Rådet for
Den Europæiske Union

Bruxelles, den 14. november 2022
(OR. en)

14565/22

Interinstitutionel sag:
2020/0266(COD)

CODEC 1702
EF 332
ECOFIN 1140
TELECOM 445
CYBER 354
PE 126

ORIENTERENDE NOTE

fra:	Generalsekretariatet for Rådet
til:	De Faste Repræsentanters Komité/Rådet
Vedr.:	Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014 – Resultat af Europa-Parlamentets førstebehandling (9.-10. november 2022 i Bruxelles)

I. INDLEDNING

I henhold til bestemmelserne i artikel 294 i TEUF og den fælles erklæring om den praktiske gennemførelse af den fælles beslutningsprocedure[1] har der fundet en række uformelle kontakter sted mellem Rådet, Europa-Parlamentet og Kommissionen for at nå til enighed om denne sag ved førstebehandlingen.

[1] EUT C 145 af 30.6.2007, s. 5.

I den forbindelse forelagde formanden for Økonomi- og Valutaudvalget (ECON), Irene TINAGLI (S&D, IT), på vegne af udvalget et kompromisændringsforslag (ændringsforslag 2) til ovennævnte forslag til forordning. Der var opnået enighed om dette ændringsforslag under ovennævnte uformelle kontakter. Desuden fremsatte ID-gruppen fire ændringsforslag (ændringsforslag 3-6). Der blev ikke fremsat andre ændringsforslag.

II. AFSTEMNING

Ved afstemningen den 10. november 2022 vedtog plenarforsamlingen kompromisændringsforslaget (ændringsforslag 2) til ovennævnte forslag til forordning. Der blev ikke vedtaget andre ændringsforslag. Det således ændrede kommissionsforslag udgør Parlamentets førstebehandlingsholdning, som er indeholdt i dets lovgivningsmæssige beslutning, jf. bilaget til denne note[2].

Parlamentets holdning svarer til, hvad institutionerne tidligere var blevet enige om. Rådet bør derfor kunne godkende Parlamentets holdning.

Retsakten vil derefter blive vedtaget med den ordlyd, der svarer til Parlamentets holdning.

---

[2] Udgaven af Parlamentets holdning, der findes i den lovgivningsmæssige beslutning, er forsynet med angivelse af de ændringer, der er foretaget i Kommissionens forslag. Tilføjelser til Kommissionens tekst er fremhævet med ***fed skrift og kursiv***. Udgået tekst er markeret med "▌".

P9_TA(2022)0381

Digital finans: Forordningen om digital operationel modstandsdygtighed i den finansielle sektor (DORA)

Europa-Parlamentets lovgivningsmæssige beslutning af 10. november 2022 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 af 4. juni 2022 fra Den Europæiske Centralbank[3],

– der henviser til udtalelse af 24. februar 2021 fra Det Europæiske Økonomiske og Sociale Udvalg[4],

– der henviser til, at det kompetente udvalg har godkendt den foreløbige aftale i henhold til forretningsordenens artikel 74, stk. 4, og at Rådets repræsentant ved skrivelse af 29. juni 2022 forpligtede sig til at godkende Europa-Parlamentets holdning, jf. artikel 294, stk. 4, i traktaten om Den Europæiske Unions funktionsmåde,

– 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 erstatter, i væsentlig grad ændrer eller agter i væsentlig grad at ændre sit forslag;

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

---

[3] EUT C 343 af 26.8.2021, s. 1.
[4] EUT C 155 af 30.4.2021, s. 38.

P9_TC1-COD(2020)0266

Europa-Parlamentets holdning fastlagt ved førstebehandlingen den 10. november 2022 med henblik på vedtagelse af Europa-Parlamentets og Rådets forordning (EU) 2022/... 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, (EU) nr. 909/2014 og (EU) 2016/1011

(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[5],

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[6],

efter den almindelige lovgivningsprocedure[7], og

[5] EUT C 343 af 26.8.2021, s. 1.
[6] EUT C 155 af 30.4.2021, s. 38.
[7] Europa-Parlamentets holdning af 10.11.2022.

ud fra følgende betragtninger:

(1) I den digitale tidsalder understøtter informations- og kommunikationsteknologi (IKT) komplekse systemer, der anvendes i forbindelse med hverdagsaktiviteter. Den holder vores økonomier i gang i centrale sektorer, herunder den finansielle sektor, og fremmer det indre markeds funktion. Øget digitalisering og indbyrdes forbundethed forstærker også IKT-risiko, der gør samfundet som helhed og især det finansielle system mere sårbart over for cybertrusler eller IKT-forstyrrelser. Universel brug af IKT-systemer og en høj grad af digitalisering og konnektivitet er i dag vigtige kendetegn ved alle aktiviteter i Unionens finansielle enheder, men ***der skal gøres mere ved*** deres digitale modstandsdygtighed, og den skal integreres i deres bredere operationelle rammer.

(2) Brugen af IKT har i de seneste årtier indtaget en så central rolle inden for levering af finansielle tjenesteydelser, at den i dag har fået kritisk betydning for driften af typiske daglige funktioner i alle finansielle enheder. Digitalisering omfatter nu 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, ▌ behandling af skadesanmeldelser og back office-funktioner. ***Forsikringssektoren har også forandret sig med brugen af IKT, fra fremkomsten af forsikringsformidlere, der tilbyder deres tjenester online ved anvendelse af InsurTech, til digital tegning af forsikring.*** Finansiering er ikke kun blevet overvejende digital i hele sektoren, men digitalisering har også uddybet den indbyrdes forbundethed og afhængighed inden for den finansielle sektor og med 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, hvordan det eksisterende høje niveau af indbyrdes forbundethed blandt finansielle enheder, finansielle markeder og finansielle markedsinfrastrukturer, og navnlig deres IKT-systemers indbyrdes forbundethed, kan udgøre en systemisk sårbarhed, fordi lokaliserede cyberhændelser hurtigt kan sprede sig fra én af de ca. 22 000 finansielle enheder i Unionen til hele det finansielle system, uhindret af geografiske grænser. Alvorlige IKT-overtrædelser i den finansielle sektor har ikke kun virkninger for finansielle enheder isoleret set. De baner også vejen for udbredelsen af lokaliserede sårbarheder på tværs af de finansielle transmissionskanaler og udløser potentielt negative konsekvenser for stabiliteten i Unionens finansielle system såsom skabelse af likviditetsudstrømning og et generelt tab af tillid og tiltro til finansielle markeder.

(4) I de seneste år har politiske beslutningstagere, lovgivere og standardiseringsorganer på internationalt plan, EU-plan og nationalt plan sat fokus på IKT-risiko i et forsøg på at øge den digitale modstandsdygtighed, fastsætte standarder og koordinere det regulerings- og tilsynsmæssige arbejde. På internationalt plan sigter Baselkomitéen for Banktilsyn, Udvalget om Betalings- og Markedsinfrastrukturer, Rådet for Finansiel Stabilitet, the Financial Stability Institute samt G7 og G20 mod at udstyre kompetente myndigheder og markedsoperatører på tværs af forskellige jurisdiktioner med værktøjer, der skal styrke deres finansielle systemers modstandsdygtighed. Dette ***arbejde har også været drevet af behovet for at tage behørigt hensyn til IKT-risiko i forbindelse med et stærkt indbyrdes forbundet globalt finansielt system og for at tilstræbe større sammenhæng i relevant bedste praksis.***

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

(6) I Kommissionens meddelelse af 8. marts 2018 med titlen "Fintechhandlingsplan for en mere konkurrencedygtig og innovativ finanssektor i Europa" fremhævedes den afgørende betydning af at gøre Unionens finansielle sektor mere modstandsdygtig, herunder set fra et operationelt perspektiv, for at sikre dens teknologiske sikkerhed, og at den fungerer godt, at den hurtigt kan genoprettes efter IKT-overtrædelser og -hændelser, hvilket i sidste ende gør det muligt at udbyde finansielle tjenesteydelser på en effektiv og gnidningsfri måde i hele Unionen, herunder i situationer med stresspåvirkning, samtidig med at forbrugernes og markedets tiltro og tillid bevares.

(7) I april 2019 udsendte ***Den Europæiske Tilsynsmyndighed (****Den Europæiske Banktilsynsmyndighed) (EBA****), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010*** [8]***,*** *Den Europæiske* ***Tilsynsmyndighed (Den Europæiske*** *Tilsynsmyndighed for* ***Forsikrings- og Arbejdsmarkedspensionsordninger,*** *EIOPA),* ***der er oprettet ved*** *Europa-Parlamentets og Rådets* ***forordning (EU) nr. 1094/2010*** [9]*,* og ***Den Europæiske Tilsynsmyndighed*** *(Den Europæiske Værdipapir- og Markedstilsynsmyndighed) (ESMA****), der er oprettet ved*** *Europa-Parlamentets og Rådets* ***forordning (EU) nr. 1095/2010*** [10]***, (samlet betegnet som*** "europæiske tilsynsmyndigheder" eller "ESA'er") i fællesskab teknisk rådgivning, hvori de opfordrede til en sammenhængende tilgang til IKT-risiko inden for finansiering 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 Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

9 Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48).

10 Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84).

(8) Unionens finansielle sektor er reguleret af et fælles regelsæt og underlagt et europæisk finanstilsynssystem. Ikke desto mindre er bestemmelserne om håndtering af digital operationel modstandsdygtighed og IKT-sikkerhed endnu ikke harmoniseret fuldt ud eller konsekvent, og det til trods for, at digital operationel modstandsdygtighed er afgørende 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 digital operationel modstandsdygtighed ved at ***styrke*** mandatet for ***de kompetente myndigheder, så de får mulighed for at føre tilsyn med IKT-risikostyring i*** den finansielle sektor ***med henblik på at*** beskytte ***det indre markeds integritet og effektivitet og for at fremme, at det fungerer efter sin hensigt***.

(9) Lovgivningsmæssige forskelle og uensartede nationale regulerings- eller tilsynsmæssige tilgange med hensyn til IKT-risiko udløser hindringer for et velfungerende indre marked for finansielle tjenesteydelser, som hæmmer en problemfri udøvelse af den frie etableringsret og af retten til fri udveksling af tjenesteydelser for finansielle enheder, som har aktiviteter på et grænseoverskridende grundlag. Konkurrencen mellem samme type af finansielle enheder, som har aktiviteter i forskellige medlemsstater, kan også blive fordrejet. Dette gælder navnlig for områder, hvor EU-harmonisering har været meget begrænset, såsom test af digital operationel modstandsdygtighed, eller ikkeeksisterende, såsom overvågning af IKT-tredjepartsrisici. Forskelle, der skyldes en påtænkt udvikling på nationalt plan, vil kunne udløse yderligere hindringer for et velfungerende indre marked til skade for markedsdeltagere og den finansielle stabilitet.

(10) Da bestemmelser vedrørende IKT-risiko kun delvis er blevet behandlet på EU-plan, er der på nuværende tidspunkt huller eller overlapninger på vigtige områder, f.eks. indberetning af IKT-relaterede hændelser og test af digital operationel modstandsdygtighed og uoverensstemmelser som følge 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 udbyder sine tjenesteydelser på et bredt grænseoverskridende grundlag inden for og uden for Unionen. Individuelle finansielle enheder, som har aktiviteter på et grænseoverskridende grundlag, eller som er indehavere af flere tilladelser (f.eks. kan én finansiel enhed have tilladelser til henholdsvis at udøve bankvirksomhed, udøve virksomhed som investeringsselskab og betalingsinstitut, som hver især er meddelt af en forskellig kompetent myndighed i en eller flere medlemsstater), står over for operationelle udfordringer i forbindelse med at imødegå IKT-risiko og afbøde negative virkninger af IKT-hændelser på egen hånd og på en sammenhængende omkostningseffektiv måde.

(11) Da det fælles regelsæt ikke er blevet ledsaget af en omfattende IKT-ramme eller ramme for operationel risiko, er der behov for yderligere harmonisering af centrale krav til digital operationel modstandsdygtighed for alle finansielle enheder. De ***IKT-***kapaciteter og den samlede modstandsdygtighed, som finansielle enheder med udgangspunkt i disse centrale krav skal udvikle for at modstå operationelle driftstop, vil bidrage til at bevare stabiliteten og integriteten på Unionens finansielle markeder og dermed bidrage til at sikre et højt beskyttelsesniveau for investorer og forbrugere i Unionen. Da denne forordning har til formål at bidrage til et velfungerende indre marked, bør den bygge på bestemmelserne i artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) som fortolket i overensstemmelse med EU-Domstolens (Domstolens) faste praksis.

(12) Denne forordning har til formål at konsolidere og opgradere kravene til IKT-risiko ***som en del af kravene til operationel*** risiko, som hidtil er blevet behandlet separat i forskellige EU-retsakter. Disse retsakter omfattede hovedkategorierne af finansiel risiko (f.eks. kreditrisiko, markedsrisiko, modpartskreditrisiko og likviditetsrisiko, risiko forbundet med markedsadfærd), men på tidspunktet for deres vedtagelse tacklede de ikke alle de komponenter, der indgår i operationel modstandsdygtighed, på fyldestgørende vis. I reglerne om operationel risiko blev der, da de blev yderligere udviklet i de pågældende EU-retsakter, ofte foretrukket en traditionel kvantitativ tilgang til risikohåndtering (dvs. ved at fastsætte et kapitalkrav til at dække IKT-risiko) frem for målrettede kvalitative regler for beskyttelses-, detektions-, inddæmnings-, genopretnings- og reparationskapaciteter som værn mod IKT-relaterede hændelser eller for indberetningskapaciteter og digitale testkapaciteter. Disse retsakter skulle primært omfatte og ajourføre væsentlige regler om tilsyn, markedsintegritet eller -adfærd.

Ved at konsolidere og opgradere de forskellige regler om IKT-risici bør alle bestemmelser om digital risiko i den finansielle sektor for første gang blive samlet på en konsekvent måde i én enkelt lovgivningsmæssig retsakt. Denne ***forordning*** udfylder derfor hullerne eller afhjælper uoverensstemmelserne i nogle af de nævnte tidligere retsakter, herunder med hensyn til den heri anvendte terminologi, og henviser eksplicit til IKT-risiko gennem målrettede regler om kapaciteter til IKT-risikostyring, indberetning ***af hændelser***, test af ***operationel modstandsdygtighed,*** samt overvågning af IKT-tredjepartsrisiko. ***Denne forordning bør således også øge bevidstheden om IKT-risiko og anerkende, at IKT-hændelser og manglende operationel modstandsdygtighed potentielt kan udgøre en fare for finansielle enheders soliditet.***

(13) Finansielle enheder bør følge samme tilgang og samme principbaserede regler ved behandling af IKT-risiko ***under hensyntagen til deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer.*** Konsekvens bidrager til at øge tilliden til det finansielle system og bevare dets stabilitet, navnlig i tider med ***høj afhængighed*** af IKT-systemer, platforme og infrastrukturer, hvilket medfører øgede digitale risici. Overholdelse af en grundlæggende cyberhygiejne bør også hindre, at økonomien påføres store omkostninger ved at minimere virkningerne af og omkostningerne i forbindelse med IKT-forstyrrelser.

(14) En forordning hjælper med at mindske reguleringsmæssig kompleksitet, fremmer tilsynsmæssig konvergens og øger retssikkerheden og bidrager også til at begrænse overholdelsesomkostningerne, navnlig for finansielle enheder, der har aktiviteter på tværs af grænserne, og til at mindske konkurrenceforvridninger. Valget af en forordning med henblik på oprettelse af en fælles ramme for digital operationel modstandsdygtighed i finansielle enheder er derfor den mest hensigtsmæssige metode til at sikre en homogen og sammenhængende anvendelse af alle de komponenter, der indgår i IKT-risikostyring i Unionens finansielle sektor.

(15) ▌Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[11] ***var*** den ***første horisontale*** ramme for cybersikkerhed, ***der blev vedtaget*** på EU-plan, ***som også finder anvendelse*** på tre typer af finansielle enheder, nemlig kreditinstitutter, markedspladser og centrale modparter. Eftersom direktiv (EU) 2016/1148 ***fastsatte*** en mekanisme til identifikation på nationalt plan af operatører af væsentlige tjenester, var det imidlertid kun visse kreditinstitutter, markedspladser og centrale modparter, der blev udpeget af medlemsstaterne, ***og som*** blev medtaget under dets anvendelsesområde i praksis, og som derfor skal overholde de heri fastsatte krav til IKT-risici og indberetning af hændelser. Europa-Parlamentets og Rådets direktiv (EU) .../...[12+] ***fastsætter et ensartet kriterium til bestemmelse af de enheder, der er omfattet af dets anvendelsesområde (størrelsesloftet), samtidig med at anvendelsesområdet stadig omfatter de tre typer finansielle enheder.***

---

11 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).

12 Europa-Parlamentets og Rådets direktiv (EU) .../... af... om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktiv) (EUT L ... af ... , s. ...).

+ EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)) samt nummeret, vedtagelsesdatoen og henvisningen til offentliggørelsen af nævnte direktiv i den tilhørende fodnote.

(16) Da denne forordning øger niveauet af harmonisering af de forskellige komponenter, der indgår i digital modstandsdygtighed, ved at indføre krav til IKT-risikostyring og indberetning af IKT-relaterede hændelser, som er strengere i forhold til de krav, der er fastlagt i den nuværende EU-ret om finansielle tjenesteydelser, udgør dette højere ***niveau imidlertid*** ligeledes en øget harmonisering i sammenligning med de krav, der er fastlagt i direktiv (EU) …/…[+]. Derfor udgør denne forordning lex specialis i forhold til direktiv (EU) …/…[+]**.** Det er ***samtidig*** yderst vigtigt at bevare en tæt forbindelse mellem cybersikkerhedsrammen for den finansielle sektor og Unionens horisontale ramme for cybersikkerhed, ***som i øjeblikket fastsat i direktiv (EU) …/…[+], for at*** sikre sammenhæng med de strategier om cybersikkerhed, som medlemsstaterne ▌har vedtaget, ▌, og ***for at*** give de finansielle tilsynsmyndigheder mulighed for at få kendskab til cyberhændelser, der har virkninger for de øvrige sektorer, som er omfattet af nævnte direktiv.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(17) I overensstemmelse med artikel 4, st. 2, i traktaten om Den Europæiske Union og med forbehold af Domstolens prøvelse bør denne forordning ikke berøre medlemsstaternes ansvar for så vidt angår centrale statslige funktioner vedrørende offentlig sikkerhed, forsvar og beskyttelse af den nationale sikkerhed f.eks. i forbindelse med forelæggelse af oplysninger, der ville være i strid med beskyttelsen af den nationale sikkerhed.

(18) For at muliggøre tværsektoriel læring og for effektivt at udnytte andre sektorers erfaringer med håndtering af cybertrusler bør de finansielle enheder, der er omhandlet i direktiv (EU) .../...[+] , fortsat indgå i nævnte direktivs "økosystem" (f.eks. samarbejdsgruppen og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)). ESA'er og nationale kompetente myndigheder bør have mulighed for at deltage i de strategiske politiske drøftelser og det tekniske arbejde i samarbejdsgruppen i henhold til nævnte direktiv og for at ***udveksle*** oplysninger og samarbejde yderligere med de centrale kontaktpunkter, der er udpeget eller oprettet i overensstemmelse med nævnte ***direktiv***. De kompetente myndigheder i henhold til denne forordning bør også rådføre sig med og samarbejde med CSIRT'erne. ***De kompetente myndigheder bør også kunne anmode om teknisk rådgivning hos de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med henhold til direktiv (EU) …/…[+], og etablere samarbejdsordninger, der har til formål at sikre effektive og hurtigt reagerende koordineringsmekanismer.***

▌

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(19) I betragtning af de stærke indbyrdes forbindelser mellem finansielle enheders digitale modstandsdygtighed og fysiske modstandsdygtighed er det nødvendigt med en sammenhængende tilgang i denne forordning og i Europa-Parlamentets og Rådets direktiv (EU) …/…[13+] til kritiske enheders modstandsdygtighed. Eftersom finansielle enheders fysiske modstandsdygtighed behandles omfattende af forpligtelserne med hensyn til IKT-risikostyring og IKT-indberetning i denne forordning, bør forpligtelserne i kapitel III og IV i direktiv (EU) …/…[++] ikke finde anvendelse på finansielle enheder, der er omfattet af nævnte direktivs anvendelsesområde.

(20) Udbydere af cloudcomputingtjenester er én kategori af digital ***infrastruktur***, som er omfattet af direktiv (EU) …/… [+++]***. Den*** EU-tilsynsramme (tilsynsramme), der fastlægges ved denne forordning, finder anvendelse på alle kritiske tredjepartsudbydere af IKT-tjenester, herunder udbydere af cloudcomputingtjenester, når de udbyder IKT-tjenester til finansielle enheder, ***og*** bør betragtes som et supplement til tilsynet gennemført i henhold til direktiv (EU) …/…[+++]. Derudover bør den tilsynsramme, der fastlægges ved denne forordning, omfatte udbydere af cloudcomputingtjenester i fravær af en horisontal EU-ramme om oprettelse af en digital tilsynsmyndighed.

---

[13] ***Europa-Parlamentets og Rådets direktiv*** (EU) .../... ***af … om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF*** (EUT L ... af ... , s. ...).

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 51/22 (2020/0365(COD)) samt nummeret, vedtagelsesdatoen og henvisningen til offentliggørelsen af nævnte direktiv i den tilhørende fodnote.

[++] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 51/22 (2020/0365(COD)).

[+++] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(21) For at bevare den fulde kontrol med IKT-risiko er det nødvendigt, at finansielle enheder har omfattende kapaciteter, der muliggør en stærk og effektiv IKT-risikostyring, og specifikke mekanismer og politikker med henblik på ***håndtering af alle*** IKT-relaterede ***hændelser og*** indberetning af ***større IKT-relaterede hændelser. På samme måde bør finansielle enheder indføre politikker for*** test af IKT-systemer, -kontroller og -processer samt for håndtering af IKT-tredjepartsrisici. ***Standarden for*** digital operationel modstandsdygtighed for finansielle ***enheder*** bør højnes, samtidig med at der ***også*** skabes mulighed for en forholdsmæssigt afpasset anvendelse af krav til ***visse*** finansielle enheder, ***især mikrovirksomheder, og finansielle enheder, der er omfattet af en forenklet ramme for IKT-risikostyring. For at muliggøre et effektivt tilsyn med arbejdsmarkedsrelaterede pensionskasser, der er forholdsmæssigt og imødekommer behovet for at mindske de administrative byrder for de kompetente myndigheder, bør de relevante nationale tilsynsmæssige rammer med hensyn til sådanne finansielle enheder tage højde for deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, selv hvis de relevante tærskler i artikel 5 i*** Europa-Parlamentets og Rådets ***direktiv (EU) 2016/2341[14] overskrides. Navnlig bør tilsynsaktiviteterne primært fokusere på behovet for at imødegå alvorlige risici i forbindelse med IKT-risikostyring i en bestemt enhed.***

14 Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) aktiviteter og tilsynet hermed (EUT L 354 af 23.12.2016, s. 37).

Kompetente myndigheder bør også fastholde en årvågen, men forholdsmæssig, tilgang til tilsynet med arbejdsmarkedsrelaterede pensionskasser, som i overensstemmelse med artikel 31 i direktiv (EU) 2016/2341 outsourcer en betydelig del af deres centrale forretningsområder såsom kapitalforvaltning, aktuarmæssig beregning, regnskab og dataforvaltning til tjenesteydere.

(22) Tærskler og klassificeringssystemer vedrørende indberetning af IKT-relaterede hændelser varierer væsentligt på nationalt plan. Der kan sandsynligvis opnås enighed gennem ***det*** relevante arbejde, der udføres af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2019/881[15], og samarbejdsgruppen i henhold til direktiv (EU) .../...[+], men der findes stadig, eller der kan opstå divergerende tilgange til fastsættelse af tærskler og anvendelse af klassificeringssystemer for de resterende finansielle enheder. På grund af ***disse forskelle*** er der flere krav, ***som*** de finansielle enheder skal overholde, navnlig når de har aktiviteter på tværs af flere medlemsstater, og når de er del af en finansiel koncern. ***Disse*** forskelle kan desuden potentielt 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-risikoen i tilfælde af storstilede angreb med potentielle systemiske konsekvenser til følge.

---

[15] 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).

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(23) For at mindske den administrative byrde og mulige overlappende indberetningsforpligtelser for visse finansielle enheder bør kravet om indberetning af hændelser i henhold til Europa-Parlamentets og Rådets ***direktiv (EU) 2015/2366*** [16] ***ikke længere finde anvendelse på betalingstjenesteudbydere, der er omfattet af denne forordnings anvendelsesområde. Derfor bør kreditinstitutter, e-pengeinstitutter, betalingsinstitutter og kontooplysningstjenesteudbydere som omhandlet i nævnte direktivs artikel 33, stk. 1, fra datoen for denne forordnings anvendelse i henhold til denne forordning indberette alle de operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som tidligere blev indberettet i henhold til nævnte direktiv, uanset om sådanne hændelser er IKT-relaterede.***

---

16 Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

(24) For at sætte kompetente myndigheder i stand til at opfylde ▌ tilsynsmæssige roller ved at ***opnå*** et fuldstændigt overblik over IKT-relaterede hændelsers karakter, frekvens, betydning og virkninger og for at styrke informationsudvekslingen mellem relevante offentlige myndigheder, herunder retshåndhævende myndigheder og afviklingsmyndigheder, ***bør denne forordning*** fastlægge ***en robust*** ordning for indberetning af IKT-relaterede hændelser, ***hvorved de relevante*** krav ***afhjælper nuværende mangler*** i retten om finansielle ***tjenesteydelser*** ▌ ***og*** fjerne ▌ eksisterende overlapninger og dobbeltbestemmelser for at mindske omkostningerne. Det er ▌ afgørende at harmonisere ordningen for indberetning af IKT-relaterede hændelser ved at kræve, at alle finansielle enheder indberetter til deres kompetente myndigheder ***gennem en enkelt strømlinet ramme som fastsat i denne forordning***. ESA'erne bør desuden tillægges beføjelse til yderligere at præcisere ***relevante elementer vedrørende rammen for*** indberetning af IKT-relaterede hændelser, f.eks. klassificeringssystemer, tidsrammer, datasæt, modeller og gældende tærskler. ***For at sikre fuld overensstemmelse med direktiv (EU) .../...[+] bør de finansielle enheder have mulighed for på frivillig basis at underrette den relevante kompetente myndighed om væsentlige cybertrusler, når de anser cybertruslen for at være relevant for det finansielle system, tjenestebrugere eller kunder.***

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(25) Krav til test af digital operationel modstandsdygtighed er ***blevet*** udviklet i ***visse*** finansielle delsektorer ***og udgør*** rammer, ***der ikke altid er fuldt afstemt***. Dette fører ***potentielt til en*** fordobling af omkostninger for grænseoverskridende finansielle enheder, og ▌gør den gensidige anerkendelse af resultaterne af test af ***digital operationel modstandsdygtighed*** kompleks, ***hvilket igen kan*** fragmentere ▌det indre marked.

(26) Når ***IKT-***test ikke er påkrævet, vil sårbarheder ikke blive detekteret, ***hvilket medfører, at*** en finansiel enhed ***udsættes for en IKT-risiko***, og i sidste ende ***skaber en højere risiko for*** stabiliteten og integriteten i den finansielle sektor▌. Uden en indsats på EU-plan vil test af digital operationel modstandsdygtighed fortsat være ***inkonsekvent og mangle en ordning for*** gensidig anerkendelse af ***IKT-***testresultater på tværs af de forskellige jurisdiktioner. Da det er usandsynligt, at andre finansielle delsektorer vil indgå sådanne ***test***ordninger i et meningsfuldt omfang, vil de desuden gå glip af de potentielle fordele ***ved en testramme med hensyn til*** detektion af ***IKT-***sårbarheder og -risici, og test af forsvarskapaciteter og driftsstabilitet, ***der bidrager til at øge*** tiltroen blandt kunder, leverandører og forretningspartnere. For at afhjælpe ***disse*** overlapninger, forskelle og huller er det nødvendigt at fastlægge regler for en koordineret test***ordning*** og dermed lette den gensidige anerkendelse af avancerede test for finansielle enheder, der opfylder kriterierne i denne forordning.

(27) Finansielle enheders afhængighed af brugen 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 denne afhængighed har løbende udviklet sig gennem de senere år og har drevet omkostningsreduktionen inden for finansiel formidling, muliggjort ekspansion og skalerbarhed af virksomheder i forbindelse med udrulningen af finansielle aktiviteter og stillet en bred vifte af IKT-værktøjer til styring af komplekse interne processer til rådighed.

