af digital operationel modstandsdygtighed ***i overensstemmelse med kapitel IV i denne forordning***

i) fastlægge en kommunikationsstrategi, der anvendes i tilfælde af IKT-relaterede hændelser, ***og som skal offentliggøres i henhold til artikel 13.***

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

***Efter underretning af de kompetente myndigheder kan finansielle enheder uddelegere opgaven med at efterprøve overholdelsen af kravene til IKT-risikostyring til koncerninterne virksomheder.***

***Hvis uddelegeringen, der er omhandlet i andet afsnit, tages i anvendelse, er den finansielle enhed stadig fuldt ansvarlig for at efterprøve, at kravene til IKT-risikostyring bliver overholdt.***

*Artikel 6*

*IKT-systemer, -protokoller og-værktøjer*

1. ***For at håndtere og styre IKT-risici,*** anvender og vedligeholder ***de finansielle enheder*** opdaterede IKT-systemer, -protokoller og -værktøjer, som opfylder følgende betingelser:

a) systemerne og værktøjerne er velegnede i forhold til ▌ 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 ***kritiske eller vigtige*** 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 ***de IKT-relaterede forretningsfunktioners kritiske eller vigtige betydning, samt*** 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 ***kritiske eller vigtige*** 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, ***hvor det er relevant***, 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 ***de kritiske eller vigtige*** IKT-aktivers konfiguration, ***under hensyntagen til deres formål***, samt forbindelserne og den indbyrdes forbundethed mellem disse forskellige IKT-aktiver.

5. De finansielle enheder identificerer og dokumenterer alle ***kritiske eller vigtige*** processer, der er afhængige af tredjepartsudbydere af IKT-tjenester, og identificerer sammenkoblinger med tredjepartsudbydere af IKT-tjenester, ***der understøtter kritiske eller vigtige funktioner***.

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 utidssvarende IKT-systemer, herunder systemer, der stadig er i brug og som opfylder deres funktion, men som er:

   ***a) gamle eller ved slutningen af deres levetid, hvis der er tale om hardware***

   ***b) ikke længere er i stand til at modtage støtte eller vedligeholdelse fra deres leverandør og***

   ***c) umulige eller uøkonomiske at opdatere. Der skal foretages årlige IKT-risikovurderinger af nedarvede IKT-systemer***, navnlig før og efter sammenkædning af ▌ 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 modstandsdygtigheden, stabiliteten og tilgængeligheden af IKT-systemer, ***som understøtter kritiske eller vigtige funktioner***, 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 IKT-teknologi og ▌IKT-processer, som

   a) ***maksimerer*** 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 ***interne IKT-risici, herunder*** dårlig administration, procesrelaterede risici ***og menneskelige fejl***.

4. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, skal de finansielle enheder ***i overensstemmelse med deres risikoprofil***:

   a) udvikle og dokumentere en informationssikkerhedspolitik, der fastlægger regler for beskyttelse af fortroligheden, integriteten og tilgængeligheden af deres ***IKT-ressourcer, data og informationsaktiver og samtidig sikre fuld beskyttelse af*** deres kunders IKT-ressourcer, data og informationsaktiver***, når de omfatter dele af finansielle enheders IKT-systemer***

   b) følge en risikobaseret tilgang, indføre en forsvarlig forvaltning af netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, ***der kan omfatte at*** gennemføre ▌mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb

   c) gennemføre politikker***, procedurer og kontrolforanstaltninger***, 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 ▌

   d) gennemføre politikker og protokoller for stærke autentificeringsmekanismer ***og beskyttelse af krypteringsnøgler*** på grundlag af relevante standarder og særlige kontrolsystemer ▌

   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 ***hurtigst muligt***, 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, ***hvor det er teknologisk muligt,*** og til identifikation ***og overvågning*** af potentielt væsentlige lokale fejl (single points of failure).

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

2. ***De*** i stk. 1 omhandlede detektionsmekanismer skal ▌udløse detektion af IKT-relaterede hændelser og indsatsforanstaltninger mod IKT-relaterede hændelser, ***herunder*** automatiske varlingsmekanismer for det relevante personale, som har ansvar for indsatsen mod IKT-relaterede hændelser.

3. ▌Finansielle enheder ***afsætter*** tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af IKT-anomalier og IKT-relaterede hændelser, navnlig cyberangreb.

***3a. Finansielle enheder indberetter alle IKT-relaterede hændelser, som har en indvirkning på de finansielle tjenesteydelsers stabilitet, kontinuitet eller kvalitet, herunder om hændelsen har en indvirkning på tjenesterne eller sandsynligvis vil have en indvirkning på disse tjenester.***

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 ▌udførlig politik for IKT-driftsstabilitet, ***som kan blive taget i brug som en særskilt politik*** og som en integreret del af den finansielle enheds ***bredere og overordnede*** politik for operationel driftsstabilitet.

   ***IKT-forretningskontinuitetspolitikken skal sigte mod at styre og afbøde risici, der kan have en skadelig indvirkning på finansielle enheders IKT-systemer og IKT-tjenester, og på at fremme en hurtig genopretning af dem, hvis det er nødvendigt. Ved udarbejdelsen af IKT-forretningskontinuitetspolitikken har de finansielle enheder særligt fokus på risici, der kan have en skadelig virkning på IKT-tjenester og IKT-***

***systemer.***

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:

   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 alt 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 ***kritiske eller vigtige IKT-systemer***

   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, skal have en krisestyringsfunktion***, enten som en særlig funktion eller som en del af funktionerne***

***med ansvar for reaktion på og håndtering af hændelser***. ***Krisestyringsfunktionen skal,*** hvis deres politik for IKT-driftsstabilitet eller deres IKT-katastrofeberedskabsplan aktiveres, ▌ indeholde klare procedurer for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 13.

7. De finansielle enheder fører registre over ***relevante*** aktiviteter før og under driftsforstyrrelser, når deres IKT-driftsstabilitet eller 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 ***anslåede finansielle*** omkostninger og tab, der opstår som følge af ***væsentlige*** IKT-relaterede forstyrrelser og ***større*** IKT-relaterede hændelser til de kompetente myndigheder.

***9a. ESA'erne udarbejder gennem Det Fælles Udvalg fælles retningslinjer for metoden til beregning af omkostningerne og kvantificering af de tab, der er omhandlet i stk. 9.***

*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. ***I overensstemmelse med sikkerhedskopieringspolitikken, der er omhandlet i stk. 1, litra a), bør*** systemer til sikkerhedskopiering ▌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 ***er adskilt enten fysisk eller logisk fra deres IKT-hovedsystem*** 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 genoprette 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 ***vurderer behovet for at opretholde*** redundante IKT-kapaciteter, der er udstyret med ressourcer, kapaciteter og funktionaliteter, der er tilstrækkelige og passende med henblik på at sikre forretningsmæssige behov ***og opfylde kravene til digital operationel modstandsdygtighed som fastsat i denne forordning***.