(28) Den vidtgående anvendelse af IKT-tjenester dokumenteres ved komplekse kontraktlige ordninger, i forbindelse med hvilke finansielle enheder ofte støder på vanskeligheder med at forhandle kontraktvilkår, der er tilpasset til de tilsynsmæssige standarder eller andre forskriftsmæssige krav, som de er omfattet af, eller på anden måde med at håndhæve specifikke rettigheder, f.eks. adgangs- eller revisionsrettigheder, selv hvis sidstnævnte er fastsat i deres kontraktlige ordninger. Mange af disse kontraktlige ordninger indeholder desuden ikke tilstrækkelige garantier for en fuldgyldig overvågning af underentrepriseforhold hvorved den finansielle enhed berøves sin evne til at vurdere de dertil knyttede risici. Dertil kommer, at sådanne kontraktlige ordninger 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.

(29) ***Selv om EU-retten*** vedrørende finansielle tjenesteydelser ***indeholder visse generelle regler om outsourcing***, 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-risiko. Derfor er det nødvendigt at fastsætte visse centrale principper, der skal fungere som rettesnor for finansielle enheders styring af IKT-tredjepartsrisici, ***som er af særlig betydning, når finansielle enheder benytter tredjepartsudbydere af IKT-tjenester til at støtte deres kritiske eller vigtige funktioner. Disse principper bør*** ledsages af et sæt centrale kontraktlige rettigheder i forhold til flere elementer af opfyldelse og opsigelse af kontraktlige ordninger med henblik på at yde visse minimumsgarantier for at styrke finansielle enheders evne til effektivt at overvåge alle IKT-risici, der opstår hos tredjepartstjenesteudbydere. ***Disse principper supplerer den sektorspecifikke ret, der finder anvendelse på outsourcing.***

(30) ***I dag er det tydeligt, at der er en vis*** mangel på homogenitet og konvergens ***i forbindelse med overvågningen af*** IKT-tredjepartsrisiko og afhængighed af IKT-tredjeparter. På trods af ▌ bestræbelser på at ***tackle*** outsourcing såsom EBA's retningslinjer om outsourcing fra 2019 ***og ESMA's retningslinjer for outsourcing til udbydere af cloudtjenester fra 2021***, tages der i EU-retten ikke i tilstrækkelig grad højde for den ***bredere*** problematik, der er forbundet med ***imødegåelse af*** systemisk risiko, som kan udløses af den finansielle sektors eksponering for et begrænset antal kritiske tredjepartsudbydere af IKT-tjenester. Mangl***en på regler*** på EU-plan forværres af manglen på ***nationale regler om*** mandater og værktøjer, ***som giver*** nationale tilsynsmyndigheder ***mulighed*** for at opnå en god forståelse for afhængigheden af IKT-tredjeparter og foretage en tilstrækkelig overvågning af risici, der opstår som følge af koncentrationer af ▌ afhængighed af IKT-tredjeparter.

(31) I betragtning af den potentielle systemiske risi***ko***, som øget anvendelse af outsourcing og koncentration af IKT-tredjepartsafhængighed medfører, og henset til de nationale mekanismers utilstrækkelighed ***med hensyn til at give*** finansielle ***tilsynsmyndigheder tilstrækkelige værktøjer*** til at kvantificere, kvalificere og afhjælpe konsekvenserne af IKT-risiko, der opstår hos kritiske tredjepartsudbydere af IKT-tjenester, er det nødvendigt at fastlægge en passende ***tilsynsramme***, som gør det muligt at foretage løbende overvågning af aktiviteter hos tredjepartsudbydere af IKT-tjenester, som er kritiske tredjepartsudbydere af IKT-tjenester til finansielle enheder, ***samtidig med at det sikres, at fortroligheden og sikkerheden for andre kunder end finansielle enheder bevares. Selv om koncernintern levering af IKT-tjenester indebærer specifikke risici og fordele, bør denne ikke automatisk anses for at være mindre risikofyldt end levering af IKT-tjenester fra udbydere uden for en finansiel koncern, og den bør derfor være omfattet af den samme reguleringsmæssige ramme. Når IKT-tjenester leveres inden for samme finansielle koncern, kan finansielle enheder imidlertid have en højere grad af kontrol med koncerninterne udbydere, hvilket der bør tages hensyn til i den samlede risikovurdering.***

(32) I takt med at IKT-risiko bliver mere ***og mere*** komplekse og sofistikerede, afhænger gode ***foranstaltninger til*** detektion og forebyggelse af ***IKT-risiko*** i høj grad af regelmæssig udveksling mellem finansielle enheder af trussels- og sårbarhedsefterretninger. Informationsudveksling bidrager til ***at skabe*** øget bevidsthed om cybertrusler ***. Dette*** styrker også finansielle enheders ***evne*** til at forhindre cybertrusler i at blive faktiske ***IKT–relaterede*** hændelser og sætter finansielle enheder i stand til ***mere effektivt*** at inddæmme ***virkningen*** af IKT–relaterede hændelser og til at foretage ***hurtigere*** genopretning. I fravær af vejledning på EU-plan synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, især usikkerhed omkring foreneligheden med databeskyttelsesregler, antitrustregler og regler om ansvar.

(33) Dertil kommer, at ***tvivl*** med hensyn til, hvilken type oplysninger ***der*** kan udveksles med en anden markedsdeltager eller med ikketilsynsmyndigheder (f.eks. ENISA, med henblik på analytisk input, eller Europol, med henblik på retshåndhævelse), medfører, at nyttige oplysninger tilbageholdes. Omfanget og kvaliteten af informationsudvekslingen er derfor fortsat begrænset ***og*** fragmenteret, da de relevante udvekslinger mest er lokale (gennem nationale initiativer), og da der på EU-plan ikke findes nogen konsekvente ordninger for informationsudveksling, som er skræddersyet til behovene i et integreret finansielt ***system***. ***Det er derfor vigtigt at styrke disse kommunikationskanaler.***

(34) Finansielle enheder bør ▌ tilskyndes ***til indbyrdes at udveksle oplysninger og efterretninger om cybertrusler og*** til i fællesskab at udnytte deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan til at styrke deres kapaciteter til i tilstrækkeligt omfang at vurdere, overvåge, forsvare sig mod og sætte ind over for ▌ cybertrusler ***ved at deltage i ordninger for informationsudveksling***. Det er derfor 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 den finansielle sektor til at forebygge og i fællesskab sætte ind over for cybertrusler ved hurtigt at begrænse spredningen af IKT-risici og hindre potentiel afsmitning på tværs af de finansielle kanaler. Disse mekanismer bør overholde de gældende regler i Unionens konkurrenceret, der fremgår af Kommissionens meddelelse af 14. januar 2011 med titlen "Retningslinjer for anvendelsen af artikel 101 i traktaten om Den Europæiske Unions funktionsmåde på horisontale samarbejdsaftaler", ▌ og Unionens databeskyttelsesregler, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679[17]. De bør fungere ▌ ***på grundlag af et eller flere af de retsgrundlag, der er fastsat i artikel 6 i nævnte forordning, f.eks.*** i forbindelse med behandling af personoplysninger, som er nødvendig for, at den dataansvarlige eller tredjemand kan forfølge en legitim interesse, jf. nævnte forordnings artikel 6, stk. 1, litra f), ***samt i forbindelse med behandling af personoplysninger, der er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, og som er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. henholdsvis artikel 6, stk. 1, litra c) og e), i nævnte forordning.***

[17] 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).

(35) For at opretholde et højt niveau af digital operationel modstandsdygtighed i hele den finansielle sektor og samtidig holde trit med den teknologiske udvikling bør denne forordning imødegå risici, der hidrører fra alle typer IKT-tjenester. Med henblik herpå bør definitionen af IKT-tjenester i forbindelse med denne forordning forstås bredt og omfatte digitale tjenester og datatjenester, der løbende leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere. Denne definition bør f.eks. omfatte såkaldte "over the top"-tjenester, som falder ind under kategorien elektroniske kommunikationstjenester. Den bør kun udelukke den begrænsede kategori af traditionelle analoge telefonitjenester, der kan betegnes som offentlige telefonnettjenester med omkobling (PSTN), fastnettjenester, traditionel telefoni (POTS) eller fastnettelefontjenester.

(36) Til trods for den brede dækning, der påtænkes i denne forordning, bør der ved anvendelse af reglerne om digital operationel modstandsdygtighed tages hensyn til de væsentlige forskelle mellem finansielle enheder med hensyn til ***deres*** størrelse ***og samlede*** *risiko****profil***. Som et overordnet princip bør de finansielle enheder, når de fordeler ressourcer og kapaciteter til gennemførelsen af rammen for IKT-risikostyring, nøje afveje deres IKT-relaterede behov i forhold til ***deres størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer***, mens de kompetente myndigheder fortsat bør vurdere og gennemgå tilgangen til en sådan fordeling.

(37) Kontooplysningstjenesteudbydere som omhandlet i artikel 33, stk. 1, i direktiv (EU) 2015/2366 er udtrykkeligt omfattet af nærværende forordnings anvendelsesområde under hensyntagen til deres aktiviteters særlige karakter og de dermed forbundne risici. Desuden er e-pengeinstitutter og betalingsinstitutter, der er undtaget i henhold til artikel 9, stk. 1, i Europa-Parlamentets og Rådets direktiv 2009/110/EF [18] og ***artikel 32, stk. 1, i direktiv (EU) 2015/2366, omfattet af nærværende forordnings anvendelsesområde, selv om de ikke er blevet meddelt tilladelse i henhold til direktiv 2009/110/EF til at udstede elektroniske penge, eller de ikke er blevet meddelt tilladelse i henhold til direktiv (EU) 2015/2366 til at udbyde og gennemføre betalingstjenester. Postgirokontorer som omhandlet i artikel 2, stk. 5, nr. 3), i Europa-Parlamentets og Rådets direktiv 2013/36/EU*** [19] ***er imidlertid ikke omfattet af nærværende forordnings anvendelsesområde. Den kompetente myndighed for betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og kontooplysningstjenesteudbydere, jf. artikel 33, stk. 1, i direktiv (EU) 2015/2366, bør være den kompetente myndighed, der er udpeget i henhold til artikel 22 i direktiv (EU) 2015/2366.***

---

18 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).

19 Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

(38) Da større finansielle enheder kan have adgang til flere ressourcer og hurtigt kan afsætte midler til at udvikle forvaltningsstrukturer og indføre forskellige virksomhedsstrategier, er det kun finansielle enheder, der ikke er mikrovirksomheder i denne forordnings forstand, som skal pålægges at indføre mere komplekse forvaltningsordninger. Sådanne enheder er bedre rustet til at indføre særlige ledelsesfunktioner med henblik på tilsynsordninger med tredjepartsudbydere af IKT-tjenester eller til at varetage krisestyring, til at tilrettelægge deres egen IKT-risikostyring efter modellen med tre forsvarslinjer ***eller til at etablere en intern model for risikostyring og kontrol og til at underkaste deres ramme for IKT-risikostyring intern revision.***

(39) ***Nogle finansielle enheder drager fordel af undtagelser eller er underlagt en meget lempelig reguleringsmæssig ramme i henhold til den relevante sektorspecifikke EU-ret. Sådanne finansielle enheder omfatter forvaltere af alternative investeringsfonde som omhandlet i artikel 3, stk. 2, i*** Europa-Parlamentets og Rådets ***direktiv 2011/61/EU[20], forsikrings- og genforsikringsselskaber som omhandlet i artikel 4 i*** Europa-Parlamentets og Rådets ***direktiv 2009/138/EF[21] og arbejdsmarkedsrelaterede pensionskasser, der forvalter pensionsordninger, som tilsammen ikke har mere end 15 medlemmer i alt. I lyset af disse undtagelser ville det ikke være rimeligt at medtage sådanne finansielle enheder i denne forordnings anvendelsesområde. Desuden anerkender denne forordning de særlige forhold, der gør sig gældende for markedsstrukturen for forsikringsformidling, med det resultat, at forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, der kan betegnes som mikrovirksomheder eller som små eller mellemstore virksomheder, ikke bør være omfattet af denne forordning.***

(40) ***Da enheder, der er omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU, er udelukket fra nævnte direktivs anvendelsesområde, bør medlemsstaterne derfor kunne vælge at undtage sådanne enheder, der er beliggende på deres respektive områder, fra denne forordnings anvendelse.***

---

20 Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 af 1.7.2011, s. 1).

21 Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1).

(41) ***For at tilpasse denne forordning til anvendelsesområdet for*** Europa-Parlamentets og Rådets ***direktiv 2014/65/EU[22] bør de fysiske og juridiske personer, der er omhandlet i artikel 2 og 3 i nævnte direktiv, og som må yde investeringsservice uden at skulle indhente tilladelse i henhold til direktiv 2014/65/EU, ligeledes udelukkes fra denne forordnings anvendelsesområde. I henhold til artikel 2 i direktiv 2014/65/EU er enheder, der betragtes som finansielle enheder med henblik på denne forordning, f.eks. værdipapircentraler, institutter for kollektiv investering eller forsikrings- og genforsikringsselskaber, dog også undtaget fra nævnte direktivs anvendelsesområde. Undtagelsen fra denne forordnings anvendelsesområde for de personer og enheder, der er omhandlet i artikel 2 og 3 i nævnte direktiv, bør ikke omfatte disse værdipapircentraler, institutter for kollektiv investering eller forsikrings- og genforsikringsselskaber.***

---

22 Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

(42) I henhold til sektorspecifik EU-ret er nogle finansielle enheder underlagt lempeligere krav eller undtagelser som følge af deres størrelse eller de tjenester, de leverer. Denne kategori af finansielle enheder omfatter små og ikke indbyrdes forbundne investeringsselskaber, små arbejdsmarkedsrelaterede pensionskasser, som den pågældende medlemsstat kan udelukke fra anvendelsesområdet for direktiv (EU) 2016/2341 på de betingelser, der er fastsat i artikel 5 i nævnte direktiv, og som forvalter pensionsordninger, som tilsammen ikke har mere end 100 medlemmer i alt, samt institutter, der er fritaget i henhold til direktiv 2013/36/EU. I overensstemmelse med proportionalitetsprincippet og for at bevare ånden i den sektorspecifikke EU-ret er det derfor også hensigtsmæssigt at underlægge disse finansielle enheder en forenklet ramme for IKT-risikostyring i henhold til denne forordning. Den forholdsmæssige karakter af rammen for IKT-risikostyring, der omfatter disse finansielle enheder, bør ikke ændres af de reguleringsmæssige tekniske standarder, der skal udvikles af ESA'erne. I overensstemmelse med proportionalitetsprincippet er det desuden hensigtsmæssigt også at underlægge betalingsinstitutter som omhandlet i artikel 32, stk. 1, i direktiv (EU) 2015/2366 og e-pengeinstitutter som omhandlet i artikel 9 i direktiv 2009/110/EF, der er undtaget i overensstemmelse med national ret, der gennemfører disse EU-retsakter, en forenklet ramme for IKT-risikostyring i henhold til denne forordning, hvorimod betalingsinstitutter og e-pengeinstitutter, som ikke er blevet undtaget i overensstemmelse med deres respektive nationale ret, der gennemfører sektorspecifik EU-ret, bør overholde den generelle ramme, der er fastsat ved denne forordning.

(43) ***Tilsvarende bør finansielle enheder, der betragtes som mikrovirksomheder eller er underlagt den forenklede ramme for IKT-risikostyring i henhold til denne forordning, ikke være forpligtet til at oprette en overvågningsfunktion for deres ordninger indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester eller at udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation, at overdrage ansvaret for styring af og tilsyn med IKT-risiko til en kontrolfunktion og sikre, at en sådan kontrolfunktion har en passende grad af uafhængighed for at undgå interessekonflikter, mindst én gang om året at dokumentere og gennemgå rammen for IKT-risikostyring, regelmæssigt at underkaste rammen for IKT-risikostyring intern revision,*** at foretage tilbundsgående vurderinger efter større ændringer i ***deres*** net- og informationssysteminfrastrukturer og -processer, regelmæssigt at foretage risikoanalyser af legacy-IKT-systemer, ***at underkaste gennemførelsen af planerne for IKT-indsats og -genopretning uafhængig intern revisionsgennemgang, at have en krisestyringsfunktion, at*** udvide test af driftsstabiliteten samt indsats- og genopretningsplaner til at dække ***overgangs***scenarier mellem den primære IKT-infrastruktur og redundante faciliteter***, efter deres anmodning at indberette et skøn over de samlede årlige omkostninger og tab som følge af større IKT-relaterede hændelser til de kompetente myndigheder, at opretholde redundante IKT-kapaciteter, at informere nationale kompetente myndigheder om gennemførte ændringer efter gennemgange af IKT-relaterede hændelser, løbende at overvåge relevant teknologisk udvikling,***

at etablere et omfattende program for test af digital operationel modstandsdygtighed som en integreret del af den ramme for IKT-risikostyring, der er fastsat i denne forordning, eller at vedtage og regelmæssigt gennemgå en strategi for IKT-tredjepartsrisiko. Desuden bør mikrovirksomheder kun være forpligtet til at vurdere behovet for at opretholde sådanne redundante IKT-kapaciteter på grundlag af deres risikoprofil. Mikrovirksomheder bør drage fordel af en mere fleksibel ordning for så vidt angår programmer for test af digital operationel modstandsdygtighed. Når de skal tage stilling til typen og hyppigheden af de test, der skal foretages, bør de skabe en passende balance mellem målet om at opretholde en høj digital operationel modstandsdygtighed og de tilgængelige ressourcer og deres samlede risikoprofil. Mikrovirksomheder og finansielle enheder, der er underlagt den forenklede ramme for IKT-risikostyring i henhold til denne forordning, bør undtages fra kravet om at foretage avancerede test af IKT-værktøjer, -systemer og -processer baseret på trusselsbaserede penetrationstest (TLPT), da kun finansielle enheder, der opfylder kriterierne i denne forordning, bør pålægges at foretage en sådan test. I lyset af deres begrænsede kapaciteter bør mikrovirksomheder kunne aftale med tredjepartsudbyderen af IKT-tjenester, at den finansielle enheds ret til adgang, inspektion og revision delegeres til en uafhængig tredjepart, der udpeges af tredjepartsudbyderen af IKT-tjenester, forudsat at den pågældende finansielle enhed til enhver tid kan anmode den respektive uafhængige tredjepart om alle relevante oplysninger og garantier vedrørende de resultater, som tredjepartsudbyderen af IKT-tjenester opnår.

(44) Da kun de finansielle enheder, der er udpeget med henblik på avanceret test af digital modstandsdygtighed, bør pålægges at foretage trusselsbaserede penetrationstest, bør de administrative processer og finansielle omkostninger, som gennemførelsen af sådanne test indebærer, afholdes af en lille procentdel af finansielle enheder.

(45) For at sikre fuld tilpasning af og generel konsekvens mellem finansielle enheders virksomhedsstrategier på den ene side og gennemførelse af IKT-risikostyring på den anden side bør de finansielle enheders ledelsesorganer pålægges fortsat at indtage en central og aktiv rolle i styringen og tilpasningen af rammen for IKT-risikostyring og den samlede strategi for digital operationel modstandsdygtighed. Den tilgang, som ledelsesorganer 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 overholde en streng cyberhygiejne på alle niveauer. Ledelsesorganets endelige ansvar for styringen af en finansiel enheds IKT-risiko bør være det overordnede princip i denne omfattende tilgang, der skal udmøntes yderligere i ledelsesorganets fortsatte indsats for at føre kontrol med overvågningen af IKT-risikostyring.

(46) Desuden går ***princippet om*** ledelsesorganets fulde ***og endelige*** ansvar ***for styringen af den finansielle enheds IKT-risiko*** hånd i hånd med ***behovet for at sikre*** et vist niveau af IKT***-relaterede*** investeringer og et samlet budget for den pågældende finansielle enhed, ***der gør det muligt for den finansielle enhed*** at opnå ***et højt niveau af*** digital operationel modstandsdygtighed.

(47) Med inspiration fra relevant ***bedste praksis*** og relevante retningslinjer, henstillinger eller tilgange på internationalt og nationalt plan samt på sektorplan vedrørende styring af cyberrisici fremmer denne forordning et sæt ***principper***, der letter den samlede struktur for IKT-risikostyring. Så længe de hovedkapaciteter, som finansielle enheder indfører, håndterer de forskellige funktioner ***inden for IKT-risikostyring*** (identifikation, beskyttelse og forebyggelse, detektion, indsats og genopretning, læring og udvikling og kommunikation), som er omhandlet i denne forordning, ***bør*** det ***derfor stå*** finansielle enheder frit for at anvende modeller for IKT-risikostyring, som er udformet eller kategoriseret på en anden måde.

(48) For at holde trit med et cybertrusselsbillede i udvikling bør finansielle enheder opretholde opdaterede IKT-systemer, der er pålidelige og egnede til ikke kun at garantere den databehandling, der er nødvendig for deres tjenester, men også for at sikre tilstrækkelig teknologisk modstandsdygtighed, så de i tilstrækkelig grad kan tackle yderligere behandlingsrelaterede behov som følge af stressede markedsforhold eller andre vanskelige situationer.

(49) Effektive planer for driftsstabilitet og genopretningsplaner er nødvendige for, 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 ***i overensstemmelse med deres politikker for sikkerhedskopiering***. En sådan ***genoptagelse*** bør dog på ingen måde bringe net- og informationssystemernes integritet og sikkerhed eller ***tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data*** i fare.

(50) Om end denne forordning giver finansielle enheder mulighed for at fastsætte ***deres*** mål for genopretningstid ***og genopretningspunkt*** på en fleksibel måde og dermed fastsætte sådanne mål under fuld hensyntagen til de relevante funktioners karakter og kritiske betydning og eventuelle specifikke forretningsmæssige behov, bør den ikke desto mindre kræve, at de foretager en vurdering af den potentielle samlede indvirkning på markedseffektiviteten, når sådanne mål fastsættes.

(51) ***Bagmændene bag cyberangreb har tendens til at søge at opnå finansielle gevinster direkte fra kilden og dermed udsætte finansielle enheder for væsentlige konsekvenser.*** For at ***[illegible]*** forhindre, at IKT-systemer mister deres integritet eller bliver utilgængelige***,*** og ***dermed undgå*** brud på datasikkerheden og skade på fysisk IKT-infrastruktur, bør finansielle enheders indberetning af større IKT-relaterede hændelser forbedres ***og strømlines*** væsentligt. Indberetningen af IKT-relaterede hændelser bør harmoniseres ***ved at indføre et krav om, at alle finansielle enheder*** foretager indberetning ***direkte*** til deres ***relevante*** kompetente myndigheder ***[illegible]. Hvis en finansiel enhed er underlagt tilsyn ved mere end én national kompetent myndighed, bør medlemsstaterne udpege en fælles kompetent myndighed som modtager af en sådan indberetning. Kreditinstitutter, der er klassificeret som signifikante i henhold til artikel 6, stk. 4, i Rådets forordning (EU) nr. 1024/2013[23], bør indsende en sådan indberetning til de kompetente nationale myndigheder, som efterfølgende bør fremsende indberetningen til Den Europæiske Centralbank (ECB).***

(52) ***Den direkte*** indberetning bør give finansielle tilsynsmyndigheder mulighed ***for at have øjeblikkelig*** adgang til oplysninger om ***større*** IKT-relaterede hændelser. ***Finansielle*** tilsynsmyndigheder bør ***til gengæld*** videreformidle ***detaljerne om større IKT-relaterede hændelser*** til ***offentlige*** ikkefinansielle ***[illegible]*** myndigheder (***såsom*** kompetente myndigheder og centrale kontaktpunkter ***i henhold til direktiv (EU) .../...***[+], nationale databeskyttelsesmyndigheder og til retshåndhævende myndigheder ved ***større IKT-relaterede*** hændelser af kriminel karakter) ***for at øge sådanne myndigheders kendskab til sådanne hændelser og, for så vidt angår CSIRT'er, for at fremme hurtig bistand, der kan ydes til finansielle enheder, alt efter hvad der er relevant. Medlemsstaterne bør desuden kunne bestemme, at de finansielle enheder selv bør give sådanne oplysninger til offentlige myndigheder uden for området for finansielle tjenesteydelser. Disse informationsstrømme bør give finansielle enheder mulighed for hurtigt at drage fordel af alle relevante tekniske input, rådgivning om afhjælpende foranstaltninger og efterfølgende opfølgning fra sådanne myndigheders side. Oplysningerne om større*** 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

---

23 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).

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

anonymiserede data om ***cyber***trusler og sårbarheder forbundet med en hændelse**,** for at bidrage til det bredere kollektive forsvar.

(53) Selv om alle finansielle enheder ***bør*** pålægges at foretage indberetning af ***hændelser***, ***forventes dette krav*** ikke ***at påvirke*** dem alle på samme måde**.** Relevante væsentlighedstærskler ***samt rapporteringsfrister*** bør ***således*** tilpasses ***behørigt i forbindelse med delegerede retsakter baseret på de reguleringsmæssige tekniske standarder, der skal udvikles af ESA'erne, med henblik på*** kun at dække større IKT-relaterede hændelser. Desuden ***bør der tages hensyn til*** de særlige forhold, der gør sig gældende ***for finansielle enheder, når der fastsættes tidsfrister for indberetningsforpligtelser.***

(54) Denne forordning bør fastsætte et krav om, at kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter indberetter alle operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som tidligere blev indberettet i henhold til direktiv (EU) 2015/2366, uanset hændelsens IKT-karakter.

(55) ***ESA'erne bør have til opgave at vurdere den praktiske mulighed og betingelserne for*** en mulig centralisering af indberetninger af IKT-relaterede hændelser ***på EU-niveau. En sådan centralisering kunne*** bestå 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 ***relevante*** indberetninger, som de nationale kompetente myndigheder har indgivet, og ***dermed*** varetager en koordinatorrolle. ESA'erne bør ▌i samråd med ECB og ***ENISA have til opgave*** at udarbejde en fælles rapport, hvori det undersøges, om det er praktisk muligt at oprette et ▌***fælles*** EU-knudepunkt.

(56) For at opnå ***et højt*** niveau af digital operationel modstandsdygtighed og skabe overensstemmelse med ***både de relevante*** internationale standarder (f.eks. G7 Fundamental Elements for Threat-Led Penetration Testing***) og de rammer, der anvendes i Unionen, f.eks. TIBER-EU***, bør finansielle enheder regelmæssigt teste deres IKT-systemer og medarbejdere ***med IKT-relaterede ansvar*** med hensyn til effektiviteten af deres forebyggelses-, detektions-, indsats- og genopretningskapaciteter for at afsløre og afhjælpe potentielle IKT-sårbarheder. For at ***afspejle*** de forskelle***, der eksisterer*** på tværs af og inden for de ***forskellige*** finansielle delsektorer, ***for så vidt angår*** de finansielle enheders niveau af cybersikkerheds***beredskab*** ▌, bør test omfatte en bred vifte af værktøjer og tiltag, der spænder lige fra vurdering***en*** af grundlæggende krav (f.eks. sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerhed, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest eller end-to-end-test) til mere avancerede test ***ved hjælp af*** ▌ TLPT***. En sådan avanceret test bør kun kræves af*** finansielle enheder, ***der*** set fra et IKT-perspektiv er modne nok til at kunne ***gennemføre*** den på en rimelig måde.

Den test af ***digital*** operationel modstandsdygtighed***, der kræves i henhold til denne forordning,*** bør således være mere krævende for de finansielle enheder, der opfylder kriterierne i denne forordning (f.eks. store, systemiske og IKT-modne kreditinstitutter, børser, værdipapircentraler og centrale modparter) end for andre finansielle enheder. Samtidig bør test af digital operationel modstandsdygtighed ***ved hjælp af TLPT*** – være mere relevant for ***finansielle enheder, der opererer inden for centrale*** delsektorer ***for finansielle tjenesteydelser, og*** som spiller en – systemisk rolle (f.eks. betalinger, bankvirksomhed samt clearing og afvikling), og mindre relevant for andre delsektorer (f.eks. kapitalforvaltere og kreditvurderingsbureauer).