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 ▌ tilgængeligt for den finansielle enheds personale for at sikre driftsstabilitet for kritiske ***eller vigtige funktioner***, 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, ***hvorvidt funktionen er en kritisk eller vigtig funktion*** samt 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, ***sikrer de, at dataintegriteten er af højeste standard, f.eks. ved at udføre*** flere kontroller, herunder afstemninger ▌. ***Sådanne*** 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, 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 ***større*** 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***, der vedrører håndtering af IKT-risici, der er kortlagt som følge af større IKT-relaterede hændelser***, underrettes de kompetente myndigheder om ***alle væsentlige*** ændringer ***med angivelse af de krævede forbedringer, og hvordan de sigter mod at forhindre eller afbøde forstyrrelser fremadrettet***. ***Underretning af de kompetente myndigheder om ændringer kan finde sted forud for eller efter gennemførelsen af ændringerne.***

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, ***herunder hvor tæt disse risici er på kritiske eller vigtige funktioner***, 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. ***Oplysningsprogrammerne om IKT-sikkerhed gælder for alt personale. Uddannelse vedrørende digital operationel modstandsdygtighed skal mindst omfatte alle medarbejdere med direkte adgangsrettigheder til IKT-systemerne*** og den øverste ledelse. ***Uddannelsesmodulernes kompleksitet skal stå i et rimeligt forhold til den ansattes niveau af direkte adgang til IKT-systemer og skal navnlig tage hensyn til deres adgang til kritiske eller vigtige funktioner.***

De finansielle enheder, ***der ikke er mikrovirksomheder***, 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 ***i det mindste væsentlige*** IKT-relaterede hændelser eller

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

***De kommunikationsplaner, der er omhandlet i første afsnit, skal også sikre, at der hvert år gives en oversigt over alle IKT-relaterede hændelser til kunder og modparter. En sådan offentliggørelse skal fuldt ud respektere den finansielle enheds og dens kunders og modparters forretningshemmeligheder og må ikke bringe den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, i fare.***

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 ***i det mindste større*** IKT-relaterede hændelser og til dette formål varetage rollen som talsperson over 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 ***og unødige forsinkelser***

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.

***Artikel 14a***

***Ramme for IKT-risikostyring for små og ikke indbyrdes forbundne enheder, der er omfattet af en undtagelse***

***1. I henhold til artikel 3a skal små og ikke indbyrdes forbundne investeringsselskaber og betalingsinstitutter, der er undtaget ved direktiv (EU) 2015/2366, kreditinstitutter, der er undtaget ved direktiv 2013/36/EU, e-pengeinstitutter, der er undtaget ved direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser indføre og opretholde en forsvarlig og dokumenteret ramme for IKT-risikostyring, som:***

***a) indeholder detaljer for mekanismer og foranstaltninger med henblik på en hurtig, effektiv og omfattende styring af alle IKT-risici, herunder med henblik på beskyttelsen af relevante fysiske komponenter og infrastrukturer***

***b) løbende overvåger sikkerheden og driften af alle IKT-systemer***

***c) minimerer virkningen af IKT-risici gennem anvendelsen af forsvarlige, modstandsdygtige og opdaterede IKT-systemer, protokoller og værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester***

***d) i tilstrækkelig grad beskytter datanetværks og informationssystemers fortrolighed, integritet og tilgængelighed***

***e) gør det muligt hurtigt at identificere og detektere risikokilder og anomalier i netværket og informationssystemerne og hurtigt at håndtere IKT-hændelser.***

***2. Den i stk. 1 omhandlede ramme for IKT-risikostyring skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større IKT-relaterede 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.***

***Der skal hvert år forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed.***

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 ***og processer***, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af IKT-relaterede hændelser, således at de grundlæggende årsager identificeres og ***håndteres*** 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 ***som minimum*** 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 ***større*** 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 ▌

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 ***i samordning med*** 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 ***større*** 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 tager desuden hensyn til, at små virksomheders og mikrovirksomheders rettidige og effektive håndtering af en hændelse ikke må begrænses af behovet for at overholde de klassificeringskrav, der er fastlagt i denne artikel. ESA'erne tager også hensyn til de finansielle enheders størrelse, arten, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer og deres overordnede risikoprofil.***

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

Kommissionen tillægges beføjelse til at 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. De finansielle 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.

***1a. De finansielle enheder kan på frivillig basis underrette den relevante kompetente myndighed om væsentlige cybertrusler, når de anser truslen for at være af relevans for det finansielle system, tjenestebrugere eller kunder. Den relevante kompetente myndighed kan give sådanne oplysninger til andre relevante myndigheder i overensstemmelse med stk. 5.***

2. Hvis en større IKT-relateret hændelse ***indtræffer og har væsentlige*** virkninger for tjenestebrugeres og kunders finansielle interesser, underretter de finansielle enheder uden unødigt ophold ***efter at have fået kendskab hertil*** deres tjenestebrugere og kunder om den større IKT-relaterede hændelse og underretter dem ▌ om alle de ***relevante*** foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. ***Hvis ingen tjenestebrugere og kunder lider skade som følge af de modforanstaltninger, som den finansielle enhed har truffet, bortfalder kravet om at underrette tjenestebrugerne og kunderne.***

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

   a) en indledende underretning ▌ om ***den*** større ***IKT-relaterede*** hændelse, ***som skal indeholde de oplysninger, som den underrettende enhed på grundlag af rimelige foranstaltninger har adgang til, som følger:***

      ***i) for så vidt angår hændelser, som i væsentlig grad forstyrrer adgangen til de tjenester, der leveres af den finansielle enhed, skal den kompetente myndighed underrettes uden unødig forsinkelse og under alle omstændigheder inden for 24 timer, efter at den finansielle enhed har fået kendskab til hændelsen***

      ***ii) for så vidt angår hændelser, der har en væsentlig indvirkning på den finansielle enhed, bortset fra tilgængeligheden af de tjenester, der leveres af den pågældende finansielle enhed, skal den kompetente myndighed underrettes uden unødig forsinkelse og under alle omstændigheder inden for 72 timer, efter at den finansielle enhed har fået kendskab til hændelsen***

      ***iii) for så vidt angår hændelser, som har en indvirkning på integriteten, fortroligheden eller sikkerheden af personoplysninger, som den finansielle enhed opbevarer, skal den kompetente myndighed underrettes uden unødig forsinkelse og under alle omstændigheder inden for 24 timer, efter at den finansielle enhed har fået kendskab til hændelsen***

b) en foreløbig rapport, ***så snart den oprindelige hændelses status har ændret sig i væsentlig grad, eller der foreligger nye oplysninger, som kan have en stor indvirkning på, hvordan den IKT-relaterede hændelse håndteres af den kompetente myndighed,*** 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 ***den dato***, hvor den første indberetning indgives

***ca) i tilfælde af en stadig igangværende hændelse på tidspunktet for forelæggelsen af den endelige rapport, der er omhandlet i litra c), forelægges en endelig rapport en måned efter, at der er fundet en løsning på hændelsen.***

***Den relevante kompetente myndighed som omhandlet i artikel 41 sikrer, at en finansiel enhed i behørigt begrundede tilfælde har tilladelse til at fravige de frister, der er fastsat i litra a), b), c) og ca) i dette stykke, idet der tages behørigt hensyn til de finansielle enheders mulighed for at formidle præcise og relevante oplysninger vedrørende større IKT-relaterede hændelser.***

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. ***I tilfælde af en sådan uddelegering er den finansielle enhed fortsat fuldt ud ansvarlig for opfyldelsen af kravene vedrørende indberetning af hændelser.***

5. Når den kompetente myndighed modtager den i stk. 1 omhandlede rapport, forelægger den kompetente myndighed uden unødigt ophold nærmere oplysninger om ***den større IKT-relaterede hændelse*** 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 ***eller CSIRT'er, som er udpeget i henhold til artikel 9 i direktiv (EU) 2016/1149***

***ca) den afviklingsmyndighed, der er ansvarlig for den relevante finansielle enhed. Den Fælles Afviklingsinstans (SRB) for så vidt angår de enheder, der er omhandlet i artikel 7, stk. 2, i forordning (EU) nr. 806/2014, og for de enheder og koncerner, som er omhandlet i artikel 7, stk. 4, litra b), og artikel 7, stk. 5, i forordning (EU) nr. 806/2014, hvis betingelserne for anvendelse af disse stykker er opfyldt***

***cb) nationale afviklingsmyndigheder i forbindelse med de enheder og koncerner, der er omhandlet i artikel 7, stk. 3, i forordning (EU) nr. 806/2014. De nationale afviklingsmyndigheder forelægger hvert kvartal SRB en***

***sammenfatning af de rapporter, de har modtaget i henhold til dette litra, vedrørende de enheder og koncerner, der er omhandlet i artikel 7, stk. 3, i forordning (EU) nr. 806/2014***