(57) ***Finansielle*** enheder***, der er involveret i grænseoverskridende aktiviteter, og*** som udøver ***den*** frie etableringsret eller retten til fri udveksling af tjenesteydelser i Unionen, bør opfylde et fælles sæt avancerede testkrav (fdvs. – TLPT) i deres hjemland, ***som*** bør inkludere IKT-infrastrukturerne i alle de jurisdiktioner, hvori den grænseoverskridende ***finansielle*** koncern opererer inden for Unionen, hvorved det for ***sådanne*** grænseoverskridende ***finansielle*** koncerners vedkommende gøres muligt kun at pådrage sig ***IKT-relaterede*** testomkostninger i én jurisdiktion.

(58) ***For at trække på den ekspertise, som visse kompetente myndigheder allerede har erhvervet, navnlig med hensyn til gennemførelse af TIBER-EU-rammen, bør denne forordning gøre det muligt for medlemsstater at udpege en fælles offentlig myndighed som ansvarlig i den finansielle sektor på nationalt plan for alle*** TLPT-***spørgsmål eller for kompetente myndigheder, i mangel af en sådan udpegelse, at uddelegere udøvelsen af TLPT-relaterede opgaver til en anden national finansiel kompetent myndighed.***

(59) ***Da denne forordning ikke stiller krav om, at finansielle enheder skal lade alle kritiske eller vigtige funktioner være omfattet af en enkelt trusselsbaseret penetrationstest, bør finansielle enheder frit kunne afgøre, hvilke og hvor mange kritiske eller vigtige funktioner der bør være omfattet af en sådan test.***

(60) ***Samlede test som omhandlet i denne forordning, der indebærer deltagelse af flere finansielle enheder i en*** TLPT, ***og for hvilke en tredjepartsudbyder af IKT-tjenester direkte kan indgå kontraktlige ordninger med en ekstern tester, bør kun tillades, hvis kvaliteten eller sikkerheden af de tjenester, som tredjepartsudbyderen af IKT-tjenester leverer til kunder, der er enheder, som falder uden for denne forordnings anvendelsesområde, eller fortroligheden af data forbundet med sådanne tjenester, med rimelighed kan forventes at blive negativt påvirket. Samlede test bør også være omfattet af garantier (ledelse af én udpeget finansiel enhed, kalibrering af antallet af deltagende finansielle enheder) for at sikre en streng testøvelse for de involverede finansielle enheder, som opfylder målene for TLPT i henhold til denne forordning.***

(61) For at udnytte de interne ressourcer, der er til rådighed på virksomhedsniveau, bør denne forordning gøre det muligt at anvende interne testere med henblik på at foretage TLPT under forudsætning af tilsynsmæssig godkendelse, fravær af interessekonflikter og af regelmæssige skift af anvendelsen af interne og eksterne testere (hver tredje test), samtidig med at det også kræves, at formidleren af trusselsefterretninger i TLPT'en altid skal være ekstern i forhold til den finansielle enhed. Ansvaret for at gennemføre TLPT bør forblive fuldt ud hos den finansielle enhed. Erklæringer fra myndigheder bør udelukkende have til formål at opnå gensidig anerkendelse og bør ikke udelukke eventuelle opfølgende foranstaltninger, der er nødvendige for at imødegå den IKT-risiko, som den finansielle enhed er udsat for, og de bør heller ikke betragtes som en tilsynsmæssig godkendelse af en finansiel enheds kapacitet til IKT-risikostyring og -risikoafbødning.

(62) For at sikre en forsvarlig overvågning af IKT-tredjepartsrisiko ***i den finansielle sektor*** er det nødvendigt at fastlægge en række principbaserede regler, der skal fungere som rettesnor for finansielle enheder, ***når*** de overvåger [...] risici i forbindelse med ***funktioner***, der outsources [...] til tredjepartsudbydere af IKT-***tjenester, navnlig for IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og*** mere generelt [...] i [...] forbindelse med afhængighed af ***alle*** IKT-tredjeparter.

(63) For at tage højde for kompleksiteten af de forskellige kilder til IKT-risiko og samtidig tage hensyn til de mange forskellige udbydere af teknologiske løsninger, der muliggør en gnidningsløs levering af finansielle tjenesteydelser, bør denne forordning omfatte en bred vifte af tredjepartsudbydere af IKT-tjenester, herunder udbydere af cloudcomputingtjenester, software, dataanalysetjenester og udbydere af datacentertjenester. Da finansielle enheder på effektiv og sammenhængende vis bør identificere og styre alle typer risici, herunder i forbindelse med IKT-tjenester indkøbt inden for en finansiel koncern, bør det ligeledes præciseres, at virksomheder, der er en del af en finansiel koncern og hovedsagelig leverer IKT-tjenester til deres modervirksomhed eller til dattervirksomheder eller filialer af deres modervirksomhed, samt finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder, også bør betragtes som tredjepartsudbydere af IKT-tjenester i henhold til denne forordning. Endelig, i lyset af udviklingen på betalingstjenestemarkedet, der bliver stadig mere afhængigt af komplekse tekniske løsninger, og i betragtning af nye typer betalingstjenester og betalingsrelaterede løsninger, bør deltagere i økosystemet for betalingstjenester, der leverer betalingsbehandlingsaktiviteter eller driver betalingsinfrastrukturer, også betragtes som tredjepartsudbydere af IKT-tjenester i henhold til denne forordning, bortset fra centralbanker, når de driver betalings- eller værdipapirafviklingssystemer, og offentlige myndigheder, når de leverer IKT-relaterede tjenester i forbindelse med udførelsen af statslige funktioner.

(64) En finansiel enhed bør til enhver tid ***fortsat være*** fuldt ansvarlig for opfyldelsen af ***sine*** forpligtelser i henhold til denne forordning. ***Finansielle enheder bør anvende en*** forholdsmæssigt afpasset ***tilgang til*** overvågning***en*** af de ***risici***, som opstår hos tredjeparts***udbydere*** af IKT-tjenester, under behørig hensyntagen til ***karakteren,*** omfanget, kompleksiteten og betydningen af ***deres*** 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.

(65) Udførelsen af en sådan overvågning bør følge en strategisk tilgang til IKT-tredjepartsrisiko, der formaliseres ved, at den finansielle enheds ledelsesorgan vedtager en særlig strategi for ***IKT-tredjepartsrisiko***, som tager udgangspunkt i en løbende screening af enhver afhængighed af IKT-tredjeparter. For at øge den tilsynsmæssige bevidsthed om afhængighed af IKT-tredjeparter og med henblik på yderligere at understøtte ***arbejdet i forbindelse med*** den tilsynsramme, der oprettes ved denne forordning, bør ***alle*** finansielle ***enheder forpligtes til at opretholde et register over oplysninger med alle kontraktlige ordninger om brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester. Finansielle*** tilsynsmyndigheder bør have mulighed for at anmode om ***det fulde register eller anmode om specifikke afsnit heraf og dermed indhente væsentlige oplysninger med henblik på at opnå en bredere forståelse af finansielle enheders IKT-afhængighed***.

(66) En grundig analyse forud for kontraktindgåelsen bør understøtte og gå forud for den formelle indgåelse af kontraktlige ordninger, ***navnlig ved at fokusere på elementer såsom den kritiske karakter eller betydningen af de tjenester, der understøttes af den påtænkte IKT-kontrakt, de nødvendige tilsynsmæssige godkendelser eller andre betingelser, den mulige koncentrationsrisiko, der er forbundet hermed, samt anvendelse af due diligence i processen med udvælgelse og vurdering af tredjepartsudbydere af IKT-tjenester og vurdering af potentielle interessekonflikter. I forbindelse med kontraktlige ordninger vedrørende kritiske eller vigtige funktioner bør finansielle enheder tage hensyn til tredjepartsudbydere af IKT-tjenesters brug af de seneste og højeste informationssikkerhedsstandarder. Opsigelse*** af kontraktlige ordninger ***kan*** som minimum ▌– være foranlediget ***af*** en ***række*** omstændigheder, der ***påviser*** mangler hos tredjepartsudbyderen af IKT-tjenester***, navnlig væsentlige overtrædelser af love eller kontraktvilkår, omstændigheder, der afslører en potentiel ændring i udførelsen af de funktioner, der er fastsat i de*** kontraktlige ordninger***, tegn på svagheder hos tredjepartsudbyderen af IKT-tjenester i dens samlede IKT-risikostyring eller omstændigheder, der tyder på, at den relevante kompetente myndighed ikke er i stand til at føre effektivt tilsyn med den finansielle enhed***.

(67) For at tackle de systemiske virkninger af den koncentrationsrisiko, der er forbundet med IKT-tredjeparter, ***fremmer denne forordning*** en afbalanceret løsning ***ved at anlægge*** en fleksibel og gradvis tilgang ***til en sådan koncentrationsrisiko***, da ***indførelsen af*** ufleksible lofter eller strenge begrænsninger kan hindre ***udøvelsen af*** virksomhed ***–*** og ***begrænse*** kontraktfriheden. Finansielle enheder bør foretage en grundig vurdering af ***deres påtænkte*** kontraktlige ordninger for at identificere sandsynligheden for, at sådanne risici opstår, herunder ved hjælp af tilbundsgående analyser af ***underentreprise***ordninger, navnlig når de er indgået med tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland. På nuværende tidspunkt og med henblik på at finde en rimelig balance mellem nødvendigheden af at bevare kontraktfriheden og af at sikre den finansielle stabilitet anses det ikke for hensigtsmæssigt at fastsætte regler om strenge lofter og begrænsninger for eksponeringen for IKT-tredjeparter. ***I forbindelse med tilsynsrammen bør en ledende tilsynsførende, der er udpeget i henhold til denne forordning, for så vidt angår*** kritiske tredjeparts***udbydere*** af IKT-***tjenester*** være særligt opmærksom på at opnå fuld forståelse for omfanget af den indbyrdes afhængighed ***–***, identificere specifikke tilfælde, hvor en høj koncentrationsgrad af kritiske tredjepartsudbydere af IKT-tjenester i Unionen sandsynligvis vil lægge pres på stabiliteten og integriteten i Unionens finansielle system, og ***opretholde*** en dialog med kritiske tredjepartsudbydere af IKT-tjenester, hvor en sådan ***specifik*** risiko er identificeret.

(68) For regelmæssigt at ▌ vurdere og overvåge evnen hos en tredjepartsudbyder af IKT-tjenester til sikkert at levere tjenester til en finansiel enhed, uden at dette har negative virkninger for en finansiel enheds ***digitale operationelle*** modstandsdygtighed, ***bør flere*** centrale kontraktlige elementer med tredjepartsudbydere af IKT-tjenester ***harmoniseres***. ***En sådan harmonisering bør*** omfatte minimums***områder, som er*** afgørende for, at den finansielle enhed kan foretage ***en*** fuld overvågning ***af de risici, der kan opstå fra tredjepartsudbyderen af IKT-tjenester,*** set i lyset af ***en finansiel enheds behov for at sikre*** sin digitale modstandsdygtighed, ***da den er dybt afhængig*** af de ***modtagne*** IKT-***tjenesters*** stabilitet***, funktionalitet, tilgængelighed*** og sikkerhed.

(69) Når finansielle enheder og tredjepartsudbydere af IKT-tjenester genforhandler kontraktlige ordninger ***med henblik på at opnå overensstemmelse med kravene i denne forordning, bør de sikre, at de centrale kontraktbestemmelser som fastsat i denne*** forordning ***er omfattet***.

(70) ***Definitionen af "kritisk eller vigtig funktion" i denne forordning omfatter de "kritiske funktioner" som defineret i artikel 2, stk. 1, nr. 35), i*** Europa-Parlamentets og Rådets ***direktiv 2014/59/EU[24]. Funktioner, der anses for at være kritiske i henhold til direktiv 2014/59/EU, er derfor medtaget i definitionen af kritiske funktioner i henhold til denne forordning.***

---

24 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 forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).

(71) ***Uanset den kritiske karakter eller vigtigheden af den funktion, der understøttes af IKT-tjenesterne, bør kontraktlige*** ordninger navnlig indeholde en specifikation bestående af ***de*** komplette beskrivelser af funktioner og tjenester, af steder, hvor sådanne funktioner leveres, og hvor der ***skal*** behandles data, samt ▌ beskrivelser af serviceniveauet ▌. ***Andre væsentlige elementer for at muliggøre en finansiel enheds overvågning af IKT-tredjepartsrisiko er:*** kontraktlige bestemmelser, der præciserer, hvordan adgangen, tilgængeligheden, integriteten, sikkerheden og beskyttelsen af personoplysninger sikres af tredjepartsudbyderen af IKT-tjenester, ***bestemmelser, der fastsætter de relevante*** garantier for ***at muliggøre*** adgang, ***genopretning*** og returnering ***af data*** i tilfælde af insolvens eller afvikling eller i tilfælde af, at tredjepartsudbyderen af IKT-tjenester afbryder sine forretningsaktiviteter***, samt bestemmelser, der kræver, at tredjepartsudbyderen af IKT-tjenester yder bistand i tilfælde af IKT-hændelser i forbindelse med de leverede tjenester, uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, bestemmelser om forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, samt bestemmelser om opsigelsesrettigheder og dertil knyttede minimumsfrister for opsigelse af de*** kontraktlige ordninger ***i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger***.

(72) ***Ud over sådanne kontraktlige bestemmelser og med henblik på at*** sikre, at finansielle enheder fortsat har fuld kontrol over alle udviklingstendenser på ***tredjepartsniveau***, som risikerer at forringe deres IKT-sikkerhed, bør ***kontrakterne om levering af*** IKT-tjenester, der understøtter ***kritiske eller vigtige funktioner, også indeholde følgende: en fuldstændig beskrivelse af serviceniveauer med præcise kvantitative og kvalitative præstationsmål, således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes; de relevante*** 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 levere ***de respektive IKT-tjenester; et krav til tredjepartsudbyderen af IKT-tjenester om at gennemføre og teste forretningsberedskabsplaner og indføre IKT-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver mulighed for sikker levering af tjenester, og om at deltage og samarbejde fuldt ud i den TLPT, der udføres af den finansielle enhed***.

(73) ***Kontrakter om levering af IKT-tjenester,*** der understøtter ***kritiske eller vigtige funktioner, bør også indeholde bestemmelser, der giver*** den finansielle enhed eller en udpeget tredjepart ***ret*** til adgang, inspektion og revision ***og ret til at tage kopier som*** afgørende instrumenter i de finansielle enheders løbende overvågning af de resultater, som tredjepartsudbyderen af IKT-tjenester opnår, kombineret med tjenesteudbyderens fulde samarbejde i forbindelse med inspektioner. Tilsvarende bør den finansielle enheds kompetente myndighed på grundlag af underretninger have ret til at inspicere og foretage revision af tredjepartsudbyderen af IKT-tjenester, med forbehold af beskyttelsen af fortrolige oplysninger.

(74) ***Sådanne kontraktlige*** ordninger bør ***også indeholde*** særlige exitstrategier ***for*** navnlig ***at muliggøre*** obligatoriske overgangsperioder, i løbet af hvilke tredjepartsudbydere af IKT-tjenester fortsat bør levere de relevante ***tjenester*** med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed***,*** eller ***at*** give sidstnævnte mulighed for effektivt at skifte til ***anvendelsen af*** andre tredjepartsudbydere af IKT-tjenester, eller alternativt at skifte til ***interne*** løsninger, der stemmer overens med den leverede ***IKT-***tjenestes kompleksitet. ***Desuden bør finansielle enheder, der er omfattet af direktiv 2014/59/EU, sikre, at de relevante kontrakter for IKT-tjenester er robuste og kan håndhæves fuldt ud i tilfælde af afvikling af de pågældende finansielle enheder. I overensstemmelse med afviklingsmyndighedernes forventninger bør disse finansielle enheder derfor sikre, at de relevante kontrakter for IKT-tjenester er modstandsdygtige over for afvikling. Så længe disse finansielle enheder fortsat opfylder deres betalingsforpligtelser, bør de bl.a. sikre, at de relevante kontrakter for IKT-tjenester indeholder bestemmelser om, at omstrukturering eller afvikling ikke medfører opsigelse, suspension eller ændring.***

(75) Desuden kan den frivillige anvendelse af de standard***kontraktbestemmelser, der er udviklet af offentlige myndigheder eller EU-institutioner, navnlig anvendelsen af*** kontraktbestemmelser udviklet af Kommissionen for cloudcomputingtjenester, give de finansielle enheder og ▌ tredjepartsudbydere af IKT-tjenester yderligere tryghed ved at øge deres retssikkerhedsniveau med hensyn til anvendelsen af cloudcomputingtjenester i den finansielle sektor, i fuld overensstemmelse med de krav og forventninger, der er fastsat i EU-retten om finansielle tjenesteydelser. Udarbejdelsen af standard***kontraktbestemmelser*** bygger på de foranstaltninger, der allerede var påtænkt i fintechhandlingsplanen fra 2018, ***der*** bekendtgjorde, at Kommissionen har til hensigt at tilskynde til og fremme udarbejdelsen af standardkontraktbestemmelser for finansielle enheders anvendelse af cloudcomputingtjenester og i den forbindelse trække på indsatsen blandt tværsektorielle interessenter på området for cloudcomputingtjenester, som Kommissionen har fremmet gennem inddragelse af den finansielle sektor.

(76) Med henblik på at fremme konvergens og effektivitet i forbindelse med tilsynsmæssige tilgange ***til håndtering af*** IKT-tredjepartsrisiko ***i*** den finansielle sektor ***samt for at*** styrke den digitale operationelle modstandsdygtighed i finansielle enheder, der er afhængige af kritiske tredjepartsudbydere af IKT-tjenester for levering af ***de IKT-tjenester, der understøtter leveringen af finansielle tjenesteydelser***, og dermed bidrage til at bevare stabiliteten i Unionens finansielle system og integriteten i det indre marked for finansielle tjenesteydelser, bør kritiske tredjepartsudbydere af IKT-tjenester være omfattet af en EU-tilsynsramme. ***Selv om oprettelsen af tilsynsrammen er begrundet i merværdien af at træffe foranstaltninger på EU-plan, og i kraft af den iboende rolle og de særlige forhold, der gør sig gældende for brugen af IKT-tjenester i forbindelse med levering af finansielle tjenesteydelser, bør det samtidig erindres, at denne løsning kun forekommer hensigtsmæssig inden for rammerne af denne forordning, der specifikt omhandler digital operationel modstandsdygtighed i den finansielle sektor. En sådan tilsynsramme bør imidlertid ikke betragtes som en ny model for EU-tilsyn inden for finansielle tjenesteydelser og aktiviteter.***

(77) Tilsynsrammen bør kun finde anvendelse på kritiske tredjepartsudbydere af ***IKT***-tjenester. Der bør derfor være en udpegelsesmekanisme for at tage hensyn til omfanget og karakteren af den finansielle sektors afhængighed af sådanne tredjepartsudbydere af IKT-tjenester. Denne mekanisme bør indebære et sæt kvantitative og kvalitative kriterier til fastsættelse af parametre for kritisk karakter som grundlag for medtagelse i tilsyns***rammen. For at sikre nøjagtigheden af denne vurdering og uanset tredjepartsudbyderen af IKT-tjenesters virksomhedsstruktur bør sådanne kriterier, hvis der er tale om en tredjepartsudbyder af IKT-tjenester, der er en del af en større koncern, tage hensyn til hele koncernstrukturen for tredjepartsudbyderen af IKT-tjenester. På den ene side bør kritiske*** tredjepartsudbydere af IKT-tjenester, som ikke automatisk udpeges i medfør af disse kriterier, have mulighed for ▌at deltage ▌i tilsynsrammen ***på frivillig basis***, men på den anden side bør tredjepartsudbydere af IKT-***tjenester***, ***der*** allerede ***er*** omfattet af tilsynsrammer, ***som understøtter udførelsen af*** Det Europæiske System af Centralbankers ***opgaver som*** omhandlet i artikel 127, stk. 2, i TEUF, undtages.

(78) ***Tilsvarende bør finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder, selv om de tilhører kategorien af tredjepartsudbydere af IKT-tjenester i henhold til denne forordning, også undtages fra tilsynsrammen, da de allerede er underlagt tilsynsmekanismer, der er oprettet ved den relevante EU-ret om finansielle tjenesteydelser. Hvor det er relevant, bør de kompetente myndigheder i forbindelse med deres tilsynsaktiviteter tage hensyn til den IKT-risiko, som finansielle enheder, der leverer IKT-tjenester, udgør for finansielle enheder. På grund af de eksisterende risikoovervågningsmekanismer på koncernniveau bør den samme undtagelse ligeledes indføres for tredjepartsudbydere af IKT-tjenester, der hovedsageligt leverer tjenester til enheder i deres egen koncern. Tredjepartsudbydere af IKT-tjenester, der udelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheder, der kun er aktive i den pågældende medlemsstat, bør også undtages fra udpegelsesmekanismen på grund af deres begrænsede aktiviteter og manglende grænseoverskridende virkninger.***

(*79)* ***Den digitale omstilling, der er sket inden for finansielle tjenesteydelser, har medført en hidtil uset grad af anvendelse og afhængighed af IKT-tjenester. Eftersom det er blevet utænkeligt at levere finansielle tjenesteydelser uden brug af cloudcomputingtjenester, softwareløsninger og datarelaterede tjenester, er Unionens finansielle økosystem blevet uløseligt forbundet med visse IKT-tjenester, der leveres af leverandører af IKT-tjenester. Nogle af disse leverandører, som er innovatorer i udviklingen og anvendelsen af IKT-baserede teknologier, spiller en væsentlig rolle i leveringen af finansielle tjenesteydelser eller er blevet integreret i værdikæden for finansielle tjenesteydelser. De er således blevet afgørende for stabiliteten og integriteten af Unionens finansielle system. Denne udbredte afhængighed af tjenester, der leveres af kritiske tredjepartsudbydere af IKT-tjenester, kombineret med den indbyrdes afhængighed mellem forskellige markedsoperatørers informationssystemer skaber en direkte og potentielt alvorlig risiko for Unionens system for finansielle tjenesteydelser og for kontinuiteten i leveringen af finansielle tjenesteydelser, hvis kritiske tredjepartsudbydere af IKT-tjenester påvirkes af operationelle forstyrrelser eller større cyberhændelser.***

Cyberhændelser har en markant evne til at vokse og sprede sig i hele det finansielle system i betydeligt hurtigere tempo end andre typer risici, der overvåges i den finansielle sektor, og kan brede sig over sektorer og geografiske grænser. De har potentiale til at udvikle sig til en systemisk krise, hvor tilliden til det finansielle system udhules på grund af forstyrrelser af funktioner, der understøtter realøkonomien, eller til betydelige finansielle tab, der når et niveau, som det finansielle system ikke kan holde til, eller som kræver anvendelse af omfattende foranstaltninger til at absorbere chok. For at forhindre, at disse scenarier finder sted og derved bringer den finansielle stabilitet og integritet i Unionen i fare, er det afgørende at sikre konvergens i tilsynspraksis vedrørende IKT-tredjepartsrisiko inden for finansiering, navnlig gennem nye regler, der giver Unionen mulighed for at føre tilsyn med kritiske tredjepartsudbydere af IKT-tjenester.

(80) Tilsynsrammen afhænger i høj grad af graden af samarbejde mellem den ledende tilsynsførende og den kritiske tredjepartsudbyder af IKT-tjenester, der til finansielle enheder leverer tjenester, som påvirker leveringen af finansielle tjenesteydelser. Et vellykket tilsyn er bl.a. baseret på den ledende tilsynsførendes evne til effektivt at gennemføre overvågningsmissioner og inspektioner for at vurdere de regler, kontroller og processer, der anvendes af de kritiske tredjepartsudbydere af IKT-tjenester, samt for at vurdere deres aktiviteters potentielle kumulative indvirkning på den finansielle stabilitet og det finansielle systems integritet. Samtidig er det afgørende, at kritiske tredjepartsudbydere af IKT-tjenester følger den ledende tilsynsførendes henstillinger og imødekommer dennes betænkeligheder. Eftersom manglende samarbejde fra en kritisk tredjepartsudbyder af IKT-tjenester, der leverer tjenester, som påvirker leveringen af finansielle tjenesteydelser, f.eks. afslag på at give adgang til sine lokaler eller indgive oplysninger, i sidste ende vil fratage den ledende tilsynsførende sine afgørende værktøjer for at vurdere IKT-tredjepartsrisiko og kan have en negativ indvirkning på den finansielle stabilitet og det finansielle systems integritet, er det nødvendigt også at indføre en passende sanktionsordning.

(81) På denne baggrund bør det sikres, at den ledende tilsynsførendes behov for at kunne pålægge tvangsbøder for at tvinge kritiske tredjepartsudbydere af IKT-tjenester til at efterleve de gennemsigtigheds- og adgangsrelaterede forpligtelser, der er fastsat i denne forordning, ikke bringes i fare på grund af de vanskeligheder, som håndhævelsen af disse tvangsbøder giver anledning til over for kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i tredjelande. For at sikre, at sådanne sanktioner kan håndhæves, og for at muliggøre en hurtig indførelse af procedurer, der opretholder de kritiske tredjepartsudbydere af IKT-tjenesters ret til forsvar i forbindelse med udpegelsesmekanismen og udstedelsen af henstillinger, bør disse kritiske tredjepartsudbydere af IKT-tjenester, der leverer tjenester til finansielle enheder, som påvirker leveringen af finansielle tjenesteydelser, være forpligtet til at opretholde en passende forretningsmæssig tilstedeværelse i Unionen. På grund af tilsynets karakter og manglen på sammenlignelige ordninger i andre jurisdiktioner er der ingen egnede alternative mekanismer til at nå dette mål gennem et effektivt samarbejde med finansielle tilsynsmyndigheder i tredjelande om overvågning af virkningen af de digitale operationelle risici hidrørende fra de systemiske tredjepartsudbydere af IKT-tjenester, som betragtes som kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i tredjelande.

For at fortsætte leveringen af IKT-tjenester til finansielle enheder i Unionen bør en tredjepartsudbyder af IKT-tjenester med hjemsted i tredjelande, der er udpeget som kritisk i overensstemmelse med denne forordning, derfor senest 12 måneder efter udpegelsen træffe alle nødvendige foranstaltninger for at sikre sin registrering som selskab i Unionen ved at oprette en dattervirksomhed som defineret i gældende EU-ret, nemlig i Europa-Parlamentets og Rådets direktiv 2013/34/EU[25].

(82) Kravet om at oprette en dattervirksomhed i Unionen bør ikke forhindre den kritiske tredjepartsudbyder af IKT-tjenester i at levere IKT-tjenester og dertil knyttet teknisk support fra faciliteter og infrastruktur beliggende uden for Unionen. Denne forordning pålægger ikke en datalokaliseringsforpligtelse, da den ikke kræver, at datalagring eller -behandling skal finde sted i Unionen.

---

25 Europa-Parlamentets og Rådets direktiv 2013/34/EU af 26. juni 2013 om årsregnskaber, konsoliderede regnskaber og tilhørende beretninger for visse virksomhedsformer, om ændring af Europa-Parlamentets og Rådets direktiv 2006/43/EF og om ophævelse af Rådets direktiv 78/660/EØF og 83/349/EØF (EUT L 182 af 29.6.2013, s. 19).

(83) Kritiske tredjepartsudbydere af IKT-tjenester bør kunne levere IKT-tjenester fra et hvilket som helst sted i verden og derfor ikke nødvendigvis eller ikke kun fra lokaler beliggende i Unionen. Tilsynsaktiviteter bør først gennemføres på lokaler beliggende i Unionen og ved at interagere med enheder, der er beliggende i Unionen, herunder de dattervirksomheder, der er etableret af kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordning. Sådanne tiltag inden for Unionen kan imidlertid være utilstrækkelige til, at den ledende tilsynsførende fuldt ud og effektivt kan varetage sine opgaver i henhold til denne forordning. Den ledende tilsynsførende bør derfor også kunne udøve sine relevante tilsynsbeføjelser i tredjelande. Udøvelsen af disse beføjelser i tredjelande bør gøre det muligt for den ledende tilsynsførende at undersøge de faciliteter, hvorfra IKT-tjenesterne eller de tekniske supporttjenester faktisk leveres eller forvaltes af den kritiske tredjepartsudbyder af IKT-tjenester, og bør give den ledende tilsynsførende en omfattende og operationel forståelse af IKT-risikostyringen ved den kritiske tredjepartsudbyder af IKT-tjenester.