***cc) andre relevante offentlige myndigheder, herunder myndigheder i andre medlemsstater.***

6. EBA, ESMA eller EIOPA og ECB vurderer ***i samarbejde med ENISA*** 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

***3) yderligere at præcisere kriterierne for at fastslå indvirkningen af en større IKT-relateret hændelse på en finansiel enhed med henblik på artikel 17, stk. 3, litra a)***

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 ***første afsnit***, litra a), og det fælles udkast til gennemførelsesmæssige tekniske standarder, der er omhandlet i ***første afsnit***, litra b), for Kommissionen senest den xx 202x [Publikationskontoret: Indsæt datoen ***to*** år efter ikrafttrædelsesdatoen].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de fælles reguleringsmæssige tekniske standarder, der er omhandlet i ***første afsnit***, 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 ***første afsnit***, litra b), i overensstemmelse med artikel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

***2. Indtil resultatet af den rapport med en vurdering af muligheden for yderligere centralisering af indberetningen af hændelser, der er omhandlet i artikel 19, foreligger, udarbejder ESA'erne gennem det fælles udvalg og i samarbejde med de kompetente myndigheder, ECB, SRB og ENISA retningslinjer for udveksling af oplysninger om større IKT-relaterede hændelsesindberetninger i overensstemmelse med artikel 17, stk. 5.***

***De i første afsnit nævnte retningslinjer skal som minimum omfatte følgende:***

***a) de mest effektive kommunikationsveje***

***b) opretholdelse af sikkerheden, fortroligheden og integriteten af de data, der udveksles***

***c) eventuel inddragelse af de finansielle enheder som supplement til den udveksling af oplysninger, der er omhandlet i artikel 40.***

*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 ***fælles*** EU-knudepunkt

   b) fordele, begrænsninger og mulige risici

   ***ba) mulighed for at fastslå interoperabiliteten og vurdere dens merværdi for så vidt angår andre relevante indberetningsordninger, herunder direktiv (EU) 2016/1148***

   c) elementer af den operationelle styring

   d) betingelser for medlemskab

   e) vilkår for finansielle enheders og nationale kompetente myndigheders adgang til ***det fælles EU-knudepunkt***

   f) en foreløbig vurdering af de finansielle omkostninger, der er forbundet med oprettelsen af en operationel platform, der understøtter ***det fælles EU-knudepunkt***, 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 ***og giver også passende anonymiserede tilbagemeldinger, oplysninger og efterretninger til alle relevante finansielle enheder, hvis det kunne være fordelagtigt, på baggrund af indberetninger af større IKT-relaterede hændelser, som den modtager***.

2. ESA'erne aflægger via det fælles udvalg en årlig rapport baseret på et anonymiseret og samlet grundlag for ***indberetninger*** om ***større*** 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, ***anslåede*** 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.

***Artikel 20a***

***Operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser vedrørende visse finansielle enheder***

***Kravene fastlagt i dette kapitel finder også anvendelse på operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser og på større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, hvis disse vedrører de finansielle enheder, som er omhandlet i artikel 2, stk. 1, litra a), b) og c).***

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***, der ikke er mikrovirksomheder,*** 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 test gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. ***Hvis test gennemføres af en intern tester, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.***

5. De finansielle enheder fastlægger procedurer og politikker med henblik på at prioritere, klassificere og ***håndtere*** 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 ***sikrer, at der gennemføres passende test*** af 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.

***Disse test kan omfatte*** 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. ***3, andet afsnit***, foretager mindst hvert 3. år avancerede test ved hjælp af trusselsbaserede penetrationstest.

2. Trusselsbaserede penetrationstest skal som minimum omfatte en finansiel enheds kritiske ***eller vigtige*** funktioner og tjenester og foretages på live-produktionssystemer, der understøtter sådanne funktioner***, såfremt det er muligt, eller på forproduktionssystemer med den samme sikkerhedskonfiguration***. Det nøjagtige omfang af trusselsbaserede penetrationstest, der baseres på en vurdering af kritiske ***eller vigtige*** funktioner og tjenester, fastsættes af de finansielle enheder og valideres af de kompetente myndigheder. ***Det er ikke et krav, at en enkelt trusselsbaseret penetrationstest skal omfatte alle kritiske eller vigtige funktioner.***

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

   Hvis ***kritiske*** tredjepartsudbydere af IKT-tjenester ***og, om nødvendigt, ikkekritiske tredjepartsudbydere af IKT-tjenester*** medtages i den trusselsbaserede penetrationstest, træffer den finansielle enhed de nødvendige foranstaltninger til at sikre disse udbyderes deltagelse. ***Disse tredjepartsudbydere af IKT-tjenester må ikke pålægges at meddele oplysninger eller fremlægge detaljer om elementer, som ikke er relevante for de relevante finansielle enheders kritiske eller vigtige tjenesters risikostyringskontrol. Disse test må ikke have en negativ indvirkning på andre kunder, som tredjepartsudbyderne af IKT-tjenester har.***

   ***Hvis inddragelsen af en tredjepartsudbyder af IKT-tjenester i den trusselsbaserede penetrationstest eventuelt kan påvirke kvaliteten, fortroligheden eller sikkerheden i forbindelse med leveringen af tredjepartsudbyderens IKT-tjenester til andre kunder, som ikke er omfattet af denne forordning, eller kan påvirke den samlede integritet af de operationer, som tredjepartsudbyderen af IKT-tjenester udfører, kan den finansielle enhed og tredjepartsudbyderen af IKT-tjenester indgå en kontraktlig aftale om, at tredjepartsudbyderen af IKT-tjenester har tilladelse til direkte at indgå kontraktlige ordninger med en ekstern tester. Tredjepartsudbydere af IKT-tjenester kan indgå sådanne ordninger på vegne af alle deres finansielle enheders tjenestebrugere med henblik på at foretage en samlet afprøvning.***

   De finansielle enheder anvender effektiv risikostyringskontrol for at ***afbøde*** risici for potentielle virkninger for data, skade på aktiver og forstyrrelser for kritiske ***eller vigtige funktioner*** 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 offentlige myndighed, der er udpeget i overensstemmelse med stk. 3a, eller – hvis tredjepartsudbydere af IKT-tjenester indgår kontraktlige ordninger med eksterne testere direkte – ENISA et fortroligt sammendrag af testresultaterne og*** dokumentation, som bekræfter, at den trusselsbaserede penetrationstest er blevet gennemført i overensstemmelse med kravene. ***Denne offentlige myndighed eller ENISA, alt efter hvad der er relevant,*** udsteder en erklæring***, der bekræfter, at testen blev udført i overensstemmelse med kravene i dokumentationen, for at give mulighed for gensidig anerkendelse af trusselsbaserede penetrationstest blandt de kompetente myndigheder***. ***Erklæringen deles med den finansielle enheds kompetente myndighed og, hvis det er relevant, med den ledende tilsynsførende for den kritiske tredjepartsudbyder af IKT-tjenester.***

3. De finansielle enheder ***eller tredjepartsudbydere af IKT-tjenester, der har tilladelse til at indgå kontraktlige ordninger direkte med en ekstern tester i overensstemmelse med stk. 2 i denne artikel, indgår kontrakter med*** testere i overensstemmelse med artikel 24 med henblik på at gennemføre trusselsbaserede penetrationstest.

***Uden at det berører deres muligheder for at uddelegere opgaver og kompetencer i henhold til denne artikel til andre kompetente myndigheder, som har ansvaret for trusselsbaserede penetrationstest, identificerer*** de kompetente myndigheder finansielle enheder med henblik på at gennemføre trusselsbaserede penetrationstest på en ***forholdsmæssig*** måde ▌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.

***3a. Medlemsstaterne udpeger én enkelt offentlig myndighed, der er ansvarlig for trusselsbaserede penetrationstest i den finansielle sektor på nationalt plan, bortset fra identifikation af finansielle enheder i overensstemmelse med stk. 3, herunder trusselsbaserede penetrationstest, der foretages af finansielle enheder og af tredjepartsudbydere af IKT-tjenester, som indgår kontraktlige ordninger med eksterne testere direkte. Denne udpegede offentlige myndighed tildeles alle kompetencer og opgaver med henblik herpå.***

4. ***ESA'erne*** udarbejder ***i samordning med ENISA og*** efter høring af ECB og under hensyntagen til de relevante EU-rammer, som finder anvendelse på efterretningsbaserede ***trusselsbaserede*** penetrationstest, ***herunder TIBER-EU-rammen, ét sæt*** udkast til reguleringsmæssige tekniske standarder med henblik på yderligere at præcisere følgende:

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

b) kravene vedrørende

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

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

iii) resultaterne af testen, testens afslutnings- og udbedringsfaser

c) den type tilsynsmæssigt samarbejde, der er nødvendigt for at gennemføre ***og lette fuld gensidig anerkendelse af*** trusselsbaserede penetrationstest i forbindelse med finansielle enheder, der opererer i mere end én medlemsstat, ***og test foretaget af eksterne testere, der i overensstemmelse med stk. 2 i denne artikel direkte har indgået kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester,*** 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 ***seks*** 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 ***og tredjepartsudbydere af IKT-tjenester, der i overensstemmelse med artikel 23, stk. 2, har tilladelse til direkte at indgå kontraktlige ordninger med en ekstern tester,*** 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***, uanset om testerne er fra Unionen eller fra et tredjeland***

d) ▌på uafhængig vis ***giver*** 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) ▌er behørigt og fuldt ud dækket af relevante erhvervsansvarsforsikringer, herunder mod risici for forseelser og forsømmelighed

***ea) hvis der er tale om interne testere, er blevet godkendt til at blive anvendt af den relevante kompetente myndighed og af den offentlige myndighed, der er udpeget i overensstemmelse med artikel 23, stk. 3a, og hvor disse myndigheder***

***har kontrolleret, at den finansielle enhed har afsat tilstrækkelige ressourcer og sikret, at interessekonflikter undgås i hele testens udformnings- og gennemførelsesfaser.***

2. De finansielle enheder ***og tredjepartsudbydere af IKT-tjenester, der i overensstemmelse med artikel 23, stk. 2, har tilladelse til direkte at indgå kontraktlige ordninger med en ekstern tester,*** sikrer, at der i de ***ordninger***, 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) ***art,*** 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.

   ***ba) hvorvidt en udbyder af IKT-tjenester er en koncernintern udbyder af IKT-tjenester.***

3. De finansielle enheder***, som ikke er mikrovirksomheder,*** vedtager og gennemgår regelmæssigt en strategi for IKT-tredjepartsrisici som led i deres ramme for IKT-risikostyring ▌. 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, ***som støtter kritiske eller vigtige funktioner,*** der leveres af tredjepartsudbydere af IKT-tjenester.

   De i første afsnit omhandlede kontraktlige ordninger skal være behørigt dokumenteret ▌.

   ***De finansielle enheder skal følge eventuelle retningslinjer og andre foranstaltninger, som ESA'erne og de kompetente myndigheder har indført, indtil de gennemførelsesmæssige tekniske standarder, der er omhandlet i stk. 10, træder i kraft.***

De finansielle enheder indberetter mindst én gang om året oplysninger til de kompetente myndigheder om antallet af nye ordninger om brugen af IKT-tjenester, ***der støtter kritiske eller vigtige funktioner,*** 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 ***ajourførte*** standarder for informationssikkerhed. ***De seneste standarder tages også i betragtning, når det skal fastslås, om de indførte sikkerhedsstandarder er passende.***

7. Når finansielle enheder udøver adgangs-, inspektions- og revisionsrettigheder over for tredjepartsudbyderen af IKT-tjenester, ***som vedrører kritiske eller vigtige funktioner,*** 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 ***detaljeret*** 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 ***giver de finansielle enheder mulighed for at træffe passende korrigerende eller afhjælpende foranstaltninger, som kan omfatte en fuldstændig opsigelse af ordningerne, hvis det ikke er muligt at foretage en udbedring, eller en delvis opsigelse***

***af ordningerne, hvis det er muligt at foretage en udbedring, i henhold til gældende ret,*** som minimum under følgende omstændigheder:

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

***aa) en henstilling fra det fælles tilsynsorgan, jf. artikel 37, til en kritisk tredjepartsudbyder af IKT-tjenester***

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 ***med hensyn til*** dennes overordnede IKT-risikostyring ***af dennes kontrakt med den finansielle enhed***, 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 ***påviseligt*** ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af de respektive kontraktlige ordninger.

***8a. Med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed kan den finansielle enhed under behørigt begrundede omstændigheder og efter aftale med dennes kompetente myndigheder beslutte ikke at opsige de kontraktlige ordninger med tredjepartsudbyderen af IKT-tjenester, før den kan skifte til en anden tredjepartsudbyder af IKT-tjenester eller til interne løsninger, der svarer overens med den leverede tjenestes kompleksitet, i overensstemmelse med den exitstrategi, der er omhandlet i stk. 9.***

***8b. I tilfælde, hvor de kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester opsiges under en af de omstændigheder, der er anført i stk. 8, litra a)-d), afholder de finansielle enheder ikke omkostningerne ved at overføre data fra en tredjepartsudbyder af IKT-tjenester, hvis overførslen overstiger de omkostninger ved at overføre data, der er fastsat i den oprindelige kontrakt.***

9. ***For IKT-tjenester, der vedrører kritiske eller vigtige funktioner, indfører*** de finansielle enheder ▌exitstrategier***, som skal revideres regelmæssigt. Exitstrategierne skal*** 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***, eller i tilfælde af opsigelse af de kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester under en af de omstændigheder, der er anført i stk. 8, litra a)-d)***.

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 ***18 måneder*** 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* ***underentreprise***

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***, der understøtter kritiske eller vigtige funktioner,*** 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***, der understøtter kritiske eller vigtige funktioner,*** 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***, der understøtter kritiske eller vigtige funktioner,*** 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 ▌.

Hvis der er indgået kontraktlige ordninger for brugen af IKT-tjenester***, der understøtter kritiske eller vigtige funktioner,*** med en tredjepartsudbyder af IKT-tjenester ▌, betragter de finansielle enheder mindst følgende faktorer som relevante:

a) ▌

b) ▌

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

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

***Hvis der er indgået kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, tager de finansielle enheder ud over de betragtninger, som er omhandlet i første og andet afsnit, også hensyn til følgende:***

***i) overholdelse af Unionens databeskyttelsesregler og***

***ii) effektiv håndhævelse af reglerne i denne forordning.***

***Hvis sådanne kontraktlige ordninger omfatter underentreprise af kritiske eller vigtige funktioner, vurderer*** de finansielle enheder, hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at ***vurdere de faktorer, der er opført i andet og tredje afsnit, for 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 ***på skrift og stilles til rådighed for*** parterne ▌på papir eller i et tilgængeligt format, som kan downloades.