Den ledende tilsynsførendes mulighed for som et EU-agentur at udøve beføjelser uden for Unionens område bør være behørigt afgrænset af relevante betingelser, navnlig samtykke fra den berørte kritiske tredjepartsudbyder af IKT-tjenester. Tilsvarende bør de relevante myndigheder i tredjelandet underrettes om og ikke have gjort indsigelse mod den ledende tilsynsførendes udøvelse af aktiviteter på deres eget område. For at sikre en effektiv gennemførelse, og uden at det berører EU-institutionernes og medlemsstaternes respektive beføjelser, er det imidlertid også nødvendigt, at sådanne beføjelser er fuldt forankret i indgåelsen af administrative samarbejdsordninger med de relevante myndigheder i det berørte tredjeland. Denne forordning bør derfor give ESA'erne mulighed for at indgå administrative samarbejdsordninger med de relevante myndigheder i tredjelande, som ikke derudover bør skabe retlige forpligtelser for Unionen og dens medlemsstater.

(84) For at lette kommunikationen med den ledende tilsynsførende og sikre passende repræsentation bør kritiske tredjepartsudbydere af IKT-tjenester, som indgår i en koncern, udpege én juridisk person som deres koordinationspunkt.

(85) ***Tilsynsrammen*** bør ikke berøre medlemsstaternes beføjelser til at gennemføre deres egne tilsyns***- eller overvågnings***missioner i forhold til tredjepartsudbydere af IKT-tjenester, som ikke er ***udpeget som*** kritiske i henhold til denne forordning, men ***som*** anses for at være vigtige på nationalt plan.

(86) For at sikre effekten af den ▌institutionelle flerlagsarkitektur på området for finansielle tjenesteydelser bør Det Fælles Udvalg af ESA'er fortsat sikre samlet koordinering på tværs af sektorer af alle forhold, der vedrører IKT-risiko, i overensstemmelse med dets opgaver vedrørende cybersikkerhed. Det bør få støtte fra et nyt underudvalg ("tilsynsforummet▌"), der udfører det forberedende arbejde ▌både ***med henblik på*** individuelle afgørelser rettet mod kritiske tredjepartsudbydere af IKT-tjenester og ***med henblik på udstedelse af*** kollektive henstillinger, navnlig i forbindelse med benchmarking af tilsynsprogrammerne for kritiske tredjepartsudbydere af IKT-tjenester, og fastlæggelse af bedste praksis for håndtering af spørgsmål vedrørende IKT-koncentrationsrisiko.

(87) For at sikre et ***passende og effektivt*** tilsyn på EU-plan med ***kritiske*** tredjepartsudbydere af IKT-tjenester, ***fastsættes det i denne forordning, at enhver af de tre ESA'er kan*** udpeges som ***en*** ledende tilsynsførende ***. Den individuelle tildeling af en*** kritisk tredjepartsudbyder af IKT-tjenester ***til en af de tre ESA'er bør være resultatet af en vurdering af, hvilke finansielle enheder der overvejende opererer i de finansielle sektorer, som den pågældende ESA har ansvaret for. Denne tilgang bør føre til en afbalanceret fordeling af opgaver og ansvarsområder mellem de tre ESA'er i forbindelse med udøvelsen af tilsynsfunktionerne og bør gøre bedst mulig brug af de menneskelige ressourcer og den tekniske ekspertise, der er til rådighed i hver af de tre ESA'er***.

(88) Ledende tilsynsførende bør ***tildeles*** de nødvendige beføjelser til at foretage undersøgelser, ***gennemføre*** inspektioner på stedet og eksterne inspektioner i lokaler og på steder hos kritiske tredjepartsudbydere af IKT-tjenesters og indhente fuldstændige og ajourførte oplysninger . ***Disse beføjelser bør*** sætte ***den ledende tilsynsførende*** i stand til at opnå en reel indsigt i typen, omfanget og virkningerne af den IKT-tredjepartsrisiko, der berører finansielle enheder og i sidste ende Unionens finansielle system.

Overdragelse af hovedansvaret for tilsyn***srollen*** til ESA'erne udgør en forudsætning for at forstå og håndtere den systemiske dimension af IKT-risiko inden for finansiering. Den indvirkning, som kritiske tredjepartsudbydere af IKT-tjenester har på Unionens finansielle sektor, og de potentielle problematikker, der skyldes den ***deraf følgende*** IKT-koncentrationsrisiko ▌, kræver en kollektiv tilgang på EU-plan. ***Samtidig gennemførelse*** af flere revisioner og adgangsrettigheder, der ***udføres separat*** af en lang række kompetente myndigheder ▌ med begrænset eller ingen indbyrdes koordinering, vil ▌ ***forhindre de finansielle tilsynsmyndigheder i at få*** et fuldstændigt ***og omfattende*** overblik over IKT-tredjepartsrisiko ***i Unionen,*** samtidig med at der ***også*** skabes ▌ redundans, byrder og kompleksitet ***for*** kritiske tredjepartsudbydere af IKT-***tjenester***, ***hvis de er genstand for*** mange ***overvågnings- og inspektions***anmodninger.

(89) ***Da udpegelsen som kritisk har en betydelig indvirkning, bør denne forordning sikre, at rettighederne for kritiske tredjepartsudbydere af IKT-tjenester overholdes i hele gennemførelsen af tilsynsrammen. Inden sådanne udbydere udpeges som kritiske, bør de f.eks. have ret til at indgive en begrundet erklæring til den ledende tilsynsførende med alle relevante oplysninger med henblik på vurderingen i forbindelse med deres udpegelse. Eftersom den*** ledende ***tilsynsførende*** bør ***have beføjelse*** til at fremsætte henstillinger vedrørende IKT-risiko og passende afhjælpende foranstaltninger dertil***,*** ***hvilket omfatter beføjelsen til at gøre indsigelse mod*** visse kontraktlige ordninger, som i sidste ende påvirker stabiliteten i den finansielle enhed eller det finansielle system***, bør kritiske tredjepartsudbydere af IKT-tjenester også have mulighed for inden færdiggørelsen af disse henstillinger at fremlægge redegørelser for den forventede virkning af de løsninger, der påtænkes i henstillingen, for kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og for at udarbejde løsninger til at afbøde risici. Kritiske tredjepartsudbydere af IKT-tjenester, der er uenige i henstillingerne, bør indgive en begrundet redegørelse for deres hensigt om ikke at tilslutte sig henstillingen. Hvis en sådan begrundet redegørelse ikke indgives, eller hvis den anses for at være utilstrækkelig, bør den ledende tilsynsførende udsende en offentlig meddelelse, der kort beskriver den manglende overholdelse.***

(90) ***De kompetente myndigheder bør på behørig vis medtage opgaven med at kontrollere*** den indholdsmæssige ***overholdelse af*** henstillinger, som er ***udstedt*** af den ledende ***tilsynsførende, i deres funktioner med hensyn til*** tilsyn med finansielle enheder. ***De kompetente myndigheder bør kunne kræve, at finansielle enheder træffer yderligere foranstaltninger for at imødegå de risici, der er konstateret i den ledende tilsynsførendes henstillinger, og bør i rette tid udstede underretninger herom. Hvis den ledende tilsynsførende retter henstillinger til kritiske tredjepartsudbydere af IKT-tjenester, der er underlagt tilsyn i henhold til direktiv (EU) .../...[+], bør de kompetente myndigheder på frivillig basis og inden vedtagelsen af yderligere foranstaltninger kunne høre de kompetente myndigheder i henhold til nævnte direktiv for at fremme en koordineret tilgang til håndteringen af de pågældende kritiske tredjepartsudbydere af IKT-tjenester.***

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(91) Udøvelsen af tilsynet bør styres af tre operationelle principper, der har til formål at sikre: a) tæt koordinering mellem ESA'erne i deres rolle som ledende tilsynsførende gennem et fælles tilsynsnetværk, b) overensstemmelse med den ramme, der er fastlagt ved direktiv (EU) .../... [+] (gennem en frivillig høring af organer i henhold til nævnte direktiv, for at undgå overlapning af foranstaltninger rettet mod kritiske tredjepartsudbydere af IKT-tjenester), og c) anvendelse af omhu for at minimere den potentielle risiko for forstyrrelser af tjenester, der leveres af kritiske tredjepartsudbydere af IKT-tjenester til kunder, der er enheder, som ikke er omfattet af denne forordnings anvendelsesområde.

(92) Tilsynsrammen ***bør*** ikke erstatte eller på nogen måde eller for nogen dels vedkommende træde i stedet for ***kravet til*** de finansielle enheder om selv ***at forvalte*** de ***risici***, der er forbundet med brugen af tredjepartsudbydere af IKT-tjenester, herunder deres forpligtelse til ***at opretholde en*** løbende overvågning af [redacted] kontraktlige ordninger, der indgås med kritiske tredjepartsudbydere af IKT-tjenester. Ligeledes ***bør*** tilsynsrammen ikke berøre [redacted] finansielle enheders fulde ansvar for at overholde og opfylde alle de retlige forpligtelser***, der er fastsat i*** denne forordning og ***i den*** relevante finansielle tjenesteydelsesret.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(93) For at undgå dobbeltbestemmelser og overlapninger bør de kompetente myndigheder afholde sig fra individuelt at træffe foranstaltninger, der har til formål at overvåge risici hos den kritiske tredjepartsudbyder af IKT-tjenester***, og bør i den forbindelse basere sig på den relevante ledende tilsynsførendes vurdering.*** Alle ▌ foranstaltninger bør ***under alle omstændigheder*** koordineres og vedtages på forhånd ***med den ledende tilsynsførende*** som led i ***udførelsen af opgaver i*** tilsynsrammen.

(94) For at fremme konvergens på internationalt plan vedrørende brug af bedste praksis for gennemgangen ***og overvågningen*** af den digitale risikostyring, der foretages af tredjepartsudbydere af IKT-tjenester, bør ESA'erne opfordres til at indgå samarbejdsordninger med ▌ relevante ▌ tilsyns- og reguleringsmyndigheder i tredjelande.

(95) Med henblik på at udnytte ***de specifikke kompetencer,*** tekniske ***færdigheder og*** ekspertisen blandt ***personale, der er specialiseret i operationel risiko og IKT-risiko hos*** de kompetente myndigheder***, de tre ESA'er og, på frivillig basis, de kompetente myndigheder i henhold til direktiv (EU).../...[+],*** bør ***den*** ledende tilsynsførende trække på national tilsyns***kapacitet og -viden*** og oprette særlige undersøgelsesteams for hver kritisk tredjepartsudbyder af IKT-tjenester, samle tværfaglige teams ***til støtte for*** forberedelsen og udførelsen af tilsynsaktiviteter, herunder ***generelle undersøgelser og*** inspektioner hos kritiske tredjepartsudbydere af IKT-tjenester, samt ***med henblik på enhver*** nødvendig opfølgning heraf.

(96) Om end omkostninger som følge af tilsynsopgaver vil blive fuldt ud finansieret af gebyrer, der opkræves af kritiske tredjepartsudbydere af IKT-tjenester, vil ESA'erne dog sandsynligvis inden starten af tilsynsrammen pådrage sig omkostninger for gennemførelsen af særlige IKT-systemer, der understøtter det kommende tilsyn, eftersom der på forhånd vil skulle udvikles og deployeres særlige IKT-systemer. Denne forordning indeholder derfor bestemmelser om en hybrid finansieringsmodel, hvorved tilsynsrammen som sådan vil blive fuldt ud finansieret af gebyrer, mens udviklingen af ESA'ernes IKT-systemer vil blive finansieret af bidrag fra Unionen og de nationale kompetente myndigheder.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

(97) De kompetente myndigheder bør have alle de ***påkrævede*** tilsyns-, undersøgelses- og sanktionsbeføjelser, således at de kan sikre, at de udfører deres opgaver i henhold til denne forordning korrekt. De bør i princippet offentliggøre meddelelser om de administrative sanktioner, de pålægger. Da finansielle enheder og tredjepartsudbydere af IKT-tjenester kan have hjemsted i forskellige medlemsstater og være underlagt forskellige ▌kompetente myndigheders tilsyn***, bør anvendelsen af denne forordning lettes, dels af et*** tæt samarbejde blandt de relevante kompetente myndigheder, ▌herunder ECB for så vidt angår specifikke opgaver, som den er tillagt ved Rådets forordning (EU) nr. 1024/2013, ***dels af*** høring af ESA'erne ***gennem*** gensidig informationsudveksling og levering af bistand i forbindelse med ***relevante*** tilsynsaktiviteter.

(98) For yderligere at kvantificere og kvalificere ▌ kriterierne for ***udpegelsen af*** tredjepartsudbydere af IKT-tjenester ***som kritiske*** og harmonisere tilsynsgebyrerne bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for at supplere denne forordning ▌ for så vidt angår yderligere præcisering af de systemiske virkninger, som et svigt ***eller et operationelt driftstop*** foretaget af en tredjepartsudbyder af IKT-***tjenester*** kan få for de finansielle enheder, den ***leverer IKT-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 ***givet*** marked, omkostningerne forbundet med at migrere ***data og IKT-arbejdsbyrden til andre*** tredjepartsudbydere af IKT-tjenester ▌ 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[26]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

[26] EUT L 123 af 12.5.2016, s. 1.

(99) ***Reguleringsmæssige tekniske*** standarder bør sikre en konsekvent harmonisering af kravene i denne forordning. ESA'erne bør ***i deres egenskab af*** organer ***med*** højt specialiseret faglig kompetence 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 ***af større IKT-relaterede hændelser***, test ***samt i forbindelse med*** centrale krav med henblik på en forsvarlig overvågning af IKT-tredjepartsrisiko. 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 ***deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer***. Kommissionen bør tillægges beføjelse til at vedtage sådanne reguleringsmæssige tekniske standarder ved hjælp af delegerede retsakter i henhold til artikel 290 i TEUF og i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

(100) For at gøre det lettere at sammenligne indberetninger af større IKT-relaterede ***hændelser og større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser samt*** sikre gennemsigtighed med hensyn til kontraktlige ordninger for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, bør ESA'erne udarbejde udkast til gennemførelsesmæssige tekniske standarder, der fastlægger standardiserede modeller, formularer og procedurer, således at finansielle enheder kan indberette en større IKT-***relateret hændelse og en større operationel eller sikkerhedsmæssig betalings***relateret hændelse, samt standardiserede modeller for registret over oplysninger. Når ESA'erne udarbejder disse standarder, bør de tage hensyn til den finansielle enheds ***størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer***. 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 forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

(101) Da der allerede er fastsat yderligere krav ved delegerede retsakter og gennemførelsesretsakter baseret på de reguleringsmæssige og gennemførelsesmæssige tekniske standarder i Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009[27], (EU) nr. 648/2012[28], (EU) nr. 600/2014[29] og (EU) nr. 909/2014[30], 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.

---

27 Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer (EUT L 302 af 17.11.2009, s. 1).

28 Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

29 Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 84).

30 Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1).

(102) Eftersom denne forordning sammen med Europa-Parlamentets og Rådets direktiv (EU) .../...[31++] for at sikre fuld sammenhæng indebærer en konsolidering af bestemmelserne om IKT-risikostyring – i 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 og Europa-Parlamentets og Rådets forordning (EU) 2016/1011[32], bør nævnte forordninger ændres for at præcisere, at de ***gældende*** IKT-risikorelaterede bestemmelser er fastsat i nærværende forordning.

(103) Derfor bør anvendelsesområdet for de relevante artikler vedrørende operationel risiko, i henhold til hvilke de beføjelser, der er fastsat i forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011, gav mandat til vedtagelsen af delegerede retsakter og gennemførelsesretsakter, indskrænkes med henblik på at overføre alle de bestemmelser om ***aspekterne vedrørende*** digital operationel modstandsdygtighed, som – i dag ***indgår*** i nævnte forordninger, til nærværende forordning.

---

[31] Europa-Parlamentets og Rådets direktiv (EU) .../... af … om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor (EUT L ... af ..., s. ...).

[++] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 42/22 (2020/0268(COD)) samt nummeret, vedtagelsesdatoen og henvisningen til offentliggørelsen af nævnte direktiv i den tilhørende fodnote.

[32] 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).

(104) Den potentielle systemiske cyberrisiko, der er forbundet med anvendelsen af IKT-infrastrukturer, som muliggør drift af betalingssystemer og levering af betalingsbehandlingsaktiviteter, bør håndteres behørigt på EU-plan gennem harmoniserede regler om digital modstandsdygtighed. Kommissionen bør derfor hurtigt vurdere behovet for at gennemgå denne forordnings anvendelsesområde og samtidig tilpasse en sådan gennemgang til resultatet af den omfattende gennemgang, der er omhandlet i direktiv (EU) 2015/2366. Talrige storstilede angreb har det seneste årti vist, hvordan betalingssystemer er blevet eksponeret for cybertrusler. Med en central placering i betalingstjenestekæden og stærke indbyrdes forbindelser til det finansielle system som helhed har betalingssystemer og betalingsbehandlingsaktiviteter fået afgørende betydning for, at Unionens finansielle markeder kan fungere. Cyberangreb på sådanne systemer kan forårsage alvorlige operationelle driftsforstyrrelser med direkte konsekvenser for centrale økonomiske funktioner såsom lettelse af betalinger og indirekte virkninger for dermed forbundne økonomiske processer. Indtil der er indført en harmoniseret ordning og tilsyn med operatører af betalingssystemer og behandlingsenheder på EU-plan, kan medlemsstaterne med henblik på at anvende lignende markedspraksisser lade sig inspirere af de krav til digital operationel modstandsdygtighed, der er fastsat i denne forordning, når de anvender regler på operatører af betalingssystemer og behandlingsenheder, der er underlagt tilsyn i deres egne jurisdiktioner.

(105) ***Målet*** for denne forordning, nemlig at opnå et højt niveau af digital operationel modstandsdygtighed ***for regulerede*** finansielle enheder, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, fordi ***det kræver*** harmonisering af ***flere*** forskellige regler i EU-retten og national ret, men kan på grund af dens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor 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.

(106) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725[33] og afgav en udtalelse den 10. maj 2021[34] —

VEDTAGET DENNE FORORDNING:

[33] Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

[34] EUT C 229 af 15.6.2021, s. 16.

Kapitel I

Almindelige bestemmelser

Artikel 1

Genstand

1. For at opnå et højt fælles niveau af digital operationel modstandsdygtighed fastsætter denne forordning ensartede krav til sikkerheden i de net- og informationssystemer, der understøtter finansielle enheders forretningsprocesser på følgende måde:

a) krav til finansielle enheder vedrørende:

i) risikostyring inden for informations- og kommunikationsteknologi (IKT)

ii) indberetning af større IKT-relaterede hændelser ***og underretning, på frivillig basis, om væsentlige cybertrusler*** til de kompetente myndigheder

iii) ***indberetning af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser til de kompetente myndigheder fra de finansielle enheder, der er omhandlet i artikel 2, stk. 1, litra a)-d)***

iv) test af digital operationel modstandsdygtighed

v) udveksling af oplysninger og efterretninger om cybertrusler og sårbarheder

vi) foranstaltninger til forsvarlig styring af IKT-tredjepartsrisiko

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

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

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

2. For så vidt angår finansielle enheder, der er identificeret som væsentlige eller vigtige enheder i henhold til nationale bestemmelser om gennemførelse af artikel 3 i direktiv (EU) .../...[+], betragtes denne forordning som en sektorspecifik EU-retsakt med henblik på artikel 4 inævnte direktiv.

3. Denne forordning berører ikke medlemsstaternes ansvar for så vidt angår væsentlige statslige funktioner vedrørende offentlig sikkerhed, forsvar og national sikkerhed i overensstemmelse med EU-retten.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

Artikel 2

Anvendelsesområde

1. ***Med forbehold af stk. 3 og 4*** finder ***denne*** forordning anvendelse på følgende enheder:

a) kreditinstitutter

b) betalingsinstitutter***, herunder betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366***

c) kontooplysningstjenesteudbydere

d) e-pengeinstitutter, ***herunder e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF***

e) investeringsselskaber

f) udbydere af kryptoaktivtjenester***, som er meddelt tilladelse i henhold til*** Europa-Parlamentets og Rådets forordning (EU) .../...om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937 ("forordningen om markeder for kryptoaktiver") , og udstedere af [redacted] aktivbaserede tokens

g) værdipapircentraler

h) centrale modparter

i) markedspladser

j) transaktionsregistre

k) forvaltere af alternative investeringsfonde

l) administrationsselskaber

m) udbydere af dataindberetningstjenester

n) forsikrings- og genforsikringsselskaber

o) forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere

p) arbejdsmarkedsrelaterede ***pensionskasser***

q) kreditvurderingsbureauer

▌

r) administratorer af kritiske benchmarks

s) udbydere af crowdfundingtjenester

t) securitiseringsregistre

u) tredjepartsudbydere af IKT-tjenester.

2. Med henblik på denne forordning benævnes de enheder, der er omhandlet i stk. 1, litra a)-t), samlet "finansielle enheder".

3. Denne forordning finder ikke anvendelse på:

a) forvaltere af alternative investeringsfonde, der er omhandlet i artikel 3, stk. 2, i direktiv 2011/61/EU

b) forsikrings- og genforsikringsselskaber, der er omhandlet i artikel 4 i direktiv 2009/138/EF

c) arbejdsmarkedsrelaterede pensionskasser, som forvalter pensionsordninger, som tilsammen ikke har mere end 15 medlemmer i alt

d) fysiske eller juridiske personer, der er undtaget i henhold til artikel 2 og 3 i direktiv 2014/65/EU

e) forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, som er mikrovirksomheder eller små eller mellemstore virksomheder

f) postgirokontorer, der er omhandlet i artikel 2, stk. 5, nr. 3), i direktiv 2013/36/EU.

4. Medlemsstaterne kan undtage de enheder, som er omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU, og som er beliggende på deres respektive områder, fra denne forordnings anvendelsesområde. Hvis en medlemsstat gør brug af denne mulighed, underretter den Kommissionen herom og om eventuelle efterfølgende ændringer heraf. Kommissionen gør disse oplysninger offentligt tilgængelige på sit websted eller på anden let tilgængelig måde.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) "digital operationel modstandsdygtighed": en finansiel enheds evne til at opbygge, sikre og gennemgå sin operationelle integritet ***og pålidelighed*** ved enten direkte eller indirekte gennem anvendelse af tjenester, der leveres af en tredjeparts***udbyder*** af IKT-tjenester, at sikre det fulde spektrum af nødvendige IKT-relaterede kapaciteter med henblik på at varetage sikkerheden i de net- og informationssystemer, som en finansiel enhed anvender, og som understøtter det løbende udbud af finansielle tjenesteydelser og kvaliteten heraf, herunder ***i forbindelse med forstyrrelser***

2) "net- og informationssystem": et net- og informationssystem som defineret i artikel 6, nr. 1), i direktiv (EU) ***…/…***[+]

3) "legacy-IKT-system": ***et IKT-system, som har nået enden på sin livscyklus (end-of-life), som af teknologiske eller kommercielle årsager ikke er egnet til opgraderinger eller udbedringer, eller som ikke længere understøttes af leverandøren eller af en tredjepartsudbyder af IKT-tjenester, men som stadig er i brug og understøtter den finansielle enheds funktioner***

4) "sikkerhed i net- og informationssystemer": sikkerhed i net- og informationssystemer som defineret i artikel 6, nr. 2), i direktiv (EU) ***…/…***[+]

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

5) "IKT-risiko": enhver rimeligt identificerbar omstændighed i forbindelse med brugen af net- og informationssystemer ▌, som, hvis den forekommer, kan kompromittere sikkerheden i net- og informationssystemerne, i eventuelle teknologi***afhængige*** værktøjer eller processer, i ***operationer*** og ***processer***, eller i forbindelse med leveringen af tjenester***, ved at skabe*** negative virkninger ***i det digitale eller fysiske miljø***

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

7) "IKT***-aktiv***": ***et software- eller hardwareaktiv*** i de net- og informationssystemer***, der anvendes af den finansielle enhed***

8) ***"IKT-relateret hændelse": en enkeltstående hændelse eller en række af forbundne hændelser, som ikke har været planlagt af den finansielle enhed, og som*** kompromitterer sikkerheden i net- og informationssystemerne ***og*** har ***en*** negativ ***indvirkning*** på ▌ ***tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de*** tjenester, som den finansielle enhed leverer

9) ***"operationel eller sikkerhedsmæssig betalingsrelateret hændelse": en enkeltstående hændelse eller en række af forbundne hændelser, som ikke har været planlagt af de finansielle enheder, der er omhandlet i artikel 2, stk. 1, litra a)-d), uanset om de er IKT-relaterede eller ej, og som har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af betalingsrelaterede data eller på de betalingsrelaterede tjenester, der leveres af den finansielle enhed***

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

11) "større operationel eller sikkerhedsmæssig betalingsrelateret hændelse": en operationel eller sikkerhedsmæssig betalingsrelateret hændelse, som har en stor negativ indvirkning på de betalingsrelaterede tjenester, der leveres

12) "cybertrussel": en cybertrussel som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/881[35]

13) "væsentlig cybertrussel": en cybertrussel, hvis tekniske karakteristika indikerer, at den potentielt kan resultere i en større IKT-relateret hændelse eller en større operationel eller sikkerhedsmæssig betalingsrelateret hændelse

14) "cyberangreb": en ondsindet IKT-relateret hændelse, ***som er forårsaget*** af en trusselsaktørs forsøg på ødelæggelse, eksponering, ændring, deaktivering, tyveri af eller opnåelse af uautoriseret adgang til eller uautoriseret brug af et aktiv

---

[35] 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).

15) "trusselsefterretning": oplysninger, der er blevet sammenfattet, omdannet, analyseret, fortolket eller beriget for at skabe den nødvendige kontekst for beslutningstagning og ***for at muliggøre*** relevant og tilstrækkelig forståelse med henblik på at afbøde virkningerne af en IKT-relateret hændelse eller ***af en*** cybertrussel, herunder de tekniske detaljer ved et cyberangreb, kendskab til dem, der er ansvarlige for angrebet, deres måde at operere på og deres hensigter

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

17) "trusselsbaseret penetrationstest (TLPT)": 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 (red team-) test af den ***finansielle*** enheds kritiske live-produktionssystemer

18) "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 ***underleverandører, herunder gennem ordninger for outsourcing***

19) "tredjepartsudbyder af IKT-tjenester": en virksomhed, der leverer ***IKT***-tjenester ▌

20) "koncernintern udbyder af IKT-tjenester": en virksomhed, som er en del af en finansiel koncern, og som hovedsagelig leverer IKT-tjenester til finansielle enheder inden for samme koncern eller til finansielle enheder, der tilhører samme institutsikringsordning, herunder til deres moderselskaber, datterselskaber, filialer eller andre enheder, der er under fælles ejerskab eller kontrol

21) "IKT-tjenester": digitale tjenester og datatjenester, der ***løbende*** leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere, herunder ***hardware som en tjeneste*** og ***hardware***tjenester***, som omfatter hardwareudbyderens levering af teknisk support via software- eller firmwareopdateringer, eksklusive traditionelle analoge telefoni***tjenester

22) "kritisk eller vigtig funktion": en funktion, ***hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller*** som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret ▌

23) "kritisk tredjepartsudbyder af IKT-tjenester": en tredjepartsudbyder af IKT-tjenester, der er udpeget som kritisk i overensstemmelse med artikel [redacted] ***31***

24) "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

25) "dattervirksomhed": en dattervirksomhed i den i artikel 2, nr. 10), og artikel 22 i direktiv 2013/34/EU anvendte betydning

26) "koncern": en koncern som defineret i artikel 2, nr. 11), i direktiv 2013/34/EU

27) "modervirksomhed": en modervirksomhed i den i artikel 2, nr. 9), og artikel 22 i direktiv 2013/34/EU anvendte betydning

28) "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

29) "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, svigt eller andre typer af mangler i forbindelse med en sådan udbyder kan være til fare for en finansiel enheds evne til at varetage kritiske ***eller vigtige*** funktioner eller medføre andre former for negative virkninger for den, herunder store tab***, eller være til fare for den finansielle stabilitet i Unionen som helhed***

30) "ledelsesorgan": et ledelsesorgan som defineret 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 Europa-Parlamentets og Rådets direktiv 2009/65/EF[36], artikel 2, stk. 1, nr. 45), i forordning (EU) nr. 909/2014, artikel 3, stk. 1, nr. 20), i forordning (EU) 2016/1011 og i den relevante bestemmelse i forordningen om markeder for kryptoaktiver, eller dertil svarende personer, som varetager den faktiske drift af enheden eller nøglefunktioner i overensstemmelse med relevant EU-ret eller national ret

31) "kreditinstitut": kreditinstitut som defineret i artikel 4, stk. 1, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013[37]

---

[36] Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (EUT L 302 af 17.11.2009, s. 32).

[37] 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).