2. ***De finansielle enheder og tredjepartsudbydere af IKT-tjenester skal sikre, at*** de kontraktlige ordninger for brugen af IKT-tjenester mindst ***omfatter*** 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, ***dvs. de regioner eller lande,*** hvor de udliciterede ***IKT-funktioner*** og ***-tjenester*** eller ***IKT-funktionerne*** og ***-tjenesterne*** i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af IKT-tjenester ***på forhånd*** skal underrette den finansielle enhed, hvis den har planer om at ændre sådanne steder

c) bestemmelser om adgang til, tilgængelighed, integritet, sikkerhed***, fortrolighed*** og beskyttelse af ***oplysninger, herunder*** personoplysninger

***ca)*** bestemmelser 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***, eller i tilfælde af opsigelse af de kontraktlige ordninger***

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) ▌

f) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at yde bistand i tilfælde af en IKT-hændelse***, der vedrører den leverede tjeneste***, 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 ***passende*** grad ***sikrer***, at den finansielle enhed kan foretage en sikker levering af tjenester i overensstemmelse med dens lovramme

h) ▌

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 ***og afviklingsmyndigheders*** forventninger ***og, hvis denne kontraktlige ordning påvirker en koncernintern udbyder af IKT-tjenester inden for samme koncern, en analyse baseret på en risikobaseret tilgang***

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

i) 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 ***eller sikre effektiv afvikling og omstrukturering heraf***

ii) 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

***iia) hvis denne kontraktlige ordning påvirker en koncernintern udbyder af IKT-tjenester inden for den samme koncern, skal den analyseres baseret på en risikobaseret tilgang***

***ka) en bestemmelse om den behandling af personoplysninger, som foretages af tredjepartsudbyderen af IKT-tjenester, og som skal være i overensstemmelse med forordning (EU) 2016/679.***

***2a. De kontraktlige ordninger for varetagelsen af kritiske eller vigtige funktioner skal i tillæg til stk. 2 som minimum omfatte følgende:***

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

***b) retten til løbende at overvåge de resultater, som tredjepartsudbyderen af IKT-tjenester opnår, og som omfatter følgende:***

***i) den finansielle enheds eller en udpeget tredjeparts ret til adgang, inspektion og revision og retten til at gennemgå kopier af relevant dokumentation på stedet, hvis de er kritiske for de aktiviteter, som tredjepartsudbyderen af IKT-tjenester udfører, idet denne rets 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) den forpligtelse, som tredjepartsudbyderen af IKT-tjenester har til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører, og nærmere oplysninger om omfanget af, vilkårene for og hyppigheden af sådanne inspektioner og revisioner.***

***Uanset litra b) kan tredjepartsudbyderen af IKT-tjenester og den finansielle enhed aftale, at retten til adgang, inspektion og revision kan uddelegeres til en uafhængig tredjepart, som udpeges af tredjepartsudbyderen af IKT-tjenester, og at den finansielle enhed til enhver tid kan anmode tredjeparten om oplysninger og garantier vedrørende de resultater, som tredjepartsudbyderen af IKT-tjenester opnår.***

***2b. De kontraktlige ordninger vedrørende leveringen af IKT-tjenester fra en tredjepartsudbyder af IKT-tjenester, som har hjemsted i et tredjeland, og som er blevet udpeget som kritisk i henhold til artikel 28, stk. 9, skal i tillæg til stk. 2 og 2a i denne artikel:***

***a) fastsætte, at kontrakten er underlagt en medlemsstats lovgivning, og***

***b) garantere, at det fælles tilsynsorgan og den ledende tilsynsførende kan udføre de opgaver, der er præciseret i artikel 30, på grundlag af deres kompetencer, som er angivet i artikel 31.***

***Det må ikke kræves, at de tjenester, som de indgåede kontraktlige ordninger omhandler, skal udføres af den virksomhed, som er etableret i Unionen i henhold til en medlemsstats lovgivning***

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

***3a. De kompetente myndigheder skal kunne få adgang til de kontraktlige ordninger, der er omhandlet i denne artikel. Parterne i disse kontraktlige ordninger kan aftale at redigere kommercielt følsomme eller fortrolige oplysninger, inden de giver en sådan adgang til de kompetente myndigheder, forudsat at sidstnævnte underrettes fuldt ud om omfanget og arten af de redigerede oplysninger.***

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. ***Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de også højde for de finansielle enheders størrelse, arten, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer og deres overordnede risikoprofil.***

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [Publikationskontoret: Indsæt datoen ***18 måneder*** 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 ***tilsynsorgan***, der er oprettet i henhold til artikel 29, stk. 1, ***og efter høring af ENISA***

   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.

   ***Den ledende tilsynsførende, der er udpeget i overensstemmelse med første afsnit, litra b), er ansvarlig for det daglige tilsyn med den kritiske tredjepartsudbyder af IKT-tjenester.***

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.

***fa) væsentligheden og vigtigheden af de tjenester, som leveres af den relevante tredjepartsudbyder af IKT-tjenester.***

***2a. Det fælles tilsynsorgan underretter tredjepartsudbyderen af IKT-tjenester, før den indleder sin vurdering med henblik på den i stk. 1, litra a), omhandlede udpegelse.***

***Det fælles tilsynsorgan underretter tredjepartsudbyderen af IKT-tjenester om resultatet af den vurdering, der er omhandlet i første afsnit, ved at fremlægge et udkast til en henstilling vedrørende den kritiske betydning. Senest seks uger efter modtagelsen af dette udkast til henstilling kan tredjepartsudbyderen af IKT-tjenester forelægge det fælles tilsynsorgan en begrundet erklæring om vurderingen. Den begrundede erklæring skal indeholde alle relevante supplerende oplysninger, som tredjepartsudbyderen af IKT-tjenester betragter som relevante for at underbygge fuldstændigheden og nøjagtigheden af udpegelsesproceduren eller for at anfægte udkastet til henstilling vedrørende den kritiske betydning. Det Fælles Udvalg af ESA'er skal tage behørigt hensyn til den begrundede erklæring og kan anmode om yderligere oplysninger eller dokumentation fra tredjepartsudbyderen af IKT-tjenester, inden der træffes en afgørelse om udpegelse.***

***Det Fælles Udvalg af ESA'er underretter tredjepartsudbyderen af IKT-tjenester om, at den er blevet udpeget som kritisk tredjepartsudbyder. Tredjepartsudbyderen af IKT-tjenester har mindst tre måneder fra datoen for modtagelse af underretningen til at foretage eventuelle nødvendige tilpasninger, som gør det muligt for det fælles tilsynsorgan at udføre sine opgaver i henhold til artikel 30, og til at underrette de finansielle enheder, til hvilke tredjepartsudbyderen af IKT-tjenester leverer tjenester. Det fælles tilsynsorgan kan give tilladelse til, at tilpasningsperioden forlænges med højst tre måneder, hvis den udpegede tredjepartsudbyder af IKT-tjenester fremlægger en behørigt begrundet anmodning herom.***

3. Kommissionen tillægges beføjelser til at vedtage ***en delegeret retsakt*** i

overensstemmelse med artikel 50 for at ***præcisere*** 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. ***Det fælles tilsynsorgan*** udarbejder, offentliggør og ajourfører ***regelmæssigt i samråd med ENISA*** 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 ***fælles tilsynsorgan***, der er oprettet i henhold til artikel 29. Det ***fælles tilsynsorgan*** vurderer finansielle enheders afhængighed af tredjepartsudbydere af IKT-tjenester på grundlag af oplysninger, som det modtager fra de kompetente myndigheder.

8. ***De*** 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.

***8a. Det Fælles Udvalg af ESA'er udpeger efter henstilling fra det fælles tilsynsorgan de tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland, som er kritiske for finansielle enheder, i overensstemmelse med stk. 1, litra a).***

***Ved udpegelsen som omhandlet i dette stykkes første afsnit følger ESA'erne og det fælles tilsynsorgan de proceduremæssige skridt, der er fastsat i stk. 2a.***

9. Finansielle enheder må ikke gøre brug af en ***kritisk*** tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland***, medmindre den pågældende tredjepartsudbyder af IKT-tjenester har en virksomhed, der er etableret i Unionen i henhold til en medlemsstats lovgivning og har indgået kontraktlige ordninger i overensstemmelse med artikel 27, stk. 2b***.

*Artikel 29*

*Tilsynsrammens struktur*

1. ***Det fælles tilsynsorgan oprettes*** med henblik på at ***føre tilsyn med*** IKT-tredjepartsrisici på tværs af finansielle sektorer ***og føre direkte tilsyn med tredjepartsudbydere af IKT-tjenester, der udpeges som kritiske i henhold til artikel 28***.