32) "institut, der er fritaget i henhold til direktiv 2013/36/EU": en enhed som omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU

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

34) "lille og ikke indbyrdes forbundet investeringsselskab": et investeringsselskab, som opfylder de betingelser, der er fastsat i artikel 12, stk. 1, i Europa-Parlamentets og Rådets ***forordning (EU) 2019/2033[38]***

35) "betalingsinstitut": et betalingsinstitut som defineret i artikel ***4,*** nr. ***4***), ***i direktiv (EU) 2015/2366***

36) "betalingsinstitut, der er undtaget i henhold til direktiv (EU) 2015/2366": et betalingsinstitut, der er undtaget i henhold til artikel 32, stk. 1, i direktiv (EU) 2015/2366

37) "kontooplysningstjenesteudbyder": en kontooplysningstjenesteudbyder, jf. artikel 33, stk. 1, i direktiv (EU) 2015/2366

38) "e-pengeinstitut": et e-pengeinstitut som defineret i artikel 2, nr. 1), i direktiv 2009/110/EF

---

38 Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber og om ændring af forordning (EU) nr. 1093/2010, (EU) nr. 575/2013, (EU) nr. 600/2014 og (EU) nr. 806/2014 (EUT L 314 af 5.12.2019, s. 1).

39) "e-pengeinstitut, der er undtaget i henhold til direktiv 2009/110/EF": et e-pengeinstitut, der er omfattet af en undtagelse som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF

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

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

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

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

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

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

46) "udbyder af dataindberetningstjenester": en udbyder af dataindberetningstjenester ***i den i forordning (EU) nr. 600/2014 anvendte betydning, jf.*** artikel ***2, stk. 1, nr. 34)-36) deraf***

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

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

49) "forsikringsformidler": en forsikringsformidler som defineret i artikel 2, ***stk. 1,*** nr. 3), i Europa-Parlamentets og Rådets direktiv (EU) 2016/97[39]

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

[39] Europa-Parlamentets og Rådets direktiv (EU) 2016/97 af 20. januar 2016 om forsikringsdistribution (EUT L 26 af 2.2.2016, s. 19).

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

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

53) "lille arbejdsmarkedsrelateret pensionskasse": en arbejdsmarkedsrelateret pensionskasse, der forvalter pensionsordninger, som tilsammen har mindre end 100 medlemmer i alt

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

▌

55) "udbyder af kryptoaktivtjenester": en udbyder af kryptoaktivtjenester som defineret i den relevante bestemmelse i forordningen om markeder for kryptoaktiver

▌

56) "udsteder af aktivbaserede tokens": ***en*** udsteder af ***"***aktivbaserede ▌ tokens" som defineret i den relevante bestemmelse i forordningen om markeder for kryptoaktiver

▌

57) "administrator af kritiske benchmarks": en administrator af kritiske benchmarks" som defineret i artikel ***3,*** stk. 1, nr. ***25*****),*** i forordning (EU) ***2016/1011***

58) "udbyder af crowdfundingtjenester": en udbyder af crowdfundingtjenester som defineret i artikel ***2, stk. 1,*** litra ***e*****),** i Europa-Parlamentets og Rådets forordning (EU) ***2020/1503***[40]

59) "securitiseringsregister": et securitiseringsregister som defineret i artikel 2, nr. 23), i Europa-Parlamentets og Rådets forordning (EU) 2017/2402[41]

60) "mikrovirksomhed": en finansiel enhed***, som ikke er en markedsplads, en central modpart, et transaktionsregister eller en værdipapircentral, med mindre end ti ansatte og en årlig omsætning og/eller en årlig samlet balance på højst 2 mio. EUR***

61) "ledende tilsynsførende": den europæiske tilsynsmyndighed, som er udpeget i overensstemmelse med denne forordnings artikel 31, stk. 1, litra b)

---

[40] Europa-Parlamentets og Rådets forordning (EU) 2020/1503 af 7. oktober 2020 om europæiske crowdfundingtjenesteudbydere for erhvervslivet og om ændring af forordning (EU) 2017/1129 og direktiv (EU) 2019/1937 (EUT L 347 af 20.10.2020, s. 1).

[41] Europa-Parlamentets og Rådets forordning (EU) 2017/2402 af 12. december 2017 om en generel ramme for securitisering og om oprettelse af en specifik ramme for simpel, transparent og standardiseret securitisering og om ændring af direktiv 2009/65/EF, 2009/138/EF og 2011/61/EU og forordning (EF) nr. 1060/2009 og (EU) nr. 648/2012 (EUT L 347 af 28.12.2017, s. 35).

62) "Det Fælles Udvalg": det udvalg, som er omhandlet i artikel 54 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010

63) "lille virksomhed": en finansiel enhed med 10 eller flere ansatte men med mindre end 50 ansatte og en årlig omsætning og/eller en årlig samlet balance, der overstiger 2 mio. EUR men på højst 10 mio. EUR

64) "mellemstor virksomhed": en finansiel enhed, som ikke er en lille virksomhed, med mindre end 250 ansatte og en årlig omsætning på højst 50 mio. EUR og/eller en årlig balance på højst 43 mio. EUR

65) "offentlig myndighed": enhver offentlig enhed eller anden offentlig forvaltningsenhed, herunder nationale centralbanker.

Artikel 4

Proportionalitetsprincippet

1. Finansielle enheder gennemfører de regler, der er fastsat i kapitel II i overensstemmelse med proportionalitetsprincippet, under hensyntagen til deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer.

2. Desuden skal finansielle enheders anvendelse af kapitel III, IV og kapitel V, afdeling I, stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

3. De kompetente myndigheder tager hensyn til finansielle enheders anvendelse af proportionalitetsprincippet, når de gennemgår sammenhængen i rammen for IKT-risikostyring på grundlag af de indberetninger, som indgives efter anmodning fra de kompetente myndigheder i henhold til artikel 6, stk. 5, og artikel 16, stk. 2.

Kapitel II

IKT-risikostyring

Afdeling I

Artikel 5

Forvaltning og organisation

1. Finansielle enheder skal have indført ***en*** intern forvaltnings- og kontrol***ramme***, der ***sikrer*** en effektiv og forsigtig styring af IKT-risiko***, i overensstemmelse med artikel 6, stk. 4, for at opnå et højt niveau 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 6, stk. 1**.**

Med henblik på første afsnit er det ledelsesorganet, som

a) har det ***endelige*** ansvar for styringen af den finansielle enheds IKT-risiko

b) indfører politikker, der har til formål at sikre opretholdelse af høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data

c) fastlægger klare roller og ansvarsområder for alle IKT-relaterede funktioner ***og etablerer passende forvaltningsordninger for at sikre effektiv og rettidig kommunikation, samarbejde og koordinering mellem disse funktioner***

d) ***har det samlede ansvar for fastlæggelse og godkendelse af strategien for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, herunder fastsættelse af*** et passende risikotoleranceniveau for IKT-risiko i den finansielle enhed, jf. artikel 6, stk. 8, litra b)

e) godkender, fører tilsyn med og regelmæssigt gennemgår gennemførelsen af den finansielle enheds politik for IKT-driftsstabilitet og planer for IKT-***indsats og -genopretning***, jf. henholdsvis artikel 11, stk. 1 og 3***, der kan vedtages som en særlig specifik politik, der udgør en integrerende del af den finansielle enheds samlede politik for driftsstabilitet og indsats- og genopretningsplan***

f) godkender og regelmæssigt gennemgår ***den finansielle enheds interne*** IKT-revisionsplaner, IKT-revisioner og væsentlige ændringer heraf

g) 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*** IKT***-programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, og IKT-***færdigheder for alt [redacted]– personale

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

i) indfører indberetningskanaler på virksomhedsniveau, der gør det muligt for det at blive behørigt underrettet om følgende:

i) ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester

ii) relevante planlagte væsentlige ændringer, som vedrører tredjepartsudbydere af IKT-tjenester

iii) potentielle virkninger af sådanne ændringer på de kritiske eller vigtige funktioner, der er omfattet af disse ordninger, herunder en sammenfatning af risikoanalysen med henblik på at vurdere virkningerne af disse ændringer og ***som minimum større*** IKT-relaterede hændelser og deres virkninger samt indsatsforanstaltninger, genopretningsforanstaltninger og korrigerende foranstaltninger.

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

4. Medlemmerne af ***den finansielle enheds*** ledelsesorgan holder ***aktivt*** den viden og de færdigheder, der er nødvendige for at forstå og vurdere IKT-risiko og dens indvirkning på den finansielle enheds drift, ajour***, herunder ved regelmæssigt at følge særlige kurser, svarende til den IKT-risiko, der styres***.

Afdeling II

Artikel 6

Ramme for IKT-risikostyring

1. Finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for IKT-risikostyring ***som en del af deres samlede risikostyringssystem***, der sætter dem i stand til at håndtere IKT-risikoen hurtigt, effektivt og fyldestgørende, og som sikrer et højt niveau af digital operationel modstandsdygtighed ▌.

2. Rammen for IKT-risikostyring skal ***som minimum*** omfatte strategier, politikker, procedurer, IKT-protokoller og -værktøjer, ***som*** er nødvendige for på behørig vis og ***i tilstrækkelig grad*** at beskytte alle ***informationsaktiver og IKT-aktiver***, herunder computer***software,*** -hardware og servere, samt for at beskytte alle ***relevante fysiske komponenter og infrastrukturer, såsom*** ▌ lokaler, datacentre og sensitive udpegede områder, for at sikre tilstrækkelig beskyttelse af alle ***informationsaktiver og IKT-aktiver*** mod risici, herunder skade og uautoriseret adgang eller brug.

3. I overensstemmelse med deres ramme for IKT-risikostyring minimerer de finansielle enheder virkningerne af IKT-risiko ved at indføre passende strategier, politikker, procedurer, IKT-protokoller og -værktøjer. De forelægger fuldstændige og ajourførte oplysninger om IKT-risiko ***og om deres ramme for IKT-styring*** for de kompetente myndigheder på disses ***anmodning***.

4. Finansielle enheder, som ikke er mikrovirksomheder***, overdrager ansvaret for styring af og tilsyn med IKT-risikoen til en kontrolfunktion og sikrer, at denne kontrolfunktion har et passende uafhængighedsniveau, således at interessekonflikter undgås. Finansielle enheder*** sikrer en passende adskillelse ***og uafhængighed*** af IKT-***risiko***styringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

5. Rammen for IKT-risikostyring skal dokumenteres og gennemgås mindst én gang om året***, eller regelmæssigt for så vidt angår mikrovirksomheder***, samt når der forekommer større IKT-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. ***Der skal forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed på dens anmodning.***

6. Revisorer ▌ foretager regelmæssigt ***intern revision*** af rammen for IKT-risikostyring ***for andre finansielle enheder end mikrovirksomheder i overensstemmelse med de finansielle enheders revisionsplan. Disse revisorer skal*** besidde tilstrækkelig viden, faglig kompetence og ekspertise med hensyn til IKT-risici ***og være tilstrækkeligt uafhængige***. Hyppigheden af IKT-revisioner og deres fokus skal stå i rimeligt forhold til den finansielle enheds IKT-risiko.

7. De finansielle enheder etablerer på baggrund af konklusioner fra den interne revisionsgennemgang en formel opfølgningsproces, herunder regler for rettidig efterprøvning og udbedring af kritiske resultater af IKT-revisioner.

8. Rammen for IKT-risikostyring skal omfatte en strategi for digital ***operationel*** modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Med henblik herpå skal ***strategien for digital operationel modstandsdygtighed*** omfatte metoderne til håndtering af IKT-risiko og opfylde specifikke IKT-mål ved at

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

b) fastlægge risikotolerance***niveauet*** for IKT-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af IKT-forstyrrelser

c) fastsætte klare informationssikkerhedsmål***, herunder centrale resultatindikatorer og centrale risikoparametre***

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

e) beskrive de forskellige indførte mekanismer til detektion af IKT-relaterede hændelser, forebygge deres virkning og give beskyttelse mod den

f) dokumentere ***den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af*** antallet af indberettede større IKT-relaterede hændelser og de forebyggende foranstaltningers effektivitet

I

g) gennemføre test af digital operationel modstandsdygtighed ***i overensstemmelse med denne forordnings kapitel IV***

h) fastlægge en kommunikationsstrategi i tilfælde af IKT-relaterede hændelser***, hvis offentliggørelse er påkrævet i henhold til artikel 14.***

9. ***Finansielle enheder kan i forbindelse med strategien for digital operationel modstandsdygtighed som omhandlet i stk. 8 fastlægge*** en ***helhedsorienteret strategi med flere IKT-udbydere på koncern- eller enhedsplan***, som viser, hvor der er stor afhængighed af tredjepartsudbydere af IKT-tjenester, og begrunde den pågældende udbudssammensætning af ***tredjepartsudbydere af IKT-tjenester.***

10. ***Finansielle*** enheder kan ***i overensstemmelse med sektorspecifik EU-ret og national ret outsource*** de opgaver, der er forbundet med efterprøvning af overholdelsen af kravene til IKT-risikostyring, til koncerninterne eller eksterne virksomheder. ***I tilfælde af en sådan outsourcing er den finansielle enhed fortsat fuldt ud ansvarlig for at efterprøve overholdelsen af kravene til IKT-risikostyring.***

Artikel 7

IKT-systemer, -protokoller og-værktøjer

For at håndtere og styre IKT-risikoen anvender og vedligeholder finansielle enheder opdaterede IKT-systemer, -protokoller og -værktøjer, ***som er***:

a) ▌passende i forhold til ▌omfanget af de operationer, der ligger til grund for gennemførelsen af deres aktiviteter***, i overensstemmelse med proportionalitetsprincippet som omhandlet i artikel 4***

b) ▌pålidelige

c) ▌***udstyret med*** 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) ▌teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer.

▌

Artikel 8

Identifikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, foretager de finansielle enheder identifikation, klassificering og tilstrækkelig dokumentering af alle IKT***-understøttede*** forretningsfunktioner, ***roller og ansvarsområder,*** informationsaktiver ***og IKT-aktiver,*** der understøtter disse funktioner, samt ***deres roller og afhængigheder*** med hensyn til ▌IKT-▌***risici***. De finansielle enheder vurderer efter behov og mindst én gang om året, hvorvidt ***denne*** klassificering ▌og eventuel relevant dokumentation er tilstrækkelig.

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

3. Finansielle enheder, som ikke er mikrovirksomheder, foretager en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres IKT-understøttede forretningsfunktioner, informationsaktiver eller IKT-aktiver.

4. De finansielle enheder identificerer alle ***informationsaktiver og IKT-aktiver***, herunder på eksterne steder, ▌netværksressourcer og hardwareudstyr, og kortlægger ***dem***, der anses for kritiske. De kortlægger ***informationsaktivernes og*** IKT-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige ***informationsaktiver og*** IKT-aktiver.

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

6. Med henblik på stk. 1, 4 og 5 opretholder [redacted] finansielle enheder relevante fortegnelser ***og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i stk. 3.***

7. Finansielle enheder, som ikke er mikrovirksomheder, foretager regelmæssigt og mindst én gang om året en specifik IKT-risikovurdering af alle legacy-IKT-systemer og i alle tilfælde før og efter sammenkobling af [redacted] teknologier, applikationer eller systemer.

Artikel 9

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 IKT-systemernes og -værktøjernes ***sikkerhed og af, hvordan de*** fungerer, og minimerer virkningerne af ***IKT-***risikoen for IKT-systemer ved at indføre passende IKT-sikkerhedsværktøjer, -politikker og -procedurer.

2. De finansielle enheder udformer, indkøber og gennemfører IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der [redacted] har til formål at sikre IKT-systemernes modstandsdygtighed, stabilitet og tilgængelighed, ***især for dem, der understøtter kritiske eller vigtige funktioner,*** og at opretholde høje standarder for [redacted], ***tilgængeligheden, autenticiteten, integriteten og fortroligheden af data***, 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-***løsninger*** og -processer, ***som er hensigtsmæssige i overensstemmelse med artikel 4. Disse IKT-løsninger og -processer***:

a) sikrer sikkerheden for metoderne til overførsel af ***data***

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

c) forhindrer ***manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data***

d) sikrer, at data beskyttes mod ***risici, der opstår i forbindelse med dataforvaltning, herunder*** dårlig administration ▌**,** procesrelaterede risici ***og menneskelige fejl***.

4. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, skal de finansielle enheder

a) udvikle og dokumentere en informationssikkerhedspolitik, der fastlægger regler for beskyttelse af ***tilgængeligheden, autenticiteten, integriteten og fortroligheden*** af data**,** informationsaktiver ***og IKT-aktiver, herunder deres kunders, hvis det er relevant***

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

c) gennemføre politikker, der begrænser den fysiske ***eller logiske*** adgang til ***informationsaktiver*** og IKT-***aktiver*** udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf

d) gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer ***og beskyttelsesforanstaltninger for*** krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte ***IKT***-risikovurderingsprocesser

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

f) sørge for, at der indføres passende og omfattende ***dokumenterede*** politikker for programrettelser og opdateringer.

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

Med henblik på første afsnit, litra e), skal IKT-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Artikel 10

Detektion

1. De finansielle enheder indfører mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med IKT-netværkets ydeevne og IKT-relaterede hændelser, og til identifikation af [redacted] potentielt væsentlige single points of failure.

De i første afsnit omhandlede mekanismer testes regelmæssigt i overensstemmelse med artikel 25.

2. Ved de i stk. 1 omhandlede detektionsmekanismer skal det gøres muligt at anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse ▌ og ***igangsætte*** indsatsforanstaltninger mod IKT-relaterede hændelser, ***herunder*** automatiske varslingsmekanismer 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.

4. Udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Artikel 11

Indsats og genopretning

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, og baseret på de krav til identifikation, der er fastsat i artikel 8, indfører de finansielle enheder ▌ en omfattende politik for IKT-driftsstabilitet***, som kan vedtages som en særlig specifik politik, der skal udgøre*** en integreret del af den finansielle enheds ***samlede*** politik for driftsstabilitet.

2. De finansielle enheder gennemfører politikken for IKT-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer, der tager sigte mod:

a) at sikre, at den finansielle enheds kritiske ***eller vigtige*** funktioner er stabile

b) hurtigt, passende og effektivt at sætte ind over for og løse alle IKT-relaterede hændelser på en måde, ***der*** begrænser skaden og prioriterer genoptagelsen af aktiviteter og genopretningstiltag

c) omgående at aktivere særlige planer, der gør det muligt at anvende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer IKT-relaterede hændelser, og som forhindrer yderligere skade, samt skræddersyede indsats- og genopretningsprocedurer, der er fastlagt i henhold til artikel 12

d) at anslå foreløbige virkninger, skader og tab

e) at indføre kommunikations- og krisestyringstiltag, ***der*** sikrer, at ajourførte oplysninger videresendes til al relevant internt personale og eksterne interessenter i overensstemmelse med artikel 14, og at de indberettes til de kompetente myndigheder i overensstemmelse med artikel 19.

3. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, gennemfører de finansielle enheder ▌ dertil knyttede ***planer*** for IKT-***indsats og -genopretning***, som for finansielle enheder, der ikke er mikrovirksomheder, underkastes uafhængige ***interne*** revisionsgennemgange.

4. De finansielle enheder indfører, vedligeholder og foretager regelmæssig testning 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 den samlede politik for driftsstabilitet foretager de finansielle enheder en forretningskonsekvensanalyse (BIA) af deres eksponering for alvorlige driftsforstyrrelser. De finansielle enheder vurderer i forbindelse med BIA'en de potentielle virkninger af alvorlige driftsforstyrrelser ved hjælp af kvantitative og kvalitative kriterier ved anvendelse af interne og eksterne data og scenarieanalyser, alt efter hvad der er relevant. BIA'en skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner, støtteprocesser, tredjepartsafhængighed og informationsaktiver samt deres indbyrdes afhængighed. De finansielle enheder sikrer, at IKT-aktiver og -tjenester udformes og anvendes i fuld overensstemmelse med BIA'en, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans.

6. Som led i den omfattende IKT-risikostyring skal de finansielle enheder

a) teste deres ***planer*** for IKT-driftsstabilitet og ***planer*** for IKT-***indsats og*** -genopretning ***i forbindelse med IKT-systemer, der understøtter alle funktioner,*** mindst én gang om året ***og i tilfælde af*** væsentlige ændringer af IKT-systemer***, der understøtter kritiske eller vigtige funktioner***

b) teste de krisekommunikationsplaner, der er udarbejdet i henhold til artikel 14.

Med henblik på første afsnit, litra a), medtager finansielle enheder, som ikke er mikrovirksomheder, cyberangrebscenarier og omstillingsscenarier mellem den primære IKT-infrastruktur og redundante kapacitet, sikkerhedskopier og de redundante faciliteter, der er nødvendige for at opfylde de i artikel 12 fastsatte forpligtelser, i testplanerne.

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

7. Finansielle enheder, som ikke er mikrovirksomheder, skal have en krisestyringsfunktion, som, hvis deres ***planer*** for IKT-driftsstabilitet og ***planer*** for IKT***-indsats og -genopretning*** aktiveres, ***bl.a.*** skal indeholde klare procedurer for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

8. De finansielle enheder fører let ***tilgængelige*** registre over aktiviteter før og under driftsforstyrrelser, når deres ***planer for*** IKT-driftsstabilitet og ***planer*** for IKT***-indsats og -genopretning*** aktiveres.

9. Værdipapircentraler forelægger kopier af resultaterne af test af IKT-driftsstabiliteten eller lignende aktiviteter for de kompetente myndigheder.

10. Finansielle enheder, som ikke er mikrovirksomheder, indberetter ***et overslag over de samlede årlige*** omkostninger og tab, der opstår som følge af ***større*** IKT-relaterede hændelser, til de kompetente myndigheder ***på deres anmodning***.

11. I overensstemmelse med artikel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, udarbejder ESA'erne ***via Det Fælles Udvalg*** senest den ***… [18 måneder efter denne forordnings ikrafttræden] fælles retningslinjer for overslaget over de samlede årlige omkostninger og tab, der er omhandlet i stk. 10.***

Artikel 12

Politikker og procedurer for sikkerhedskopiering og procedurer og metoder for ***gendannelse*** og genopretning

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

   a) ***politikker og procedurer*** for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller ***fortrolighedsniveauet for dataene***

   b) procedurer og metoder for gendannelse og genopretning.

2. ***De finansielle enheder etablerer*** systemer for ***sikkerhedskopiering, der kan aktiveres i overensstemmelse med politikker og procedurer for sikkerhedskopiering, og procedurer og metoder for gendannelse og genopretning. Aktiveringen af systemerne for sikkerhedskopiering må ikke*** sætte sikkerheden i net- og informationssystemer eller ***tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data*** over styr. ***Der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.***

3. Når de finansielle enheder gendanner sikkerhedskopierede data ved anvendelse af egne systemer, anvender de IKT-systemer, der ***er fysisk og logisk adskilt fra IKT-kildesystemet. IKT-systemerne skal være*** sikkert beskyttet mod uautoriseret adgang eller IKT-korruption ***og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov***.

   For centrale modparter skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato.

   Udbydere af dataindberetningstjenester ***skal desuden sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester***.

4. Finansielle enheder, ***der ikke er mikrovirksomheder,*** opretholder redundante IKT-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. ***Mikrovirksomheder vurderer behovet for at opretholde sådanne redundante IKT-kapaciteter på grundlag af deres risikoprofil.***

5. Værdipapircentraler bibeholder mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på 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 ***eller vigtige funktioner*** på samme måde som det primære afviklingssted eller levere det serviceniveau, der er nødvendigt for, at den finansielle enhed kan udføre sine kritiske operationer inden for rammerne af genopretningsmålene

   c) være umiddelbart tilgængeligt for den finansielle enheds personale for at sikre driftsstabilitet for kritiske ***eller vigtige funktioner*** i tilfælde af, at det primære afviklingssted ikke står til rådighed.

6. Når de finansielle enheder fastlægger målene for genopretningstid og genopretningspunkt for hver funktion, tager de hensyn til, ***om det er en kritisk eller vigtig funktion og*** de potentielle samlede virkninger for markedseffektiviteten. Sådanne tidsmål skal sikre, at de aftalte serviceniveauer overholdes i ekstreme scenarier.

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

Artikel 13

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 de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

2. De finansielle enheder foretager gennemgange af IKT-relaterede hændelser, efter at en ***større*** IKT***-relateret*** hændelse ***forstyrrer*** deres kerneaktiviteter, analyserer årsagerne til forstyrrelserne og identificerer nødvendige forbedringer af IKT-operationerne eller inden for rammerne af den i artikel 11 omhandlede politik for IKT-driftsstabilitet.

Finansielle enheder, som ikke er mikrovirksomheder, underretter ***på anmodning*** de kompetente myndigheder om ændringer, der ***er blevet gennemført efter gennemgange af IKT–relaterede hændelser som omhandlet i første afsnit***.

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

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

b) kvaliteten og hastigheden af udførelsen af en kriminalteknisk analyse, ***hvor det skønnes hensigtsmæssigt***

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

d) effektiviteten af den interne og eksterne kommunikation.

3. Erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske IKT-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af ***planer for IKT-*** driftsstabilitet og ***planer for IKT-indsats og -***genopretning skal sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende indarbejdes i IKT-risikovurderingsprocessen. Disse resultater danner grundlag for passende gennemgange af relevante komponenter i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1.

4. De finansielle enheder overvåger effektiviteten af gennemførelsen af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8. De kortlægger IKT-risikoens udvikling over tid, analyserer hyppigheden, typerne, omfanget af og udviklingen i IKT-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed, med henblik på at forstå graden af IKT-risikoeksponering***, navnlig i forbindelse med kritiske eller vigtige funktioner,*** og forbedre den finansielle enheds cybermodenhed og cyberberedskab.

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

6. De finansielle enheder udvikler programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Disse programmer og kurser skal omfatte alle medarbejdere og den øverste ledelse ***og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Hvis det er relevant, inddrager finansielle enheder også tredjepartsudbydere af IKT-tjenester i deres relevante uddannelsesordninger i overensstemmelse med artikel 30, stk. 2, litra i)***.

7. Finansielle enheder, ***der ikke er mikrovirksomheder,*** overvåger løbende den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning 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 for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14

Kommunikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, sørger de finansielle enheder for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af ***som minimum større*** IKT-relaterede hændelser eller ▌- sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

2. Som led i rammen for IKT-risikostyring gennemfører de finansielle enheder kommunikationsplaner for internt personale og for eksterne interessenter. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale, der er involveret i IKT-risikostyring, navnlig det personale, der er ansvarligt for indsats og genopretning, og personale, der skal underrettes.

3. Mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for IKT-relaterede hændelser og til dette formål varetage ▌- ***funktionen*** vedrørende offentligheden og medierne.

Artikel 15

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

ESA'erne udarbejder via Det Fælles Udvalg og i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) ***fælles*** udkast til reguleringsmæssige tekniske standarder med henblik på:

a) at præcisere, hvilke yderligere elementer der skal indgå i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug, bevare ***tilgængeligheden, autenticiteten, integriteten og fortroligheden af data***, herunder kryptografiske teknikker, og garantere en nøjagtig og hurtig dataoverførsel uden større forstyrrelser ***og unødige forsinkelser***

▌

b) at videreudvikle komponenter i kontrollen med de rettigheder vedrørende adgangsforvaltning, der er omhandlet i artikel 9, 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-risikoen ved hjælp af passende indikatorer, herunder for mønstre vedrørende netværksbrug, tidspunkter, IT-aktivitet og ukendt udstyr

c) at videreudvikle de mekanismer, der er anført i artikel 10, stk. 1, for at muliggøre en hurtig detektion af anormale aktiviteter, og de kriterier, der er fastsat i artikel 10, stk. 2, for at udløse detektion af IKT-relaterede hændelser og indsatsforanstaltninger

d) yderligere at præcisere de komponenter, der er indeholdt i den ***politik for*** IKT-***driftsstabilitet***, der er omhandlet i artikel 11, stk. 1

e) yderligere at præcisere test af de planer for IKT-driftsstabilitet, der er omhandlet i artikel 11, stk. 6, for at sikre, at sådanne test tager 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 svigt forårsaget af eventuelle relevante tredjepartsudbydere af IKT-tjenester og, hvor det er relevant, de politiske risici i de respektive udbyderes jurisdiktioner

f) yderligere at præcisere de komponenter, der er indeholdt i de ***planer*** for IKT-***indsats og -genopretning***, der er omhandlet i artikel 11, stk. 3

g) yderligere at præcisere indholdet i og formatet af den rapport om gennemgangen af rammen for IKT-risikostyring, der er omhandlet i artikel 6, stk. 5.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer og tager samtidig behørigt hensyn til eventuelle særlige kendetegn som følge af aktiviteternes særlige karakter på tværs af forskellige sektorer for finansielle tjenesteydelser.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [***12 måneder efter datoen for denne forordnings ikrafttræden]***.