   ***Det fælles tilsynsorgans rolle begrænses til tilsynsbeføjelser, der er knyttet til IKT-risici vedrørende de IKT-tjenester, som leveres til finansielle enheder af kritiske tredjepartsudbydere af IKT-tjenester.***

   ***Det fælles tilsynsorgan*** drøfter regelmæssigt relevante udviklingstendenser vedrørende IKT-risici og -sårbarheder og fremmer en ensartet tilgang til overvågning af IKT-

tredjepartsrisici på EU-plan.

2. ***Det fælles tilsynsorgan*** 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.

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

3. ***Det fælles tilsynsorgan*** er sammensat af ***de administrerende direktører*** for ESA'erne***,*** én repræsentant på højt niveau for personalet i ***hver ESA og én repræsentant på højt niveau fra mindst otte af de nationale kompetente myndigheder***. Én repræsentant fra henholdsvis Europa-Kommissionen, ESRB, ECB og ENISA ***og mindst én uafhængig ekspert, der udnævnes i overensstemmelse med stk. 3a i denne artikel,*** deltager ▌ som observatører.

   ***Efter den årlige udpegelse af kritiske tredjepartsudbydere af IKT-tjenester, i henhold til artikel 28, stk. 1, litra a), træffer Det Fælles Udvalg af ESA'er afgørelse om, hvilke nationale kompetente myndigheder der skal være medlemmer af det fælles tilsynsorgan under hensyntagen til følgende faktorer:***

   ***a) antallet af kritiske tredjepartsudbydere af IKT-tjenester, der er etableret i eller leverer tjenester i en medlemsstat***

   ***b) de finansielle enheders afhængighed af kritiske tredjepartsudbydere af IKT-tjenester i en medlemsstat***

   ***c) en national kompetent myndigheds relative ekspertise***

   ***d) en national kompetent myndigheds tilgængelige ressourcer og kapacitet***

   ***e) behovet for, at det fælles tilsynsorgans drift og beslutningstagning er strømlinet, enkel og effektiv.***

   ***Det fælles tilsynsorgan deler sin dokumentation og sine afgørelser med alle nationale kompetente myndigheder, der ikke er medlemmer af det fælles tilsynsorgan.***

   ***Det fælles tilsynsorgans arbejde understøttes og bistås af særligt personale fra ESA'erne.***

***3a. Den uafhængige ekspert, der er omhandlet i denne artikels stk. 3, udnævnes som observatør af det fælles tilsynsorgan efter en offentlig og gennemsigtig ansøgningsproces.***

   ***Den uafhængige ekspert udnævnes for en toårig periode på grundlag af sin ekspertise i finansiel stabilitet, digital operationel modstandsdygtighed og IKT-sikkerhedsspørgsmål.***

   ***Den udnævnte uafhængige ekspert må ikke varetage noget hverv på nationalt plan, EU-plan eller internationalt plan. Den uafhængige ekspert handler uafhængigt og objektivt udelukkende i Unionens interesse som helhed og må ikke søge eller modtage***

***instrukser fra Unionens institutioner eller organer, medlemsstaternes regeringer eller noget andet offentligt eller privat organ.***

***Det fælles tilsynsorgan kan beslutte at udnævne mere end én uafhængig ekspert som observatør.***

4. 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 ***senest den [EUT: Indsæt datoen 18 måneder efter denne forordnings ikrafttrædelsesdato]*** for samarbejdet mellem ***det fælles tilsynsorgan, den ledende tilsynsførende*** og de kompetente myndigheder om de nærmere procedurer og betingelser, som vedrører varetagelsen af opgaver mellem de kompetente myndigheder og ***det fælles tilsynsorgan***, samt nærmere oplysninger om den informationsudveksling, der er nødvendig for de kompetente myndigheder, således at de kan sikre opfølgning af de henstillinger, som ***det fælles tilsynsorgan*** i medfør af artikel 31, stk. 1, litra d), fremsætter over for kritiske tredjepartsudbydere af IKT-tjenester.

5. 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.

6. ***Det fælles tilsynsorgan*** forelægger hvert år Europa-Parlamentet, Rådet og Kommissionen en rapport om anvendelsen af denne afdeling ▌.

*Artikel 30*

*Den ledende tilsynsførendes opgaver*

1. Den ledende tilsynsførende***, der er udnævnt i henhold til artikel 28, stk. 1, litra b), leder og koordinerer det daglige tilsyn med kritiske tredjepartsudbydere af IKT-tjenester og er det primære kontaktpunkt for disse kritiske tredjepartsudbydere af IKT-tjenester***.

***1a.*** ***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. ***Vurderingen skal primært fokusere på de IKT-tjenester, der støtter kritiske eller vigtige funktioner, som den kritiske tredjepartsudbyder af IKT-tjenester leverer til finansielle enheder, men kan også være bredere, hvis det er relevant for vurderingen af risiciene for disse funktioner.***

2. Den i stk. ***1a*** 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 tid 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 ***større*** 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. ***1a*** omhandlede vurdering***, som den ledende tilsynsførende har foretaget***, ***udarbejder og fremsætter det fælles tilsynsorgan, under koordinering og ledelse af den ledende tilsynsførende, udkast til*** en klar, detaljeret og begrundet individuel tilsynsplan for hver enkelt kritisk tredjepartsudbyder af IKT-tjenester.

***Når det fælles tilsynsorgan udarbejder udkastet til tilsynsplan, hører det alle relevante kompetente myndigheder og de i artikel 8 i direktiv (EU) 2016/1148 omhandlede centrale kontaktpunkter for at sikre, at der ikke er nogen uoverensstemmelser eller overlapninger med de forpligtelser, der påhviler kritiske tredjepartsudbydere af IKT-tjenester i henhold til det pågældende direktiv.***

***Tilsynsplanen vedtages årligt af den ledende tilsynsførendes bestyrelse.***

***Forud for vedtagelsen*** skal ***udkastet til tilsynsplan*** meddeles den kritiske tredjepartsudbyder af IKT-tjenester.

***Efter modtagelsen af udkastet til tilsynsplan har den kritiske tredjepartsudbyder af IKT-tjenester en frist på seks uger til at gennemgå og indgive en begrundet erklæring om udkastet til tilsynsplan. En sådan begrundet erklæring kan kun indgives, hvis den kritiske tredjepartsudbyder af IKT-tjenester er i stand til at fremlægge dokumentation for, at gennemførelsen af tilsynsplanen ville kunne medføre konsekvenser eller forstyrrelser i et uforholdsmæssigt stort omfang for kunder, der ikke er omfattet af denne forordning, eller hvis der findes en mere effektiv eller virkningsfuld løsning til håndtering af de identificerede IKT-risici. Hvis der indgives en sådan erklæring, skal den kritiske tredjepartsudbyder af IKT-tjenester foreslå det fælles tilsynsorgan en mere effektiv og virkningsfuld løsning for at nå målene i udkastet til tilsynsplan.***

***Inden vedtagelsen af tilsynsplanen skal den ledende tilsynsførendes bestyrelse tage behørigt hensyn til den begrundede erklæring og kan anmode om yderligere oplysninger eller dokumentation fra tredjepartsudbyderen af IKT-tjenester.***

4. Når de i 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 ***det fælles tilsynsorgan***.

*Artikel 31*

***Tilsynsbeføjelser***

1. Med henblik på varetagelsen af de i denne afdeling omhandlede opgaver tillægges den ledende tilsynsførende følgende beføjelser ***med hensyn til de tjenester, der leveres af kritiske tredjepartsudbydere af IKT-tjenester til finansielle enheder***:

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

   b) at foretage generelle undersøgelser og inspektioner ***på stedet*** 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 ***stk. 1a*** omhandlede henstillinger

***1a. Med henblik på udførelsen af de i denne afdeling omhandlede opgaver og på grundlag af de oplysninger, som den ledende tilsynsførende har indhentet, og resultaterne af de undersøgelser, der er foretaget af den ledende tilsynsførende, har det fælles tilsynsorgan beføjelse til*** 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 ***det fælles tilsynsorgan*** 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 ***det fælles tilsynsorgan*** 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 ***det fælles tilsynsorgan*** 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 ***og har ikke en virksomhed, der er oprettet i Unionen i henhold til en medlemsstats nationale ret***