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 forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 16

Forenklet ramme for IKT-risikostyring

1. Nærværende forordnings artikel 5-15 finder ikke anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder:

a) indføre og vedligeholde en robust og dokumenteret ramme for IKT-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af IKT-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer

b) løbende overvåge alle IKT-systemers sikkerhed og drift

c) minimere virkningen af IKT-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte IKT-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne

d) gøre det muligt hurtigt at konstatere og detektere IKT-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere IKT-relaterede hændelser

e) konstatere stor afhængighed af tredjepartsudbydere af IKT-tjenester

f) sikre kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger

g) regelmæssigt teste de planer og foranstaltninger, der er omhandlet i litra f), samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a) og c)

h) gennemføre, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g), og af de efterfølgende analyser af hændelserne, i IKT-risikovurderingsprocessen og efter behov og IKT-risikoprofil udvikle programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

2. Den i stk. 1, andet afsnit, litra a) omhandlede ramme for IKT-risikostyring skal dokumenteres og gennemgås regelmæssigt og ved forekomst af større IKT-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed på dennes anmodning.

3. ESA'erne udarbejder via Det Fælles Udvalg og i samråd med ENISA fælles udkast til reguleringsmæssige tekniske standarder med henblik på:

a) yderligere at præcisere de elementer, der skal indgå i rammen for IKT-risikostyring som omhandlet i stk. 1, andet afsnit, litra a)

b) yderligere at præcisere de elementer, der for så vidt angår systemer, protokoller og værktøjer mindsker virkningerne af den IKT-risiko, der er omhandlet i stk. 1, andet afsnit, litra c), med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data

c) yderligere at præcisere de komponenter, der er indeholdt i de planer for IKT-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f)

d) yderligere at præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g), og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes

e) yderligere at præcisere indholdet og formatet af den rapport om gennemgangen af rammen for IKT-risikostyring, der er omhandlet i stk. 2.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [12 måneder efter datoen for denne forordnings ikrafttræden].

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit 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 III

Styring, klassificering og indberetning af IKT-relaterede hændelser

Artikel 17

Proces for styring af IKT-relaterede hændelser

1. De finansielle enheder ***definerer,*** fastlægger og gennemfører en proces for styring af IKT-relaterede hændelser for at detektere, styre og indberette IKT-relaterede hændelser ▌.

2. ***De finansielle enheder registrerer alle IKT-relaterede hændelser og væsentlige cybertrusler.*** 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***, dokumenteres*** og ***håndteres for at*** forhindre, at sådanne hændelser forekommer.

3. Som led i den proces for styring af IKT-relaterede hændelser, der er omhandlet i stk. 1:

a) indføres der tidlige advarselsindikatorer

b) fastlægges der procedurer til at identificere, spore, logge, kategorisere og klassificere IKT-relaterede hændelser alt efter deres prioritet og vigtighed og alt efter den kritiske betydning i overensstemmelse med de kriterier, der er fastlagt i artikel 18, stk. 1

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

d) udarbejdes der planer for kommunikation til personale, eksterne interessenter og medier i overensstemmelse med artikel 14 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

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

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

Artikel 18

Klassificering af IKT-relaterede hændelser ***og cybertrusler***

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

a) antallet ***og/eller relevansen*** af ***kunder*** eller finansielle modparter, som er berørt, ***og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt*** af den IKT-relaterede hændelse, og hvorvidt den IKT-relaterede hændelse har haft indvirkning på omdømmet

b) varigheden af den IKT-relaterede hændelse, herunder tjeneste***ns*** 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 med hensyn til ***tilgængelighed, autenticitet, integritet eller fortrolighed af data***

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

f) de økonomiske virkninger***, navnlig direkte og indirekte omkostninger og tab,*** af den IKT-relaterede hændelse i både absolutte og relative tal.

2. De finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

3. ESA'erne udarbejder via Det Fælles Udvalg ▌og ***i*** samråd med ECB og ENISA fælles udkast til reguleringsmæssige tekniske standarder, som yderligere præciserer følgende:

a) kriterierne i stk. 1, herunder væsentlighedstærskler til bestemmelse af større IKT-relaterede hændelser ***eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som*** er omfattet af indberetningspligten i artikel 19, stk. 1

b) de kriterier, som de kompetente myndigheder skal anvende med henblik på at vurdere relevansen af større IKT-relaterede hændelser ***eller, alt efter hvad der er relevant, af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, for de relevante myndigheder i*** andre medlemsstater ▌, og de nærmere oplysninger i ***rapporterne om større*** IKT-relaterede hændelser ***eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser,*** som skal udveksles med andre kompetente myndigheder i henhold til artikel 19, stk. 6 og 7

c) kriterierne i denne artikels stk. 2, herunder høje væsentlighedstærskler til bestemmelse af væsentlige cybertrusler.

4. Når ESA'erne udarbejder de i denne artikels stk. 3 omhandlede fælles udkast til reguleringsmæssige tekniske standarder, tager de hensyn til ***kriterierne i artikel 4, stk. 2, samt*** de internationale standarder, den ***vejledning og*** de specifikationer, der er udarbejdet og offentliggjort af ENISA, herunder, hvor det er relevant, specifikationer for andre økonomiske sektorer. ***Med henblik på anvendelse af kriterierne i artikel 4, stk. 2, tager ESA'erne behørigt hensyn til behovet for, at mikrovirksomheder og små og mellemstore virksomheder mobiliserer tilstrækkelige ressourcer og kapaciteter til at sikre, at IKT-relaterede hændelser håndteres hurtigt.***

ESA'erne forelægger disse fælles udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [***12 måneder*** efter datoen ***for denne forordnings*** ikrafttræden].

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i stk. 3 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.

Artikel 19

Indberetning af større IKT-relaterede hændelser ***og frivillig underretning om væsentlige cybertrusler***

1. De finansielle enheder indberetter større IKT-relaterede hændelser til den relevante kompetente myndighed som omhandlet i artikel 46 ***i overensstemmelse med*** denne artikels stk. 4.

Hvis en finansiel enhed er underlagt tilsyn af mere end en national kompetent myndighed som omhandlet i artikel 46, udpeger medlemsstaterne en fælles kompetent myndighed som den relevante kompetente myndighed, der er ansvarlig for at udføre de i denne artikel omhandlede funktioner og opgaver.

Kreditinstitutter, der er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, indberetter større IKT-relaterede hændelser til den relevante nationale kompetente myndighed, der er udpeget i overensstemmelse med artikel 4 i direktiv 2013/36/EU, og som øjeblikkeligt videresender den pågældende rapport til ECB.

Med henblik på første afsnit udarbejder de finansielle enheder efter indsamling og analyse af alle relevante oplysninger ***den indledende underretning og de rapporter, der er omhandlet i denne artikels stk. 4***, ved brug af de modeller, der er omhandlet i artikel 20, og indgiver dem til den kompetente myndighed. ***Hvis det er teknisk umuligt at indgive den indledende underretning ved brug af modellen, meddeler de finansielle enheder den kompetente myndighed den på anden vis.***

Den ***indledende underretning og de rapporter, der er omhandlet i stk. 4,*** 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.

Med forbehold af den finansielle enheds indberetning i henhold til første afsnit til den relevante kompetente myndighed kan medlemsstaterne derudover bestemme, at visse eller alle finansielle enheder også skal indgive den indledende underretning og hver enkelt rapport som omhandlet i denne artikels stk. 4 ved brug af de modeller, der er omhandlet i artikel 20, til de kompetente myndigheder eller til de enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), som er udpeget eller oprettet i overensstemmelse med direktiv (EU) …/…[+].

[+] EUT: Indsæt venligst nummeret på det direktiv, der er indeholdt i dokument PE-CONS 32/22 (2020/0359(COD)), i teksten.

2. De finansielle enheder kan på frivillig basis underrette den relevante kompetente myndighed om væsentlige cybertrusler, når de anser truslen for at være relevant for det finansielle system, tjenestebrugere eller kunder. Den relevante kompetente myndighed kan give sådanne oplysninger til andre relevante myndigheder som omhandlet i stk. 6.

Kreditinstitutter, der er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, kan på frivillig basis underrette den relevante nationale kompetente myndighed, der er udpeget i overensstemmelse med artikel 4 i direktiv 2013/36/EU, og som øjeblikkeligt videresender underretningen til ECB, om væsentlige cybertrusler.

Medlemsstaterne kan bestemme, at disse finansielle enheder, som på frivillig basis indgiver en underretning, jf. først afsnit, også kan videresende den pågældende underretning til de CSIRT'er, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) …/...[+].

[+] EUT: Indsæt venligst nummeret på det direktiv, der er indeholdt i dokument PE-CONS 32/22 (2020/0359(COD)), i teksten.

3. Hvis en større IKT-relateret hændelse ***indtræffer og*** har [redacted] indflydelse på [redacted] kunders finansielle interesser, underretter de finansielle enheder uden unødigt ophold, så snart de ***får kendskab til den,*** deres [redacted] kunder om den større IKT-relaterede hændelse og ***om de*** foranstaltninger***, der*** er truffet for at afbøde de negative virkninger af en sådan hændelse.

I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe.

4. De finansielle enheder ***indgiver inden for de frister, der skal fastsættes i overensstemmelse med*** artikel 20***, stk. 1, litra a), nr. 2), følgende til den relevante kompetente myndighed***:

a) en indledende underretning [redacted]

b) en foreløbig rapport efter den indledende underretning, jf. litra a), ***så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større IKT-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger,*** efterfulgt, alt efter hvad der er relevant, 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, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn ▌.

5. De finansielle enheder kan ***i overensstemmelse med EU- og national sektorspecifik ret outsource*** opfyldelsen af indberetningsforpligtelserne i henhold til denne artikel til en tredjepartstjenesteudbyder ▌. ***I tilfælde*** af en ***sådan outsourcing er*** den ***finansielle enhed fortsat fuldt ud ansvarlig for at opfylde kravene vedrørende indberetning af hændelser***.

6. Når den kompetente myndighed modtager den ***indledende underretning og hver enkelt*** rapport som omhandlet i stk. ***4***, forelægger den ***rettidigt*** nærmere oplysninger om den ***større IKT-relaterede*** hændelse for ***følgende modtagere på grundlag af deres respektive kompetencer, alt efter hvad der er relevant***:

a) EBA, ESMA eller EIOPA ▌

b) ECB ▌ i tilfælde af finansielle enheder som omhandlet i artikel 2, stk. 1, litra a), b) og d),

c) de ***kompetente myndigheder,*** de centrale kontaktpunkter ***eller CSIRT'er***, der er udpeget eller oprettet ***i overensstemmelse med*** direktiv (EU) …/…[+]

[+] EUT: Indsæt venligst nummeret på det direktiv, der er indeholdt i dokument PE-CONS 32/22 (2020/0359(COD)), i teksten.

d) afviklingsmyndighederne som omhandlet i artikel 3 i direktiv 2014/59/EU og Den Fælles Afviklingsinstans (SRB) for så vidt angår de enheder, der er omhandlet i artikel 7, stk. 2, i Europa-Parlamentets og Rådets ***forordning (EU) nr. 806/2014[42], og for så vidt angår de enheder og koncerner, der er omhandlet i artikel 7, stk. 4, litra b), og artikel 7, stk. 5, i forordning (EU) nr. 806/2014, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35), i direktiv 2014/59/EU, og***

e) andre relevante offentlige myndigheder i henhold til national ret.

7. ***Efter modtagelse af oplysningerne i overensstemmelse med stk. 6*** vurderer EBA, ESMA eller EIOPA og ECB ***i samråd med ENISA og i samarbejde med den relevante kompetente myndighed,*** om den større IKT-relaterede hændelse er relevant for ***kompetente*** myndigheder ***i andre medlemsstater. Efter denne vurdering underretter EBA, ESMA eller EIOPA*** så hurtigt som muligt ***de relevante kompetente myndigheder i andre medlemsstater*** 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.

---

42 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).

8. Den underretning, som ESMA skal indgive i henhold til denne artikels stk. 7, berører ikke den kompetente myndigheds ansvar for hurtigt at videresende nærmere oplysninger om den større IKT-relaterede hændelse til den relevante myndighed i værtslandet, hvis en værdipapircentral har betydelige grænseoverskridende aktiviteter i værtslandet, den større IKT-relaterede hændelse forventes at have alvorlige konsekvenser for de finansielle markeder i værtslandet, og hvis der er samarbejdsordninger mellem de kompetente myndigheder med hensyn til tilsyn med finansielle enheder.

Artikel 20

Harmonisering af indholdet af og modeller for indberetninger

ESA'erne udarbejder via Det Fælles Udvalg og ***i*** samråd med ENISA og ECB følgende:

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

i) at fastlægge indholdet af indberetningerne om større IKT-relaterede hændelser ***for at afspejle de kriterier, der er fastsat i artikel 18, stk. 1, og indarbejde yderligere elementer såsom nærmere oplysninger til fastlæggelse af relevansen af indberetningerne for andre medlemsstater og om, hvorvidt hændelsen udgør en større operationel eller sikkerhedsmæssig betalingsrelateret hændelse***

ii) at fastsætte fristerne for den indledende underretning og for hver enkelt rapport som omhandlet i artikel 19, stk. 4

iii) at fastlægge indholdet af underretningen om væsentlige cybertrusler.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer, navnlig med henblik på at sikre, at forskellige frister, jf. dette stykkes litra a), nr. ii), alt efter hvad der er relevant, kan afspejle særlige forhold i de finansielle sektorer, uden at det berører opretholdelsen af en konsekvent tilgang til indberetning af IKT-relaterede hændelser i henhold til denne forordning og til direktiv (EU) .../...[+]. ESA'erne skal, alt efter hvad der er relevant, begrunde, hvis de afviger fra de tilgange, der er anlagt i forbindelse med nævnte direktiv

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

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

ESA'erne forelægger det fælles udkast til reguleringsmæssige tekniske standarder, der er omhandlet i ***stk. 1,*** litra a), og det fælles udkast til gennemførelsesmæssige tekniske standarder, der er omhandlet ***stk. 1,*** litra b), for Kommissionen senest den ... [***18 måneder*** efter datoen for ***denne forordnings ikrafttræden***].

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

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

Artikel 21

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 den praktiske mulighed for yderligere centralisering af indberetningen af hændelser gennem oprettelse af et fælles EU-knudepunkt for finansielle enheders indberetning af større IKT-relaterede hændelser. I den fælles rapport 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 fælles rapport skal mindst omfatte følgende elementer:

   a) forudsætninger for oprettelsen af ***et fælles*** EU-knudepunkt

   b) fordele, begrænsninger og ***risici, herunder*** risici ***forbundet med den høje koncentration af følsomme oplysninger***

c) den nødvendige kapacitet til at sikre interoperabilitet med andre relevante indberetningsordninger

d) elementer af den operationelle styring

e) betingelser for medlemskab

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

g) en foreløbig vurdering af de finansielle omkostninger, der er forbundet med oprettelse 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 ... [***24 måneder*** efter datoen ***for denne forordnings*** ikrafttræden].

Artikel 22

Tilsynsmæssig feedback

1. ***Med forbehold af teknisk input, rådgivning eller afhjælpende foranstaltninger og efterfølgende opfølgning herpå, som CSIRT'erne, hvis det er relevant,*** i overensstemmelse med national ret ***kan tilvejebringe i henhold til direktiv (EU) …/…***[+], kvitterer den kompetente myndighed***, når den modtager den indledende underretning og hver enkelt rapport, jf. artikel 19, stk. 4,*** for modtagelse heraf og ***kan, hvis det er praktisk muligt, rettidigt give*** den finansielle enhed ***relevant og forholdsmæssig*** feedback eller vejledning ***på højt niveau***, navnlig ved at ***stille alle relevante anonymiserede oplysninger og efterretninger om lignende trusler til rådighed,*** og kan drøfte, hvilke afhjælpende foranstaltninger der ***har fundet anvendelse*** over for den finansielle enhed, ***og*** måder, hvorpå negative virkninger kan minimeres ***og afbødes*** på tværs af den ***finansielle*** sektor. ***Med forbehold af den modtagne tilsynsmæssige feedback er de finansielle enheder fortsat fuldt ud ansvarlige for håndteringen og konsekvenserne af de IKT-relaterede hændelser, der er indberettet i henhold til artikel 19, stk. 1.***

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

2. ESA'erne aflægger via Det Fælles Udvalg baseret på et anonymiseret og samlet grundlag årligt rapport om ***større*** IKT-relaterede ***hændelser, hvis nærmere indhold stilles til rådighed af*** de kompetente myndigheder ***i overensstemmelse med artikel 19, stk. 6***, og der som minimum angiver antallet af ***større*** IKT-relaterede hændelser, deres karakter og indvirkning på finansielle enheders eller ***kunders*** operationer samt de afhjælpende foranstaltninger, der er truffet, og de omkostninger, der er afholdt.

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

Artikel 23

Operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser vedrørende kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter

De krav, der er fastlagt i dette kapitel, finder også anvendelse på operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser og større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, hvis de vedrører kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter.

Kapitel IV

Test af digital operationel modstandsdygtighed

Artikel 24

Generelle krav til gennemførelsen af test af digital operationel modstandsdygtighed

1. Med henblik på at vurdere beredskabet i forhold til ***håndtering af*** IKT-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger udarbejder, opretholder og gennemgår de finansielle enheder***, der ikke er mikrovirksomheder, under hensyntagen til kriterierne i artikel 4, stk. 2,*** et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed som en integrerende del af den i artikel 6 omhandlede ramme for IKT-risikostyring.

2. Programmet for test af digital operationel modstandsdygtighed skal omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26.

3. Når de finansielle enheder***, der ikke er mikrovirksomheder,*** gennemfører det i denne artikels stk. 1 omhandlede program for test af digital operationel modstandsdygtighed, følger de en risikobaseret tilgang***, idet de tager hensyn til kriterierne i artikel 4, stk. 2,*** under ***behørig hensyntagen*** til et IKT-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

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

5. De finansielle enheder***, der ikke er mikrovirksomheder,*** fastlægger procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres 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***, der ikke er mikrovirksomheder, sikrer, at der gennemføres passende test af*** alle IKT-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Artikel 25

Test af IKT-værktøjer og -systemer

1. Det i artikel 24 omhandlede program for test af den digitale operationelle modstandsdygtighed skal ***i overensstemmelse med kriterierne i artikel 4, stk. 2,*** indeholde bestemmelser om gennemførelse af ***af*** relevante test ***såsom*** sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

2. Værdipapircentraler og centrale modparter foretager sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og IKT-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

3. Mikrovirksomheder gennemfører de i stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af IKT-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til IKT-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Artikel 26

Avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT

1. Finansielle enheder***, der hverken er enheder som omhandlet i artikel 16, stk. 1, første afsnit, eller mikrovirksomheder, og som er*** identificeret i overensstemmelse med nærværende artikels stk. ***8, tredje afsnit,*** foretager mindst hvert tredje år avancerede test ved hjælp af TLPT. ***På grundlag af den finansielle enheds risikoprofil og under hensyntagen til de operationelle omstændigheder kan den kompetente myndighed om nødvendigt anmode den finansielle enhed om at reducere eller øge denne hyppighed.***

2. ***Hver trussels***baseret penetrations***test*** skal omfatte ***flere eller samtlige*** kritiske ***eller vigtige*** funktioner hos en finansiel enhed og foretages på live-produktionssystemer, der understøtter sådanne funktioner.

De finansielle enheder identificerer alle relevante underliggende IKT-systemer, -processer og -teknologier, der understøtter kritiske ***eller vigtige*** funktioner og alle relevante ***IKT-***tjenester, herunder ***dem, der understøtter kritiske eller vigtige*** funktioner og tjenester, der er blevet outsourcet eller udliciteret til tredjepartsudbydere af IKT-tjenester.

De finansielle enheder vurderer, hvilke kritiske eller vigtige funktioner, der skal være omfattet af TLPT. Resultatet af denne vurdering bestemmer det nøjagtige omfang af TLPT og valideres af de kompetente myndigheder.

3. Hvis tredjepartsudbydere af IKT-tjenester medtages i TLPT's anvendelsesområde, træffer den finansielle enhed de nødvendige foranstaltninger ***og sikkerhedsforanstaltninger*** for at sikre deltagelse af ***sådanne tredjeparts***udbydere ***af IKT-tjenester*** i TLPT***, og den har til enhver tid det fulde ansvar for at sikre overholdelse af denne forordning.***

4. Uden at det berører stk. 2, første og andet afsnit, kan den finansielle enhed og tredjepartsudbyderen af IKT-tjenester, hvis deltagelse af en tredjepartsudbyder af IKT-tjenester i TLPT ***som omhandlet i stk. 3 med rimelighed kan forventes at have en negativ indvirkning på kvaliteten eller sikkerheden af de tjenester, som tredjepartsudbyderen af IKT-tjenester leverer til kunder, der er enheder, som ikke henhører under denne forordnings anvendelsesområde, eller på fortroligheden af data forbundet med sådanne tjenester, skriftligt aftale, at tredjepartsudbyderen af IKT-tjenester direkte indgår kontraktlige ordninger med en ekstern tester med henblik på under ledelse af en udpeget finansiel enhed at foretage en samlet*** TLPT***, der omfatter flere finansielle enheder (samlet test), som tredjepartsudbyderen af IKT-tjenester leverer IKT-tjenester til.***

Denne samlede test skal omfatte en relevant vifte af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, som de finansielle enheder har udliciteret til den pågældende tredjepartsudbyder af IKT-tjenester. Den samlede test betragtes som en TLPT***, som gennemføres af de finansielle enheder, der deltager i den samlede test.***

Antallet af finansielle enheder, der deltager i den samlede test, afpasses behørigt under hensyntagen til kompleksiteten og typen af de involverede tjenester.

5. De finansielle enheder anvender ***i samarbejde med tredjepartsudbydere af IKT-tjenester og andre involverede parter, herunder testere, men med undtagelse af de kompetente myndigheder,*** effektive risikostyringskontroller for at ***mindske*** risici for potentielle virkninger ***på*** data, skade på aktiver og forstyrrelser af kritiske ***eller vigtige funktioner,*** tjenester eller operationer i den finansielle enhed selv, hos dens modparter eller i den finansielle sektor.

6. Efter afslutning af testen, og efter at der er opnået enighed om rapporter og udbedringsplaner, forelægger den finansielle enhed og, hvor det er relevant, de eksterne testere den ***myndighed, der er udpeget i overensstemmelse med stk. 9 eller 10, en sammenfatning af de relevante resultater, udbedringsplanerne og*** den dokumentation, som ***viser***, at TLPT er blevet gennemført i overensstemmelse med kravene.

7. Myndighederne forelægger de finansielle enheder en erklæring, der bekræfter, at testen er blevet gennemført i overensstemmelse med de krav, der fremgår af dokumentationen, for at give mulighed for gensidig anerkendelse af trusselsbaserede penetrationstest mellem de kompetente myndigheder. Den finansielle enhed underretter den relevante kompetente myndighed om erklæringen, sammenfatningen af de relevante resultater og udbedringsplanerne.

Med forbehold af denne erklæring har de finansielle enheder til enhver tid fortsat det fulde ansvar for virkningen af de i stk. 4 omhandlede test.

8. De finansielle enheder indgår en kontrakt med testere med henblik på at gennemføre TLPT i overensstemmelse med artikel 27. ***Hvis de finansielle enheder anvender interne testere med henblik på at gennemføre*** TLPT***, skal de indgå kontrakt med eksterne testere ved hver tredje test.***

Kreditinstitutter, som er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, må kun anvende eksterne testere i overensstemmelse med artikel 27, stk. 1, litra a)-e).

De kompetente myndigheder identificerer finansielle enheder, som ***pålægges*** at gennemføre TLPT ***under hensyntagen til kriterierne i artikel 4, stk. 2***, på grundlag af en vurdering af følgende:

a) virkningsrelaterede faktorer, navnlig i hvilket omfang de tjenester, der leveres, og de aktiviteter, der udføres af den finansielle enhed, indvirker på den finansielle sektor

b) eventuelle betænkeligheder vedrørende finansiel stabilitet, herunder den finansielle enheds systemiske karakter på EU-plan eller nationalt 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.

9. Medlemsstaterne kan udpege en fælles offentlig myndighed i den finansielle sektor til at være ansvarlig for TLPT***-relaterede spørgsmål i den finansielle sektor på nationalt plan og overdrager den alle kompetencer og opgaver med henblik herpå.***

10. I tilfælde af manglende udpegelse, jf. denne artikels stk. 9, og med forbehold af beføjelserne til at identificere de finansielle enheder, der skal gennemføre TLTP***, kan en kompetent myndighed delegere udførelsen af visse eller alle de opgaver, der er omhandlet i denne artikel og artikel 27, til en anden national myndighed i den finansielle sektor.***

11. ***ESA'erne*** udarbejder ***efter aftale med*** ECB ***fælles*** udkast til reguleringsmæssige tekniske standarder ***i overensstemmelse med TIBER-EU-rammen med henblik på*** yderligere at præcisere følgende*:*

a) de kriterier, der anvendes med henblik på anvendelsen ***af*** stk. 8***, andet afsnit***

b) krav til og standarder for anvendelsen af interne testere

c) kravene vedrørende:

i) omfanget af de i stk. 2 omhandlede TLPT

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

iii) resultaterne af testen, testens afslutnings- og udbedringsfaser

d) den type tilsynsmæssigt ***og andet relevant*** samarbejde, der er nødvendigt for at gennemføre TLPT, ***og for at lette den gensidige anerkendelse af den pågældende test,*** i forbindelse med finansielle enheder, ***der*** opererer i mere end én medlemsstat, således at der sikres et passende niveau af tilsynsmæssig deltagelse og en fleksibel gennemførelse for at tage højde for særlige forhold i finansielle delsektorer eller lokale finansielle markeder.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de behørigt hensyn til eventuelle særlige kendetegn, der opstår som følge af aktiviteternes særlige karakter på tværs af forskellige sektorer for finansielle tjenesteydelser.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [***18 måneder efter*** datoen ***for denne forordnings*** ikrafttræden].

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit 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.

Artikel 27

Krav til testere ***vedrørende gennemførelsen af*** TLPT

1. De finansielle enheder må kun anvende testere til gennemførelsen af TLPT, 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 ***og*** red team-test

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

d) ▌- afgiver en uafhængig garanti for eller en revisionsrapport vedrørende forsvarlig risikostyring i forbindelse med gennemførelsen af TLPT, 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.

2. Når de anvender interne testere, skal de finansielle enheder i tillæg til kravene i stk. 1 sikre, at følgende betingelser er opfyldt:

a) en sådan anvendelse er blevet godkendt af den relevante kompetente myndighed eller den fælles offentlige myndighed, som er udpeget i overensstemmelse med artikel 26, stk. 9 og 10

b) den relevante kompetente myndighed har efterprøvet, at den finansielle enhed har afsat tilstrækkelige særlige ressourcer, og sikret, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser, og

c) formidleren af trusselsefterretninger er ekstern i forhold til den finansielle enhed.

3. De finansielle enheder sikrer, at der i de ***kontrakter***, der indgås med eksterne testere, kræves en forsvarlig forvaltning af resultaterne af TLPT, og at enhver databehandling heraf, herunder enhver form for generering, lagring, aggregering, udkast, rapportering, kommunikation eller destruktion, ikke medfører risici for den finansielle enhed.

Kapitel V
Styring af IKT-tredjepartsrisici

Afdeling I
Centrale principper for forsvarlig styring af IKT-tredjepartsrisici

Artikel 28
Generelle principper

1. De finansielle enheder styrer IKT-tredjepartsrisiko som en integreret del af IKT-risiko inden for deres ramme for IKT-risikostyring som omhandlet i artikel 6, stk. 1, og i overensstemmelse med følgende principper:

a) 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 finansiel tjenesteydelsesret

b) De finansielle enheders styring af IKT-tredjepartsrisiko skal gennemføres under hensyntagen til proportionalitetsprincippet, idet følgende tages i betragtning:

i) ***karakteren,*** omfanget, kompleksiteten og betydningen af den IKT-relaterede afhængighed

ii) 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 ***tilgængeligheden*** af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

2. Finansielle enheder***, der hverken er enheder som omhandlet i artikel 16, stk. 1, første afsnit, eller er mikrovirksomheder,*** vedtager og gennemgår regelmæssigt en strategi for IKT-tredjepartsrisiko som led i deres ramme for IKT-risikostyring, idet de tager hensyn til den strategi med flere udbydere, der er omhandlet i artikel 6, stk. 9***, hvor det er relevant***. Strategien for IKT-tredjepartsrisiko skal omfatte en politik for brugen af IKT-tjenester***, der understøtter kritiske eller vigtige funktioner***, og som leveres af tredjepartsudbydere af IKT-tjenester, og skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet gennemgår ***på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne*** regelmæssigt de risici, der er konstateret i forbindelse ***med kontraktlige ordninger for brugen af IKT-tjenester, der understøtter*** kritiske eller vigtige funktioner.

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

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

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

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 ***enhver*** planlagt ***kontraktlig ordning for brugen af IKT-tjenester, der understøtter*** kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

4. Inden de finansielle enheder indgår en kontraktlig ordning for brugen af IKT-tjenester, skal de:

a) vurdere, om den kontraktlige ordning omfatter ***brugen af IKT-tjenester, der understøtter*** 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***, jf. artikel 29***

d) foretage fornøden due diligence over for potentielle tredjepartsudbydere af IKT-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af IKT-tjenester er egnet

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

5. De finansielle enheder må kun indgå kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester, der overholder ▌ passende ***standarder for informationssikkerhed. Når disse kontraktlige ordninger vedrører kritiske eller vigtige funktioner, tager de finansielle enheder, inden de indgår ordningerne, behørigt hensyn til tredjepartsudbydere af IKT-tjenesters brug af de seneste*** informationssikkerhedsstandarder af højeste kvalitet.

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

Hvis de kontraktlige ordninger***, der indgås med tredjepartsudbydere af IKT-tjenester for brugen af IKT-tjenester,*** indebærer ▌ en høj grad af ***teknisk*** kompleksitet, efterprøver den finansielle enhed, om revisorerne, hvad enten de er interne, ▌ eksterne ***eller en pulje af revisorer,*** besidder de nødvendige færdigheder og den nødvendige viden til effektivt at udføre de relevante revisioner og vurderinger.

7. De finansielle enheder sikrer, at de kontraktlige ordninger for brugen af IKT-tjenester som minimum ***kan*** opsiges i enhver af følgende situationer:

a) ***væsentlig*** overtrædelse begået af tredjepartsudbyderen af IKT-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår

b) forhold, der er identificeret under overvågningen af IKT-tredjepartsrisiko, 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) dokumenterede svagheder hos tredjepartsudbyderen af IKT-tjenester***, som vedrører dennes*** samlede IKT-risikostyring, og navnlig i den måde, hvorpå denne garanterer ***tilgængeligheden, autenticiteten, integriteten og fortroligheden*** af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger

d) hvis den kompetente myndighed ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

8. ***For så vidt angår IKT-tjenester, der understøtter kritiske eller vigtige funktioner,*** indfører ***de finansielle*** enheder exitstrategier **[…]**. ***Exitstrategierne skal*** tage højde for de risici, der kan opstå hos tredjeparts***udbydere*** af IKT-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede IKT-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af IKT-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende IKT-tjenester ***eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester i en af de i stk. 7 anførte situationer***.

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 de leverede tjenester til kunder lider skade.

Exitplanerne skal være omfattende, veldokumenterede og***, i overensstemmelse med kriterierne i artikel 4, stk. 2,*** testet i tilstrækkeligt omfang ***samt gennemgået regelmæssigt***.

De finansielle enheder identificerer alternative løsninger og udarbejder overgangsplaner, således at de kan fratage tredjepartsudbyderen af IKT-tjenester de udliciterede IKT-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt.

De finansielle enheder indfører passende beredskabsforanstaltninger for at opretholde driftsstabiliteten i tilfælde af de i første afsnit omhandlede omstændigheder.

9. ESA'erne udarbejder via Det Fælles Udvalg udkast til gennemførelsesmæssige tekniske standarder for at fastlægge standardmodeller med henblik på det i stk. 3 omhandlede ***register*** over ***oplysninger, herunder oplysninger, som er fælles for alle kontraktlige ordninger for brugen af IKT-tjenester***. ESA'erne forelægger disse udkast til gennemførelsesmæssige tekniske standarder for Kommissionen senest den ... [***12 måneder*** efter datoen for denne forordnings ikrafttræden].

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

10. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige ***tekniske*** standarder ▌ for yderligere at præcisere det detaljerede indhold af den i stk. 2 omhandlede politik vedrørende de kontraktlige ordninger for brugen af IKT-tjenester***, der understøtter kritiske eller vigtige funktioner,*** som leveres af tredjepartsudbydere af IKT-tjenester ▌.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [***12 måneder*** efter datoen ***for denne forordnings*** ikrafttræden].

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit 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.

Artikel 29

Foreløbig vurdering af IKT-koncentrationsrisiko på enhedsniveau

1. Når finansielle enheder foretager identifikation og vurdering af de risici, der er omhandlet i artikel 28, stk. 4, litra c), tager de også hensyn til, hvorvidt den påtænkte indgåelse 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) indgåelse af 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 fordele og omkostninger ved alternative løsninger såsom brug 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 de kontraktlige ordninger for brugen af IKT-tjenester***, der understøtter kritiske eller vigtige funktioner,*** omfatter muligheden for, at en tredjepartsudbyder af IKT-tjenester giver IKT-tjenester, der understøtter en kritisk eller vigtig funktion, videre i underentreprise til andre tredjepartsudbydere af IKT-tjenester, afvejer de finansielle enheder de fordele og risici, der kan opstå i forbindelse med en sådan underentreprise, navnlig hvis der er tale om en IKT-underleverandør med hjemsted i et tredjeland.

Hvis de kontraktlige ordninger vedrører IKT-tjenester***, der understøtter kritiske eller vigtige funktioner*** ▌, tager de finansielle enheder ***behørigt*** hensyn til ▌ de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af IKT-tjenester går konkurs, ***samt*** eventuelle ***begrænsninger***, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data.

▌

Hvis der er indgået kontraktlige ordninger for brug 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 til de i andet afsnit omhandlede forhold også hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland.

Hvis de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, indeholder bestemmelser om underentreprise, vurderer ***de finansielle*** enheder, hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed.

Artikel 30

Centrale kontraktbestemmelser

1. Rettigheder og forpligtelser for den finansielle enhed og for tredjepartsudbyderen af IKT-tjenester skal fordeles klart og fastlægges ▌ skriftligt. Den samlede kontrakt ***skal omfatte service***niveauaftaler ***og*** dokumenteres i ét skriftligt dokument, som parterne skal have adgang til på papir, eller i et ***dokument i et andet varigt*** og tilgængeligt format, som kan downloades.

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

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

   b) de steder***, navnlig de regioner eller lande,*** hvor de udliciterede funktioner og ***IKT-***tjenester eller funktionerne og ***IKT-***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 disse steder

c) bestemmelser om ***tilgængelighed, autenticitet, integritet og fortrolighed*** med hensyn til ***data***beskyttelse***, herunder*** personoplysninger ▌

d) ***bestemmelser*** om sikring af adgang, ***genopretning*** og tilbagesendelse i et lettilgængeligt 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***

e***)*** ***beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf*** ▌

▌

f) ***forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den IKT-tjeneste, som leveres til den finansielle enhed***

g) 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

h) opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders ***og afviklingsmyndighedernes forventninger***

▌

i) betingelserne for deltagelse af tredjepartsudbydere af IKT-tjenester i de finansielle enheders programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6.

3. De kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, skal ud over de elementer, der er omhandlet i stk. 2, mindst omfatte følgende***:***

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

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

c) krav til tredjepartsudbyderen af IKT-tjenester om at gennemføre og teste beredskabsplaner og indføre IKT-sikkerhedsforanstaltninger, -værktøjer og -politikker, ***som giver et passende niveau af*** sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme

d) ***forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27***

e) retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af IKT-tjenester leverer, hvilket indebærer følgende:

i) den finansielle enheds eller en udpeget tredjeparts ***og den kompetente myndigheds uindskrænkede*** ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation ***på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af IKT-tjenesters operationer***, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker

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

iii) forpligtelsen for ***tredjepartsudbyderen af IKT-tjenester*** 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

iv) forpligtelsen til at give nærmere oplysninger om omfanget af, ***de procedurer, som skal følges,*** og hyppigheden af ***sådanne inspektioner og*** revisioner

▌

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

i) i løbet af hvilken tredjepartsudbyderen af IKT-tjenester fortsat leverer de respektive funktioner eller ***IKT-***tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed ***eller sikre en effektiv afvikling eller omstrukturering heraf***

ii) som giver den finansielle enhed mulighed for at ***migrere*** til en anden tredjepartsudbyder af IKT-tjenester eller skifte til ***interne*** løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Uanset litra e) kan tredjepartsudbyderen af IKT-tjenester og den finansielle enhed, som er en mikrovirksomhed, beslutte, at den finansielle enheds ret til adgang, inspektion og revision kan delegeres 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.

4. Når finansielle enheder og tredjepartsudbydere af IKT-tjenester forhandler om kontraktlige ordninger, overvejer de anvendelsen af standardkontraktbestemmelser, som ***de offentlige myndigheder*** har udviklet til specifikke tjenester.

5. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige tekniske standarder med henblik på yderligere at præcisere de i stk. 2, litra a), omhandlede elementer, som en finansiel enhed skal fastlægge og vurdere, når den giver IKT-tjenester, der understøtter kritiske eller vigtige funktioner, i underentreprise.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den ... [***18 måneder*** efter datoen ***for denne forordnings*** ikrafttræden].

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 forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Afdeling II

Tilsynsramme for kritiske tredjepartsudbydere af IKT-tjenester

Artikel 31

Udpegelse af kritiske tredjepartsudbydere af IKT-tjenester

1. ESA'erne skal via Det Fælles Udvalg og efter henstilling fra det tilsynsforum, der er oprettet i henhold til artikel 32, stk. 1,

   a) udpege de tredjepartsudbydere af IKT-tjenester, der er kritiske for finansielle enheder ***efter en vurdering, der tager*** hensyn til kriterierne i stk. 2

   b) som ▌ ledende tilsynsførende for hver kritisk tredjepartsudbyder af IKT-tjenester ***udpege den ESA, der i overensstemmelse med*** forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 eller (EU) nr. 1095/2010 er ansvarlig ***for de finansielle enheder, der tilsammen besidder den største andel samlede aktiver*** ud af værdien af ▌ de samlede aktiver for alle de finansielle enheder, der benytter sig af tjenester fra den ***pågældende*** kritiske tredjepartsudbyder af IKT-tjenester, således som det fremgår af ***summen af*** de individuelle balancer ▌ for disse finansielle enheder.

2. Den udpegelse, der er omhandlet i stk. 1, litra a), skal ***i forbindelse med IKT-tjenester, der leveres af tredjepartsudbyderen af IKT-tjenester,*** 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 og den samlede værdi af aktiverne hos de*** finansielle enheder, som den pågældende tredjepartsudbyder af IKT-tjenester leverer tjenester til

b) den systemiske karakter eller betydning af de finansielle enheder, der er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester, 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 nr. 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, 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 i forbindelse med helt eller delvist at migrere de relevante data og arbejdsbyrden fra den pågældende tredjepartsudbyder af IKT-tjenester til en anden tredjepartsudbyder af IKT-tjenester, enten på grund af betydelige finansielle omkostninger, tid eller andre ressourcer, som migreringen kan kræve, eller en øget IKT-risiko eller andre operationelle risici, som den finansielle enhed kan blive eksponeret for ved en sådan migrering.

3. ***Hvis*** tredjepartsudbyderen af IKT-tjenester ***indgår i en koncern, tages kriterierne i stk. 2 i betragtning i forhold til de IKT-***tjenester, der ***leveres af koncernen som helhed.***

4. ***Kritiske tredjepartsudbydere af IKT-tjenester, som indgår i en koncern, udpeger én juridisk person som koordineringspunkt for at sikre en passende repræsentation og kommunikation med den ledende tilsynsførende.***

5. ***Den ledende tilsynsførende underretter tredjepartsudbyderen af IKT-tjenester om resultatet af den vurdering, der fører til udpegelsen, jf. stk. 1, litra a). Senest seks uger efter datoen for underretningen kan tredjepartsudbyderen af IKT-tjenester forelægge den ledende tilsynsførende en begrundet erklæring med alle relevante oplysninger med henblik på vurderingen. Den ledende tilsynsførende tager den begrundede erklæring i betragtning og kan anmode om, at der forelægges yderligere oplysninger inden for 30 kalenderdage efter modtagelsen af en sådan erklæring.***

Efter at have udpeget en tredjepartsudbyder af IKT-tjenester som kritisk underretter ESA'erne gennem Det Fælles Udvalg tredjepartsudbyderen af IKT-tjenester om en sådan udpegelse og om startdatoen for, hvornår de reelt vil være omfattet af tilsynsaktiviteter. Denne startdato må ikke være senere end en måned efter underretningen. Tredjepartsudbyderen af IKT-tjenester underretter de finansielle enheder, som de leverer tjenester til, om deres udpegelse som kritiske.

6. Kommissionen tillægges beføjelser til at vedtage ***en*** delegeret ***retsakt*** i overensstemmelse med artikel 57 for at ***supplere denne forordning ved yderligere at præcisere de*** kriterier, der er omhandlet i denne artikels stk. 2***, senest den … [18 måneder fra datoen for denne forordnings ikrafttræden]***.

7. Den udpegelse, der er omhandlet i stk. 1, litra a), må først anvendes, når Kommissionen har vedtaget en delegeret retsakt i overensstemmelse med stk. 6.

8. Den udpegelse, der er omhandlet i stk. 1, litra a), finder ikke anvendelse på følgende***:***

i) finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder

ii) 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

iii) koncerninterne udbydere af IKT-tjenester

iv) tredjepartsudbydere af IKT-tjenester, der udelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheder, der kun er aktive i den pågældende medlemsstat.

9. ESA'erne udarbejder, offentliggør og ajourfører årligt via Det Fælles Udvalg listen over kritiske tredjepartsudbydere af IKT-tjenester på EU-plan.

10. Med henblik på stk. 1, litra a), videregiver de kompetente myndigheder på et årligt og aggregeret grundlag de rapporter, der er omhandlet i artikel 28, stk. 3, ***tredje afsnit***, til det tilsynsforum, der er oprettet i henhold til artikel 32. Tilsynsforummet vurderer finansielle enheders afhængighed af tredjepartsudbydere af IKT-tjenester på grundlag af oplysninger, som det modtager fra de kompetente myndigheder.

11. ***De*** tredjepartsudbydere af IKT-tjenester, der ikke er opført på den i stk. 9 omhandlede liste, kan anmode om at blive ***udpeget som kritiske i overensstemmelse med stk. 1, litra a)***.

Med henblik på første afsnit indgiver tredjepartsudbyderen af IKT-tjenester en begrundet anmodning til EBA, ESMA eller EIOPA, som via Det Fælles Udvalg træffer afgørelse, om den pågældende tredjepartsudbyder af IKT-tjenester ***skal udpeges som kritisk*** i overensstemmelse med stk. 1, litra a).

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

12. Finansielle enheder benytter ***kun tjenester, der udbydes af*** en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, ***der er*** udpeget som kritisk i overensstemmelse med stk. 1, litra a), hvis ***sidstnævnte har*** etableret ***en dattervirksomhed*** i Unionen ***senest 12 måneder efter udpegelsen***.

13. Den i stk. 12 omhandlede kritiske tredjepartsudbyder af IKT-tjenester underretter den ledende tilsynsførende om eventuelle ændringer af ledelsesstrukturen i den dattervirksomhed, der er etableret i Unionen.

Artikel 32

Tilsynsrammens struktur

1. Det Fælles Udvalg opretter i overensstemmelse med artikel ***57, stk. 1,*** i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 tilsynsforummet som et underudvalg med henblik på at støtte det arbejde, der udføres i Det Fælles Udvalg og af den ledende tilsynsførende, der er omhandlet i artikel 31, stk. 1, litra b), med hensyn til IKT-tredjepartsrisiko på tværs af finansielle sektorer. Tilsynsforummet udarbejder udkast til fælles holdninger og udkast til fælles retsakter vedtaget af Det Fælles Udvalg inden for dette område.

   Tilsynsforummet drøfter regelmæssigt relevante udviklingstendenser vedrørende IKT-risiko og -sårbarheder og fremmer en konsekvent tilgang til overvågning af IKT-tredjepartsrisiko på EU-plan.

2. Tilsynsforummet foretager på årsbasis en kollektiv vurdering af resultaterne og konklusionerne fra ***de tilsyns***aktiviteter, 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-koncentrationsrisiko og undersøge foranstaltninger til modvirkning af risikoafsmitning på tværs af sektorer.

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

4. Tilsynsforummet er sammensat af:

a) formændene for ESA'erne

b) én repræsentant på højt niveau fra det nuværende personale i den relevante kompetente myndighed, ***jf. artikel 46***, fra hver medlemsstat

c) ***de*** administrerende direktører for hver ESA og en repræsentant fra henholdsvis Kommissionen, ESRB, ECB og ENISA – som observatører

d) ***hvor det er hensigtsmæssigt, yderligere en repræsentant for en kompetent myndighed, jf. artikel 46, fra hver medlemsstat som observatør***

e) ***hvor det er relevant, en repræsentant for de kompetence myndigheder udpeget eller oprettet i overensstemmelse med direktiv (EU) …/…[+], som har ansvar for tilsynet med en væsentlig eller vigtig enhed, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester, som observatør***

Tilsynsforummet kan, hvor det er hensigtsmæssigt, rådføre sig med uafhængige eksperter, der er udpeget i overensstemmelse med stk. 6.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

5. Hver medlemsstat udpeger den relevante kompetente myndighed, hvis ansatte skal være den repræsentant på højt niveau, der er omhandlet i stk. 4, første afsnit, litra b), og underretter den ledende tilsynsførende herom.

ESA'erne offentliggør på deres websted listen over højtstående repræsentanter fra det nuværende personale i den relevante kompetente myndighed udpeget af medlemsstaterne.

6. De uafhængige eksperter, der er omhandlet i stk. 4, andet afsnit, udpeges af tilsynsforummet fra en pulje af eksperter, der udvælges efter en offentlig og gennemsigtig ansøgningsproces.

De uafhængige eksperter udpeges for en toårig periode på grundlag af deres ekspertise i finansiel stabilitet, digital operationel modstandsdygtighed og IKT-sikkerhedsspørgsmål. De handler uafhængigt og objektivt udelukkende i Unionens interesse som helhed og må ikke søge eller modtage instrukser fra EU-institutioner eller -organer, medlemsstaters regeringer eller noget andet offentligt eller privat organ.

7. I overensstemmelse med artikel 16 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 udsteder ESA'erne ***senest den … [18 måneder efter denne forordnings ikrafttræden]*** med henblik på denne afdeling retningslinjer for samarbejdet mellem ESA'erne og de kompetente myndigheder om de nærmere procedurer og betingelser for tildelingen og varetagelsen af opgaver mellem de kompetente myndigheder og ESA'erne samt nærmere oplysninger om den informationsudveksling, der er nødvendig for, at de kompetente myndigheder kan sikre opfølgning af henstillinger, jf. artikel 35, stk. 1, litra d), rettet til kritiske tredjepartsudbydere af IKT-tjenester.

8. Kravene i denne afdeling berører ikke anvendelsen af ***direktiv (EU) .../...***[+] og af andre EU-regler om tilsyn, som finder anvendelse på udbydere af cloudcomputingtjenester.

9. ESA'erne forelægger gennem Det Fælles Udvalg og på grundlag af det forberedende arbejde, der udføres af tilsynsforummet, årligt en rapport om anvendelsen af denne afdeling for Europa-Parlamentet, Rådet og Kommissionen.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

Artikel 33

Den ledende tilsynsførendes opgaver

1. Den ***ledende tilsynsførende, der er udpeget i overensstemmelse med artikel 31, stk. 1, litra b), fører tilsyn med de tildelte kritiske tredjepartsudbydere af IKT-tjenester og er med henblik på alle spørgsmål vedrørende tilsynet det primære kontaktpunkt for disse kritiske tredjepartsudbydere af IKT-tjenester***.

2. Den ledende tilsynsførende vurderer ***med henblik på stk. 1***, om hver enkelt kritisk tredjepartsudbyder af IKT-tjenester har indført omfattende, robuste og effektive regler, procedurer, mekanismer og ordninger til styring af den IKT-risiko, som den kan udsætte finansielle enheder for.

Den vurdering, der er omhandlet i første afsnit, skal primært fokusere på de IKT-tjenester, som leveres af den kritiske tredjepartsudbyder af IKT-tjenester, og som understøtter finansielle enheders kritiske eller vigtige funktioner. Hvis det er nødvendigt for at imødegå alle relevante risici, skal denne vurdering omfatte IKT-tjenester, der understøtter andre funktioner end dem, der er kritiske eller vigtige.

3. Den i stk. 2 omhandlede vurdering dækker 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 – ***tilgængelighed, autenticitet, integritet eller fortrolighed***

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

c) risikostyringsprocesser, herunder politikker for IKT-risikostyring, politik for IKT-driftsstabilitet og planer for IKT-***indsats*** og -genopretning

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

e) identifikation, overvågning og hurtig indberetning af ***væsentlige*** 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) test 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.

4. På grundlag af den i stk. 2 omhandlede vurdering ***og i samordning med det fælles tilsynsnetværk, der er omhandlet i artikel 34, stk. 1***, vedtager den ledende tilsynsførende en klar, detaljeret og begrundet individuel tilsynsplan, ***der beskriver de årlige tilsynsmål og de vigtigste tilsynstiltag, der er planlagt*** for hver enkelt kritisk tredjepartsudbyder af IKT-tjenester. Denne plan skal hvert år meddeles den kritiske tredjepartsudbyder af IKT-tjenester.

Forud for vedtagelsen af tilsynsplanen skal den ledende tilsynsførende meddele udkastet til tilsynsplan til den kritiske tredjepartsudbyder af IKT-tjenester.

Efter modtagelsen af udkastet til tilsynsplan kan den kritiske tredjepartsudbyder af IKT-tjenester inden for 15 kalenderdage indsende en begrundet erklæring, der dokumenterer den forventede virkning på kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og, hvis det er relevant, udarbejde løsninger til at afbøde risici.

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

Artikel 34

Operationel koordinering mellem ledende tilsynsførende

1. For at sikre en konsekvent tilgang til tilsynsaktiviteter og med henblik på at muliggøre koordinerede generelle tilsynsstrategier og sammenhængende operationelle tilgange og arbejdsmetoder opretter de tre ledende tilsynsførende, der er udpeget i overensstemmelse med artikel 31, stk. 1, litra b), et fælles tilsynsnetværk, der skal koordinere indbyrdes i forbindelse med de forberedende faser og koordinere udførelsen af tilsynsaktiviteter med hensyn til deres respektive kritiske tredjepartsudbydere af IKT-tjenester, der føres tilsyn med, og i forbindelse med eventuelle tiltag, der måtte være nødvendige i henhold til artikel 42.

2. Med henblik på stk. 1 udarbejder de ledende tilsynsførende en fælles tilsynsprotokol, der præciserer de nærmere procedurer, der skal følges for at gennemføre den daglige koordinering og sikre hurtige udvekslinger og reaktioner. Protokollen revideres regelmæssigt for at afspejle de operationelle behov, navnlig de praktiske tilsynsordningers udvikling.

3. De ledende tilsynsførende kan på ad hoc-basis anmode ECB og ENISA om at yde teknisk rådgivning, udveksle praktiske erfaringer eller deltage i specifikke koordineringsmøder i det fælles tilsynsnetværk.

Artikel 35

Den ledende tilsynsførendes beføjelser

1. Med henblik på varetagelsen af de i denne afdeling omhandlede opgaver tillægges den ledende tilsynsførende følgende beføjelser med hensyn til de kritiske tredjepartstjenesteudbydere af IKT-tjenester:

a) at anmode om alle relevante oplysninger og dokumentation i overensstemmelse med artikel 37

b) at foretage generelle undersøgelser og inspektioner i overensstemmelse med henholdsvis artikel 38 og 39

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

d) at udstede henstillinger vedrørende de områder, der er omhandlet i artikel 33, stk. 3, og navnlig følgende:

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

ii) anvendelse af betingelser og vilkår, herunder den tekniske gennemførelse heraf, i henhold til hvilke de kritiske tredjepartsudbydere af IKT-tjenester leverer tjenester til finansielle enheder, og som den ledende tilsynsførende skønner relevante for at forhindre, at der genereres single points of failure, eller at disse forstærkes, eller for at minimere de eventuelle systemiske virkninger på tværs af Unionens finansielle sektor i tilfælde af IKT-koncentrationsrisici

iii) eventuelle planlagte underentrepriser, hvor den ledende tilsynsførende på baggrund af undersøgelsen af de oplysninger, der er indhentet i overensstemmelse med artikel 37 og 38, skønner, at videregivelse i underentreprise, herunder ordninger for ***underentrepriser***, som de kritiske tredjepartsudbydere af IKT-tjenester planlægger at indgå med tredjepartsudbydere af IKT-tjenester eller med IKT-underleverandører med hjemsted i et tredjeland, kan udløse risici for den finansielle enheds levering af tjenester eller risici for den finansielle stabilitet

iv) at afholde sig fra at indgå en ordning om videregivelse i underentreprise, når følgende kumulative betingelser er opfyldt:

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

– underentreprisen vedrører kritiske eller vigtige funktion for den finansielle enhed, ***og***

– ***den ledende tilsynsførende vurderer, at anvendelsen af en sådan underentreprise udgør en klar og alvorlig risiko for den finansielle stabilitet i Unionen eller for finansielle enheder, herunder finansielle enheders evne til at overholde tilsynskravene.***

Tredjepartsudbydere af IKT-tjenester videregiver med henblik på dette litras nr. iv) ved brug af den model, der er omhandlet i artikel 41, stk. 1, litra b), oplysninger om underentrepriser til den ledende tilsynsførende.

2. Ved udøvelsen af de beføjelser, der er omhandlet i denne artikel, skal den ledende tilsynsførende:

a) sikre regelmæssig koordinering inden for det fælles tilsynsnetværk og navnlig tilstræbe konsekvente tilgange, alt efter hvad der er relevant, med hensyn til tilsynet med kritiske tredjepartsudbydere af IKT-tjenester

b) tage behørigt hensyn til den ramme, der er fastsat ved direktiv (EU) .../...[+], og om nødvendigt høre de relevante kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med nævnte direktiv, for at undgå overlapning af tekniske og organisatoriske foranstaltninger, som kan finde anvendelse på kritiske tredjepartsudbydere af IKT-tjenester i henhold til nævnte direktiv

c) så vidt muligt tilstræbe at minimere risikoen for forstyrrelser i tjenester, som kritiske tredjepartsudbydere af IKT-tjenester leverer til kunder, der er enheder, som ikke er omfattet af denne forordnings anvendelsesområde.

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

Inden den ledende tilsynsførende udsteder henstillinger i overensstemmelse med stk. 1, litra d), giver den tredjepartsudbyderen af IKT-tjenester mulighed for inden for 30 kalenderdage at fremlægge relevante oplysninger, der dokumenterer den forventede virkning på kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og, hvis det er relevant, udarbejde løsninger til at afbøde risici.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

4. Den ledende tilsynsførende underretter det fælles tilsynsnetværk om resultatet af udøvelsen af de beføjelser, der er omhandlet i stk. 1, litra a) og b). Den ledende tilsynsførende videregiver uden unødig forsinkelse de rapporter, der er omhandlet i stk. 1, litra c), til det fælles tilsynsnetværk og til de kompetente myndigheder for de finansielle enheder, der anvender IKT-tjenester leveret af den pågældende kritiske tredjepartsudbyder af IKT-tjenester.

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

6. ***I tilfælde af hel eller delvis manglende overholdelse af de foranstaltninger, der skal træffes i henhold til udøvelsen af beføjelserne i stk. 1, litra a), b) og c), og efter udløbet af en periode på mindst 30 kalenderdage fra den dato, hvor den kritiske tredjepartsudbyder af IKT-tjenester har modtaget underretning om de respektive foranstaltninger, vedtager*** den ledende tilsynsførende ***en afgørelse, der pålægger*** en tvangsbøde for at tvinge den kritiske tredjepartsudbyder af IKT-tjenester til at efterleve ***disse foranstaltninger***.