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

– ***underentreprisen vil medføre alvorlige og klare risici for den finansielle enhed eller den finansielle stabilitet i Unionens finansielle system.***

***1b. De beføjelser, der er omhandlet i stk. 1 og 1a, udøves med hensyn til de IKT-tjenester, der understøtter ikkekritiske eller vigtige funktioner, som tilvejebringes af den kritiske tredjepartsudbyder af IKT-tjenester, når det er nødvendigt.***

***1c. Når den ledende tilsynsførende og det fælles tilsynsorgan udøver de i stk. 1 og 1a omhandlede beføjelser, tager de behørigt hensyn til de rammer, der er fastlagt i direktiv (EU) 2016/1148, og hører, hvor det er nødvendigt, de relevante kompetente myndigheder som fastsat i dette direktiv for at undgå unødvendig overlapning med tekniske og organisatoriske foranstaltninger, som kan gælde for kritiske tredjepartsudbydere af IKT-tjenester i henhold til samme direktiv.***

2. ***Forud for færdigbehandlingen og udstedelsen af henstillinger, i overensstemmelse med stk. 1a, underretter det fælles tilsynsorgan den kritiske tredjepartsudbyder af IKT-tjenester om sine hensigter og giver tredjepartsudbyderen af IKT-tjenester mulighed for at fremlægge oplysninger, som denne mener, der bør tages hensyn til, inden henstillingen færdigbehandles, eller med henblik på at anfægte de påtænkte henstillinger. En henstilling kan anfægtes på grundlag af, at den ville kunne medføre konsekvenser eller forstyrrelser i et uforholdsmæssigt stort omfang for kunder, som ikke er omfattet af nærværende forordning, eller at der findes en mere effektiv eller virkningsfuld løsning for at håndtere de identificerede risici.***

3. Kritiske tredjepartsudbydere af IKT-tjenester samarbejder i god tro med ***og bistår*** den ledende tilsynsførende ***og det fælles tilsynsorgan*** med hensyn til varetagelsen af ***deres*** opgaver.

4. ***I tilfælde af hel eller delvis manglende overholdelse af de foranstaltninger, der skal træffes i henhold til stk. 1, litra a), b) eller c), og efter udløbet af en periode på mindst 60 kalenderdage fra den dato, hvor den kritiske tredjepartsudbyder af IKT-tjenester modtog underretning om foranstaltningen***, ***kan den ledende tilsynsførende beslutte*** at pålægge tvangsbøder for at tvinge den kritiske tredjepartsudbyder af IKT-tjenester til at efterleve kravene.

***4a. De i stk. 4 omhandlede tvangsbøder pålægges kun af den ledende tilsynsførende som en sidste udvej og i tilfælde, hvor den kritiske tredjepartsudbyder af IKT-tjenester ikke har overholdt de foranstaltninger, der skal træffes i overensstemmelse med stk. 1, litra a), b) eller 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 ***op til*** 1 % af den gennemsnitlige daglige omsætning på verdensplan, ***som vedrører tjenester, der leveres til finansielle enheder, der er omfattet af denne forordning, og*** 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. Domstolene 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.

   ***Kritiske tredjepartsudbydere af IKT-tjenester skal kun levere de oplysninger, der er omhandlet i første afsnit, for så vidt angår de tjenester, der leveres til finansielle enheder, som er omfattet af denne forordning, og som anvender tjenester fra kritiske tredjepartsudbydere af IKT-tjenester til kritiske eller vigtige funktioner. Kritiske tredjepartsudbydere af IKT-tjenester skal underrette den relevante finansielle enhed om de anmodninger, der er specifikke for den pågældende finansielle enhed.***

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 ***ved en afgørelse*** 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 ***rimelig*** 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, ***eller hvis de ikke fremlægges inden for den tidsfrist, som er omhandlet i litra d)***

   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 ***35***, stk. 1, foretage de nødvendige undersøgelser af tredjepartsudbydere af IKT-tjenester ***i overensstemmelse med proportionalitetsprincippet***. ***Ved gennemførelsen af undersøgelserne skal den ledende tilsynsførende udvise forsigtighed og sikre, at rettighederne for de kunder hos kritiske tredjepartsudbydere af IKT-tjenester, som ikke er omfattet af nærværende forordning, beskyttes, herunder i relation til indvirkningen på serviceniveauer, tilgængeligheden af data og fortroligheden.***

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) ***på sikker vis at gennemgå*** 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.

***Beføjelsen til at foretage inspektioner på stedet, som omhandlet i første afsnit, er ikke begrænset til steder i Unionen, forudsat at inspektionen af et sted i et tredjeland opfylder alle følgende krav:***

- ***den er nødvendig, for at den ledende tilsynsførende kan udføre sine opgaver i henhold til denne forordning***
- ***den har en direkte forbindelse til leveringen af IKT-tjenester til finansielle enheder i Unionen***
- ***den er relevant for en igangværende undersøgelse.***

***1a. Når den ledende tilsynsførende og undersøgelsesholdet gennemfører inspektioner på stedet, skal de udvise forsigtighed og sikre, at rettighederne for kunder hos kritiske tredjepartsudbydere af IKT-tjenester, som ikke er omfattet af denne forordning, beskyttes, herunder i relation til indvirkningen på serviceniveauer, tilgængeligheden af data og fortroligheden.***

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, ***som det efter den ledende tilsynsførendes vurdering er hensigtsmæssigt og teknologisk relevant at inspicere, og som*** 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 på stedet, 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***, fra de andre ESA'er*** 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 vedtager ***det fælles tilsynsorgan*** henstillinger rettet mod 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 ***og det fælles tilsynsorgan*** 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 ***det fælles tilsynsorgan***, 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 ***det fælles tilsynsorgan*** i henhold til artikel 31, stk. ***1a***, underretter de kritiske tredjepartsudbydere af IKT-tjenester ***det fælles tilsynsorgan*** om, hvorvidt de agter at følge disse henstillinger. ***Det fælles tilsynsorgan*** videregiver straks disse oplysninger til de kompetente myndigheder***, som de pågældende finansielle enheder hører under***.

2. De kompetente myndigheder ***underretter de finansielle enheder, der har indgået kontraktlige aftaler med kritiske tredjepartsudbydere af IKT-tjenester, om de risici, der er identificeret af det fælles tilsynsorgan i henstillingerne til disse kritiske tredjepartsudbydere af IKT-tjenester i overensstemmelse med artikel 31, stk. 1a, og*** overvåger, om de finansielle enheder tager hensyn til de risici, der er identificeret. ***Det fælles tilsynsorgan fører tilsyn med, om de kritiske tredjepartsudbyderne af IKT-tjenester har håndteret de risici, der er identificeret i henstillingerne.***

3. ***Hvis de reguleringsmæssige mål ikke kan sikres gennem andre foranstaltninger, og de nationale kompetente myndigheder har udstedt advarsler til de berørte finansielle enheder på grundlag af oplysninger fra det fælles tilsynsorgan, kan den ledende tilsynsførendes bestyrelse, efter henstilling fra det fælles tilsynsorgan og efter høring af*** de kompetente myndigheder***, som de berørte finansielle enheder hører under, beslutte*** midlertidigt ***at suspendere***, enten helt eller delvist, anvendelsen eller udrulningen af en tjeneste, som ***leveres til finansielle enheder, som er udsat for*** de risici, der er identificeret i de henstillinger, der er meddelt de kritiske tredjepartsudbydere af IKT-tjenester***, indtil disse risici*** er blevet afhjulpet. De kan om nødvendigt***, og som en sidste udvej,*** kræve, at de ***kritiske tredjepartsudbydere af IKT-tjenester*** helt eller delvist opsiger de relevante kontraktlige ordninger, der er indgået med de ***finansielle enheder, som er udsat for de risici, der er identificeret***.