7. De i stk. 6 omhandlede tvangsbøder pålægges dagligt, indtil der er opnået efterlevelse, og i højst seks måneder efter meddelelsen af afgørelsen om at pålægge den kritiske tredjepartsudbyder af IKT-tjenester en tvangsbøde.

8. Størrelsen af tvangsbøderne, der beregnes fra den dato, der er anført i afgørelsen om pålæggelse af tvangsbøder, udgør ***op til*** 1 % af den kritiske tredjepartsudbyder af IKT-tjenesters gennemsnitlige daglige omsætning på verdensplan i det foregående regnskabsår. ***Ved fastsættelsen af tvangsbødens størrelse tager den ledende tilsynsførende hensyn til følgende kriterier vedrørende manglende overholdelse af de foranstaltninger, der er omhandlet i stk. 6:***

   i) den manglende overholdelses grovhed og varighed

   ii) hvorvidt den manglende overholdelse er forsætlig eller skyldes uagtsomhed

iii) niveauet af samarbejde mellem tredjepartsudbyderen af IKT-tjenester og den ledende tilsynsførende.

Med henblik på første afsnit skal den ledende tilsynsførende for at sikre en konsekvent tilgang deltage i samråd inden for det fælles tilsynsnetværk.

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

10. ***Den ledende tilsynsførende*** 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.

11. Inden der pålægges tvangsbøder i henhold til stk. 6, giver den ledende tilsynsførende repræsentanter for den kritiske tredjepartsudbyder af IKT-***tjenester***, som er genstand for proceduren, mulighed for at blive hørt om de konstaterede forhold og baserer sine afgørelser udelukkende på forhold, 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. Den kritiske tredjepartsudbyder af IKT-tjenester, der er genstand for proceduren, har ret til aktindsigt i dossieret 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 36

Den ledende tilsynsførendes udøvelse af beføjelser uden for Unionen

1. Når tilsynsmålene ikke kan nås ved at interagere med den dattervirksomhed, der er oprettet med henblik på artikel 31, stk. 12, eller ved at udøve tilsynsaktiviteter i lokaler i Unionen, kan den ledende tilsynsførende udøve de i de følgende bestemmelser omhandlede beføjelser i ethvert lokale i et tredjeland, som med henblik på levering af tjenester til finansielle enheder i Unionen ejes eller på nogen måde anvendes af en kritisk tredjepartsudbyder af IKT-tjenester i forbindelse med dennes forretningsaktiviteter, funktioner eller tjenester, herunder alle administrative, forretningsmæssige eller operationelle kontorer, lokaler, arealer, bygninger eller andre ejendomme:

a) i artikel 35, stk. 1, litra a), og

b) i artikel 35, stk. 1, litra b), i overensstemmelse med artikel 38, stk. 2, litra a), b) og d), og artikel 39, stk. 1, og artikel 39, stk. 2, litra a).

De i første afsnit omhandlede beføjelser kan udøves med forbehold af overholdelse af alle følgende betingelser:

i) den ledende tilsynsførende anser det for nødvendigt, at der foretages inspektion i et tredjeland, for at denne fuldt ud og effektivt kan udføre sine opgaver i henhold til denne forordning

ii) inspektionen i et tredjeland er direkte knyttet til leveringen af IKT-tjenester til finansielle enheder i Unionen

iii) den pågældende kritiske tredjepartsudbyder af IKT-tjenester giver sit samtykke til, at der foretages en inspektion i et tredjeland, og

iv) den relevante myndighed i det pågældende tredjeland er blevet officielt underrettet af den ledende tilsynsførende og har ikke gjort indsigelse herimod.

2. Uden at det berører EU-institutionernes og medlemsstaternes respektive beføjelser, indgår EBA, ESMA eller EIOPA med henblik på stk. 1 administrative samarbejdsordninger med den relevante myndighed i tredjelandet med henblik på at gøre det muligt for den ledende tilsynsførende og det team, den har udpeget til opgaven i det pågældende tredjeland, at foretage gnidningsløse inspektioner i det pågældende tredjeland. Disse samarbejdsordninger må ikke skabe retlige forpligtelser for Unionen og dens medlemsstater og heller ikke forhindre medlemsstaterne og deres kompetente myndigheder i at indgå bilaterale eller multilaterale aftaler med disse tredjelande og deres relevante myndigheder.

Disse samarbejdsordninger præciserer som minimum følgende elementer:

a) procedurerne for koordinering af de tilsynsaktiviteter, der udføres i henhold til denne forordning, og enhver tilsvarende overvågning af IKT-tredjepartsrisiko i den finansielle sektor, der udøves af den relevante myndighed i det pågældende tredjeland, herunder nærmere oplysninger om videreformidling af sidstnævntes samtykke til, at den ledende tilsynsførende og dens udpegede team kan foretage generelle undersøgelser og inspektioner på stedet som omhandlet i stk. 1, første afsnit, på det område, der hører under dens jurisdiktion

b) mekanismen for overførsel af relevante oplysninger mellem EBA, ESMA eller EIOPA og den relevante myndighed i det pågældende tredjeland, navnlig i forbindelse med oplysninger, som den ledende tilsynsførende kan anmode om i henhold til artikel 37

c) mekanismerne for øjeblikkelig underretning fra den relevante myndighed i det pågældende tredjeland til EBA, ESMA eller EIOPA om tilfælde, hvor en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, der er udpeget som kritisk i henhold til artikel 31, stk. 1, litra a), anses for at have overtrådt de krav, som den er forpligtet til at opfylde i henhold til det pågældende tredjelands gældende ret, når den leverer tjenester til finansieringsinstitutter i det pågældende tredjeland, samt de anvendte afhjælpende foranstaltninger og sanktioner

d) regelmæssig overførsel af opdateringer om regulerings- eller tilsynsmæssig udvikling vedrørende overvågning af IKT-tredjepartsrisiko for finansieringsinstitutter i det pågældende tredjeland

e) nærmere oplysninger, der om nødvendigt gør det muligt for én repræsentant for den relevante tredjelandsmyndighed at deltage i de inspektioner, der foretages af den ledende tilsynsførende og det udpegede team.

3. Når den ledende tilsynsførende ikke er i stand til at udføre tilsynsaktiviteter uden for Unionen, jf. stk. 1 og 2, skal denne

a) udøve sine beføjelser i henhold til artikel 35 på grundlag af alle de kendsgerninger og dokumenter, den råder over

b) dokumentere og redegøre for eventuelle konsekvenser af, at den ikke er i stand til at udføre de påtænkte tilsynsaktiviteter som omhandlet i denne artikel.

Der tages hensyn til de potentielle konsekvenser, der er omhandlet i dette stykkes litra b), i den ledende tilsynsførendes henstillinger fremsat i henhold til artikel 35, stk. 1, litra d).

Artikel 37

Anmodning om oplysninger

1. Den ledende tilsynsførende kan efter simpel anmodning eller ved en afgørelse kræve, at 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, politikker, dokumentation, rapporter om IKT-sikkerhedsrevision, indberetninger af IKT-relaterede hændelser samt oplysninger om parter, som den kritiske tredjepartsudbyder af IKT-tjenester har outsourcet operationelle funktioner eller aktiviteter til.

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

a) henvise til denne artikel som retsgrundlag for anmodningen

b) angive formålet med anmodningen

c) præcisere, hvilke oplysninger der kræves

d) fastsætte en frist for fremlæggelsen af oplysningerne

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

3. Når den ledende tilsynsførende ***ved afgørelse*** kræver udlevering af 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 fremlæggelsen af oplysningerne

e) angive de tvangsbøder, der er omhandlet i artikel 35, stk. 6, og som finder anvendelse, hvis de ønskede oplysninger er ufuldstændige***, eller hvis de ikke fremlægges inden for den tidsfrist, som er omhandlet i dette stykkes litra d)***

f) oplyse om retten til at appellere afgørelsen til 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 forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. De oplysninger, der anmodes om, udleveres af repræsentanterne for de kritiske tredjepartsudbydere af IKT-tjenester. Behørigt befuldmægtigede advokater kan udlevere oplysningerne på deres klienters vegne. Den kritiske tredjepartsudbyder af IKT-tjenester bærer det fulde ansvar, hvis oplysningerne er ufuldstændige, ukorrekte eller vildledende.

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

Artikel 38

Generelle undersøgelser

1. For at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af det ***fælles*** undersøgelsesteam, der er omhandlet i artikel 40, ***stk. 1***, om nødvendigt foretage undersøgelser af ***kritiske*** tredjepartsudbydere af IKT-tjenester.

2. Den ledende tilsynsførende har beføjelse til:

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

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

   c) at indkalde repræsentanter for den ***kritiske*** tredjepartsudbyder af IKT-tjenester med henblik på mundtlige eller skriftlige redegørelser for 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 optegnelser over 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 35, stk. 6, hvis de krævede optegnelser, data, dokumenterede procedurer eller ethvert andet materiale eller svarene på de spørgsmål, der stilles til repræsentanter for tredjepartsudbyderne af IKT-tjenester, ikke fremlægges eller er ufuldstændige.

4. Repræsentanterne for de ***kritiske*** tredjepartsudbydere 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 35, stk. 6, 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. ***Den*** ledende ***tilsynsførende*** underretter i god tid før indledningen af undersøgelsen de kompetente myndigheder for de finansielle enheder, som anvender IKT-tjenesterne fra den pågældende ***kritiske*** tredjepartsudbyder af IKT-tjenester, om den påtænkte undersøgelse og om de bemyndigede personers identitet.

Den ledende tilsynsførende meddeler det fælles tilsynsnetværk alle oplysninger, der er videregivet i henhold til første afsnit.

Artikel 39 ▌

Inspektioner

1. For at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af de ***fælles*** undersøgelsesteams, der er omhandlet i artikel 40, stk. 1, betræde og foretage alle nødvendige inspektioner på stedet i alle forretningslokaler, arealer eller ejendomme, som tilhører tredjepartsudbyderne af IKT-***tjenester***, f.eks. hovedkontorer, operationscentraler og sekundære lokaler, samt foretage eksterne inspektioner.

Med henblik på udøvelsen af de beføjelser, der er omhandlet i første afsnit, hører den ledende tilsynsførende det fælles tilsynsnetværk.

2. De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget til at foretage inspektion på stedet, ***har beføjelse til at***

a) betræde alle sådanne forretningslokaler, arealer eller ejendomme, og

b) ▌forsegle alle ***sådanne*** forretningslokaler ▌, regnskaber eller registre i det for inspektionen nødvendige tidsrum og omfang.

De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget, 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 35, stk. 6, hvis repræsentanterne for de berørte ***kritiske*** tredjepartsudbydere af IKT-tjenester ikke lader sig underkaste inspektionen.

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

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

5. ***Den*** 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.

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 skal angive inspektionens genstand og formål, fastsætte tidspunktet for inspektionens påbegyndelse og oplyse om de tvangsbøder, der er omhandlet i artikel 35, stk. 6, 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 kræve, at de finansielle enheder opsiger de kontraktlige ordninger, der er indgået med den pågældende kritiske tredjepartsudbyder af IKT-tjenester.

Artikel 40

Løbende tilsyn

1. Når den ledende ***tilsynsførende*** udfører ***tilsynsaktiviteter, navnlig*** generelle undersøgelser eller ▌inspektioner, bistås denne af ***et fælles*** undersøgelsesteam, som er oprettet for hver af de kritiske tredjepartsudbydere af IKT-tjenester.

2. Det fælles undersøgelsesteam, der er omhandlet i stk. 1, skal bestå af medarbejdere fra:

a) ESA'erne

b) de relevante kompetente myndigheder, der fører tilsyn med de finansielle enheder, som den kritiske tredjepartsudbyder af IKT-tjenester leverer IKT-tjenester til ▌

c) den nationale kompetente myndighed, der er omhandlet i artikel 32, stk. 4, litra e), på frivillig basis

d) én national kompetent myndighed fra den medlemsstat, hvor den kritiske tredjepartsudbyder af IKT-tjenester har hjemsted, på frivillig basis.

Medlemmerne af det fælles undersøgelses***team*** skal have ekspertise med hensyn til IKT-anliggender og operationel risiko. Arbejdet i det fælles undersøgelsesteam koordineres af en udpeget medarbejder under ***den ledende tilsynsførende*** ("koordinatoren for den ledende tilsynsførende").

3. Inden for 3 måneder fra fuldførelsen af en undersøgelse eller en inspektion og efter at have hørt tilsynsforummet vedtager den ledende tilsynsførende henstillinger, som skal fremsættes over for den berørte kritiske tredjepartsudbyder af IKT-tjenester, i henhold til de i artikel 35 omhandlede beføjelser.

4. De i stk. 3 omhandlede henstillinger meddeles omgående den kritiske tredjepartsudbyder af IKT-tjenester og de kompetente myndigheder for de finansielle enheder, som den leverer IKT-tjenester til.

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

Artikel 41

Harmonisering af de betingelser, der muliggør udførelsen af tilsynsaktiviteter

1. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige tekniske standarder for at præcisere følgende:

a) de oplysninger, som en tredjepartsudbyder af IKT-tjenester skal fremlægge i sin ansøgning om frivillig anmodning om at blive udpeget som kritisk, jf. artikel 31, stk. 11

b) indholdet***, strukturen*** og formatet af de oplysninger, som tredjeparts***udbydere*** af IKT-tjenester ***skal indgive, offentliggøre eller aflægge rapport om*** i henhold til artikel 35, stk. 1***, herunder modellen for afgivelse af oplysninger om underentrepriseordninger***

c) kriterierne for fastlæggelse af sammensætningen af det fælles undersøgelsesteam***, der sikrer en afbalanceret deltagelse af medarbejdere fra ESA'erne og fra de relevante kompetente myndigheder, deres udpegelse, opgaver og arbejdsordninger***

d) de nærmere oplysninger om de kompetente myndigheders vurdering af de foranstaltninger, som kritiske tredjepartsudbydere af IKT-tjenester har truffet på grundlag af henstillinger fra ***den*** ledende ***tilsynsførende***, jf. artikel 42, stk. 3.

2. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den … [***18 måneder*** efter datoen ***for denne forordnings*** ikrafttræden].

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

Artikel 42

De kompetente myndigheders opfølgning

1. Senest ***60*** kalenderdage efter modtagelsen af de henstillinger, der er fremsat af ***den*** ledende ***tilsynsførende*** i henhold til artikel 35, stk. 1, litra d), underretter de kritiske tredjepartsudbydere af IKT-tjenester ***enten*** den ledende tilsynsførende om, ***at de agter*** at følge ***henstillingerne, eller de giver en begrundet redegørelse for, hvorfor de agter ikke at følge*** henstillingerne. ***Den*** ledende ***tilsynsførende*** videregiver straks disse oplysninger til de kompetente myndigheder ***for de pågældende finansielle enheder.***

2. Den ledende tilsynsførende offentliggør det, hvis en kritisk tredjepartsudbyder af IKT-tjenester undlader at underrette den ledende tilsynsførende i overensstemmelse med stk. 1, eller hvis den redegørelse, som den kritiske tredjepartsudbyder af IKT-tjenester har givet, ikke anses for at være tilstrækkelig. De offentliggjorte oplysninger skal oplyse om identiteten af den kritiske tredjepartsudbyder af IKT-tjenester og om typen og arten af den manglende overholdelse. Sådanne oplysninger begrænses til, hvad der er relevant og forholdsmæssigt med henblik på at sikre offentlighedens bevidsthed, medmindre en sådan offentliggørelse vil kunne forvolde de involverede parter uforholdsmæssig stor skade eller i alvorlig grad bringe de finansielle markeders velordnede funktion og integritet eller stabiliteten af hele eller dele af Unionens finansielle system i fare.

Den ledende tilsynsførende underretter tredjepartsudbyderen af IKT-tjenester om den pågældende offentliggørelse.

3. De kompetente myndigheder ***informerer de relevante*** finansielle enheder ***om*** de risici, der er identificeret i de henstillinger, som er fremsat over for kritiske tredjepartsudbydere af IKT-***tjenester*** i overensstemmelse med artikel 35, stk. 1, ***litra*** d).

Når de finansielle enheder styrer IKT-tredjepartsrisici tager de hensyn til de risici, der er omhandlet i første afsnit.

4. Hvis en kompetent myndighed vurderer, at en finansiel enhed ikke tager hensyn til eller ikke i tilstrækkelig grad i sin styring af IKT-tredjepartsrisiko imødegå de specifikke risici, der er identificeret i henstillingerne, underretter den den finansielle enhed om muligheden for, at der inden for 60 kalenderdage efter modtagelsen af en sådan underretning træffes en afgørelse i henhold til stk. 6, i fravær af passende kontraktlige ordninger, der tager sigte på at imødegå sådanne risici.

5. De kompetente myndigheder kan efter at have modtaget rapporterne omhandlet i artikel 35, stk. 1, litra c), og inden de træffer en afgørelse som omhandlet i nærværende artikels stk. 6, på frivillig basis høre de kompetente myndigheder, der er udpeget eller oprettet overensstemmelse med direktiv (EU) …/…[+], som har ansvar for tilsynet med en væsentlig eller vigtig enhed opført, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

6. De kompetente myndigheder kan, ***som en sidste udvej, efter underretningen og eventuelt høringen som fastsat i nærværende artikels stk. 4 og 5,*** i henhold til artikel 50 træffe en afgørelse, der kræver, at finansielle enheder midlertidigt, enten helt eller delvist, suspenderer anvendelsen eller udrulningen af en tjeneste, som den kritiske tredjepartsudbyder af IKT-tjenester leverer, indtil de risici, der er identificeret i de henstillinger, der er fremsat over for de kritiske tredjepartsudbydere af IKT-***tjenester***, er blevet imødegået. De kan om nødvendigt kræve, at finansielle enheder helt eller delvist opsiger de relevante kontraktlige ordninger, der er indgået med de kritiske tredjepartsudbydere af IKT-tjenester.

7. Hvis en kritisk tredjepartsudbyder af IKT-tjenester på grundlag af en tilgang, der divergerer fra den, som den ledende tilsynsførende anbefaler, nægter at tilslutte sig henstillinger, og en sådan divergerende tilgang kan have negativ indvirkning på et stort antal finansielle enheder eller en betydelig del af den finansielle sektor, og individuelle advarsler fra de kompetente myndigheder ikke har resulteret i konsekvente tilgange, der afbøder den potentielle risiko for den finansielle stabilitet, kan den ledende tilsynsførende efter at have hørt tilsynsforummet afgive ikkebindende og ikkeoffentlige udtalelser til de kompetente myndigheder for at fremme konsekvente og konvergerende tilsynsmæssige opfølgningsforanstaltninger, alt efter hvad der er relevant.

8. ***Efter at have modtaget rapporterne omhandlet i artikel 35, stk. 1, litra c), tager de kompetente myndigheder, når*** de træffer en afgørelse som omhandlet i nærværende artikels stk. 6, ▌ hensyn til typen og omfanget af den risiko, som ikke imødegås af den kritiske tredjepartsudbyder af IKT-tjenester, samt alvoren af den manglende overholdelse, under hensyntagen til følgende kriterier:

a) den manglende overholdelses grovhed og varighed

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

c) om en økonomisk forbrydelse er blevet fremmet eller foranlediget af eller på anden måde kan tilskrives den manglende overholdelse

d) hvorvidt den manglende overholdelse er forsætlig eller skyldes uagtsomhed

e) hvorvidt suspensionen eller opsigelsen af de kontraktlige ordninger skaber en risiko for kontinuiteten af den finansielle enheds forretningsaktiviteter, uanset den finansielle enheds bestræbelser på at undgå afbrydelser af leveringen af dens tjenester

f) når det er relevant, den udtalelse, som på frivillig basis i overensstemmelse med denne artikels stk. 5 er indhentet fra de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) …/…[+], og som har ansvar for tilsynet med en væsentlig eller vigtig enhed, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester.

De kompetente myndigheder giver de finansielle enheder den nødvendige tid for dem til at tilpasse de kontraktlige ordninger med kritiske tredjepartsudbydere af IKT-tjenester for at undgå skadelige virkninger for deres digitale operationelle modstandsdygtighed og for dem til at indføre exitstrategier og overgangsplaner som omhandlet i artikel 28.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

9. Den afgørelse, der er omhandlet i denne artikels stk. 6, meddeles medlemmerne af tilsynsforummet, jf. artikel 32, stk. 4, litra a), b) og c), og det fælles tilsynsnetværk.

De kritiske tredjepartsudbydere af IKT-tjenester, der er berørt af de i stk. 6 omhandlede afgørelser, samarbejder fuldt ud med de påvirkede finansielle enheder, navnlig i forbindelse med suspension eller opsigelse af deres kontraktlige ordninger.

10. De kompetente myndigheder orienterer regelmæssigt den ledende ***tilsynsførende*** om de tilgange og foranstaltninger, de har iværksat i forbindelse med deres tilsynsopgaver vedrørende finansielle enheder, samt om de kontraktlige ***ordninger***, som de finansielle enheder har indgået, når kritiske tredjeparts***udbydere*** af IKT-tjenester kun delvist eller slet ikke har tilsluttet sig de henstillinger, som den ledende ***tilsynsførende*** har fremsat over for dem.

11. Den ledende tilsynsførende kan efter anmodning fremkomme med yderligere præciseringer vedrørende de udstedte henstillinger for at vejlede de kompetente myndigheder om opfølgningsforanstaltningerne.

Artikel 43

Tilsynsgebyrer

1. Den ***ledende tilsynsførende*** opkræver ***i overensstemmelse med den delegerede retsakt, der er omhandlet i denne artikels stk. 2,*** gebyrer hos kritiske tredjepartsudbydere af IKT-tjenester, som fuldt ud dækker ***den ledende tilsynsførendes*** nødvendige udgifter i forbindelse med varetagelsen af ***tilsyns***opgaver i henhold til denne forordning, herunder godtgørelse af eventuelle omkostninger, der kan opstå som følge af det arbejde, der udføres af ***det fælles undersøgelsesteam, som er omhandlet i artikel 40, samt omkostningerne til rådgivning ydet af de uafhængige eksperter som omhandlet i artikel 32, stk. 4, andet afsnit, i forbindelse med forhold, der hører under området for de direkte*** tilsynsaktiviteter ▌.

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 skal stå i et rimeligt forhold til dennes omsætning.

2. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 57 for at supplere denne forordning ved at fastsætte gebyrbeløbene og den måde, hvorpå de skal betales, senest den … ***[18 måneder fra datoen for denne forordnings ikrafttræden]***.

Artikel 44

Internationalt samarbejde

1. ***Med forbehold af artikel 36*** kan EBA, ESMA og EIOPA i overensstemmelse med artikel 33 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010 indgå administrative ordninger med tredjelandes regulerings- og tilsynsmyndigheder for at fremme det internationale samarbejde om IKT-tredjepartsrisiko på tværs af forskellige finansielle sektorer, navnlig ved at udvikle bedste praksis for gennemgang af praksis 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 fælles 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 tredjelandsmyndigheder, med fokus på udviklingen inden for IKT-tredjepartsrisiko og konsekvenserne for den finansielle stabilitet, markedets integritet, investorbeskyttelsen og det indre markeds funktionsmåde.

Kapitel VI

Ordninger for informationsudveksling

Artikel 45

Ordninger for informationsudveksling af oplysninger og efterretninger om cybertrusler

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

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

   b) finder sted inden for betroede fællesskaber af finansielle enheder

c) gennemføres gennem ordninger for informationsudveksling, der beskytter de udvekslede oplysningers potentielt sensitive karakter, og som er omfattet af adfærdsregler med fuld respekt for forretningshemmeligheder, beskyttelse af personoplysninger i overensstemmelse med forordning (EU) 2016/679 og retningslinjer for konkurrencepolitikken.

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 de kan indgå i ordninger for informationsudveksling, ***om inddragelse af tredjepartsudbydere af IKT-tjenester og*** 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, alt efter hvad der er relevant, ophør af deres medlemskab, når det træder i kraft.

Kapitel VII

Kompetente myndigheder

Artikel 46

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 denne forordning, i overensstemmelse med de beføjelser, som tillægges dem ved de respektive retsakter:

a) for kreditinstitutter ***og for institutter, der er fritaget i henhold til direktiv 2013/36/EU:*** den kompetente myndighed, der er udpeget i henhold til nævnte direktivs artikel 4, ***og for kreditinstitutter, der er klassificeret som signifikante i henhold til artikel 6, stk. 4, i*** forordning (EU) nr. 1024/2013***: ECB i overensstemmelse med de ved nævnte forordning tillagte beføjelser og opgaver***

b) for betalings***institutter, herunder betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, e-pengeinstitutter, herunder dem, der er undtaget i henhold til direktiv 2009/110/EF, og kontooplysnings***tjenesteudbydere ***som omhandlet i artikel 33, stk. 1, i direktiv (EU) 2015/2366***: den kompetente myndighed, der er udpeget i henhold til artikel 22 i direktiv (EU) 2015/2366

c) for investeringsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 4 i Europa-Parlamentets og Rådets direktiv (EU) 2019/2034[43]

d) for udbydere af kryptoaktivtjenester***, der er meddelt tilladelse i henhold til forordningen om markeder for kryptoaktiver***, og udstedere af ▌– aktivbaserede tokens: den kompetente myndighed, der er udpeget i overensstemmelse med den relevante bestemmelse i nævnte forordning

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

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

g) for markedspladser og udbydere af dataindberetningstjenester: den kompetente myndighed, der er udpeget i henhold til artikel 67 i direktiv 2014/65/EU, og ***den kompetente myndighed som defineret i artikel 2, stk. 1, nr. 18), i forordning (EU) nr. 600/2014***

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

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

[43] Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 af 27. november 2019 om tilsyn med investeringsselskaber og om ændring af direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU (EUT L 314 af 5.12.2019, s. 64).

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

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

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

m) for arbejdsmarkedsrelaterede pensions***kasser***: den kompetente myndighed, der er udpeget i henhold til artikel 47 i direktiv (EU) 2016/2341

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

I

o) for administratorer af kritiske benchmarks: den kompetente myndighed, der er udpeget i henhold til artikel 40 og 41 i forordning ***(EU) 2016/1011***

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

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

Artikel 47

Samarbejde med strukturer og myndigheder, der er oprettet ved ***direktiv (EU) …/…***[+]

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 ***14 i direktiv (EU) …/…***[+], kan ESA'erne og de kompetente myndigheder ***deltage i samarbejdsgruppens aktiviteter for så vidt angår spørgsmål, der vedrører deres tilsynsaktiviteter i forbindelse med finansielle enheder. ESA'erne og de kompetente myndigheder*** kan anmode om at blive indbudt til ***at deltage i*** samarbejdsgruppens aktiviteter ***for så vidt angår spørgsmål i forbindelse med væsentlige eller vigtige enheder, der er omfattet af direktiv (EU) …/…***[+] ***og desuden er blevet udpeget som kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordnings artikel 31***.

2. ***Hvis det er relevant, kan de kompetente*** myndigheder rådføre sig ***og dele oplysninger*** med henholdsvis de centrale kontaktpunkter og de ***CSIRT'er***, der er udpeget eller oprettet i overensstemmelse med ***direktiv (EU) …/…***[+].

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

3. Hvis det er relevant, kan de kompetente myndigheder anmode om relevant teknisk rådgivning og bistand fra de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) …/…[+], og etablere samarbejdsordninger, således at der kan oprettes effektive og hurtige koordineringsmekanismer.

4. De ordninger, der er omhandlet i denne artikels stk. 3, kan bl.a. præcisere procedurerne for koordinering af tilsynsaktiviteter i forbindelse med væsentlige eller vigtige enheder, der er omfattet af direktiv (EU) …/…[+] og er udpeget som kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordnings artikel 31, herunder med henblik på i overensstemmelse med national ret at gennemføre undersøgelser og inspektioner på stedet samt med henblik på mekanismer til udveksling af oplysninger mellem de kompetente myndigheder i henhold til denne forordning og de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med nævnte direktiv, hvilket omfatter adgang til oplysninger, som sidstnævnte myndigheder har anmodet om.

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

Artikel 48

Samarbejde mellem myndigheder

1. De kompetente myndigheder arbejder tæt sammen indbyrdes og, hvis det er relevant, med den ledende tilsynsførende.

2. De kompetente myndigheder og den ledende tilsynsførende udveksler rettidigt alle de relevante oplysninger om kritiske tredjepartsudbydere af IKT-tjenester, som er nødvendige for, at de kan udføre