4. Når ***den ledende tilsynsførendes bestyrelse*** træffer de i stk. 3 omhandlede afgørelser, tager det 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) hvorvidt 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

   ***da) hvorvidt suspensionen eller opsigelsen indebærer en risiko for manglende kontinuitet i forretningsaktiviteterne for kunderne hos den kritiske tredjepartsudbyder af IKT-tjenester.***

***4a. De i stk. 3 omhandlede afgørelser gennemføres først, når alle berørte finansielle enheder er blevet behørigt underrettet herom. De berørte finansielle enheder***

***indrømmes en frist, som ikke må gå videre end, hvad der er strengt nødvendigt, for at tilpasse deres ordninger for outsourcing og kontraktlige ordninger med kritiske tredjepartsudbydere af IKT-tjenester på en sådan måde, at den digitale operationelle modstandsdygtighed ikke bringes i fare, og at deres exitstrategier og overgangsplaner, som omhandlet i artikel 25, gennemføres.***

***De kritiske tredjepartsudbydere af IKT-tjenester, der er omfattet af de i stk. 3 i denne artikel angivne afgørelser, skal samarbejde fuldt ud de berørte finansielle enheder.***

5. De kompetente myndigheder orienterer regelmæssigt ***det fælles tilsynsorgan*** om de tilgange og foranstaltninger, de har iværksat i forbindelse med deres tilsynsopgaver vedrørende finansielle enheder.

*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 omkostninger***, der opstår som følge af udførelsen af de i denne afdeling fastsatte opgaver,*** og stå i et rimeligt forhold til dennes omsætning.

***1a. Hvis der indgås en administrativ ordning med en regulerings- og tilsynsmyndighed i et tredjeland i overensstemmelse med stk. 1 i denne artikel, kan den pågældende myndighed indgå i det undersøgelseshold, der er omhandlet i artikel 35, stk. 1.***

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 ***bestræber sig på*** indbyrdes og med ***tredjepartsudbydere af IKT-tjenester*** at 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 og ***tredjepartsudbydere af IKT-tjenesters*** digitale operationelle modstandsdygtighed, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre cybertruslernes spredningsevne, understøtte forsvarskapaciteter, teknikker til detektion af trusler, strategier for afbødning eller indsats- og genopretningsfaser

   b) finder sted inden for pålidelige grupper af finansielle enheder og ***tredjepartsudbydere af IKT-tjenester***

   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[26] og retningslinjer for konkurrencepolitikken[27].

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.

---

[26] 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).

[27] 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).

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

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 ***og udbydere*** af kryptoaktiver, udstedere ***og udbydere*** 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 ***og operatører af værdipapirafviklingssystemer***: 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 ***pensionsordninger***: den kompetente myndighed, der er udpeget i henhold til artikel 47 i direktiv (EU) 2016/2341 den kompetente myndighed, der er udpeget i henhold til artikel 47 i direktiv (EU) 2016/2341

o) 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) ***2016/1011***

r) for udbydere af crowdfundingtjenester: den kompetente myndighed, der er udpeget i henhold til ***artikel 29*** i forordning (EU) ***2020/1503***

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, ***inviteres*** ESA'erne og de kompetente myndigheder ***til at deltage i samarbejdsgruppens arbejde, for så vidt dette arbejde vedrører henholdsvis overvågning af og tilsyn med enheder, som er opført under punkt 7 i bilag II til direktiv (EU) 2016/1148, og som desuden er blevet udpeget som kritiske tredjepartsudbydere af IKT-tjenester i henhold til artikel 28 i denne forordning.***

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.

***2a. Den ledende tilsynsførende underretter og samarbejder med de kompetente myndigheder, der er udpeget i henhold til direktiv (EU) 2016/1148, før denne foretager generelle undersøgelser og inspektioner på stedet, jf. artikel 33 og 34 i denne forordning.***

*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, ***Den Fælles Afviklingsinstans for så vidt angår oplysninger vedrørende enheder, der er omfattet af anvendelsesområdet for forordning (EU) nr. 806/2014,*** 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 ***en væsentlig cybertrussel***, 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***, de nationale afviklingsmyndigheder og Den Fælles Afviklingsinstans for så vidt angår oplysninger vedrørende de enheder, der er omfattet af anvendelsesområdet for forordning (EU) nr. 806/2014,*** 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 ***anses*** 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 **12 måneder** 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, ***pålagte sanktioner samt, undtagelsesvis,*** de ansvarlige personers identitet.

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 tre år fra den [*EUT: indsæt datoen 5 år efter nærværende forordnings ikrafttræden*]. ***Kommissionen udarbejder senest ni måneder inden udløbet af den femårige periode en rapport om delegationen af beføjelser. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.***

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 af 13. april 2016 om bedre lovgivning.

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 ***tre*** måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med ***tre*** måneder på Europa-Parlamentets eller Rådets initiativ.

KAPITEL IX

OVERGANGSBESTEMMELSER OG AFSLUTTENDE BESTEMMELSER

AFDELING I

*Artikel 51*

*Revisionsklausul*

Senest den [*Publikationskontoret: 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. ***Rapporten skal som minimum indeholde en gennemgang af følgende:***

***a)*** ***muligheden for at udvide denne forordnings anvendelsesområde til at omfatte betalingssystemoperatører***

***b)*** ***den frivillige karakter af indberetningen af alvorlige cybertrusler***

***c)*** kriterierne for udpegelse af kritiske tredjepartsudbydere af IKT-tjenester i henhold til artikel 28, stk. 2 ***og***

***d)*** ***effektiviteten af det fælles tilsynsorgans beslutningstagning og udvekslingen af oplysninger mellem det fælles tilsynsorgan og de nationale kompetente myndigheder, der ikke er medlemmer.***

*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:

"1. 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.

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

2) Stk. 2 udgår.

3) 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]."

*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 — **24** måneder efter ikrafttrædelsesdatoen*].

Dog finder artikel 23 og 24 anvendelse fra den [*Publikationskontoret: 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 […].

| | |
|---|---|
| *For Europa-Parlamentet* | *For Rådet* |
| *Formand* | *Formand* |

## PROCEDURE I KORRESPONDERENDE UDVALG

| | |
|---|---|
| **Titel** | Digital operationel modstandsdygtighed i den finansielle sektor og ændring af forordning (EF) nr. 10602009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014 |
| **Referencer** | COM(2020)0595 – C9-0304/2020 – 2020/0266(COD) |
| **Dato for høring af EP** | 24.9.2020 |
| **Korresponderende udvalg**<br>Dato for meddelelse på plenarmødet | ECON<br>17.12.2020 |
| **Rådgivende udvalg**<br>Dato for meddelelse på plenarmødet | ITRE IMCO<br>17.12.2020 17.12.2020 |
| **Ingen udtalelse**<br>Dato for afgørelse | ITRE IMCO<br>15.10.2020 27.10.2020 |
| **Ordførere**<br>Dato for valg | Billy Kelleher<br>15.10.2020 |
| **Behandling i udvalg** | 14.4.2021 14.6.2021 |
| **Dato for vedtagelse** | 1.12.2021 |
| **Resultat af den endelige afstemning** | +: 44<br>–: 5<br>0: 5 |
| **Til stede ved den endelige afstemning – medlemmer** | Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle |
| **Til stede ved den endelige afstemning – stedfortrædere** | Lefteris Christoforou |
| **Dato for indgivelse** | 7.12.2021 |

## ENDELIG AFSTEMNING VED NAVNEOPRÅB
## I KORRESPONDERENDE UDVALG

| 44 | + |
|---|---|
| ECR | Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle |
| NI | Enikő Győri |
| PPE | Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere |
| Renew | Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin |
| S&D | Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli |
| Verts/ALE | Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun |

| 5 | - |
|---|---|
| ID | Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen |
| NI | Lefteris Nikolaou-Alavanos |

| 5 | 0 |
|---|---|
| ID | Valentino Grant, Antonio Maria Rinaldi, Marco Zanni |
| The Left | José Gusmão, Martin Schirdewan |

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller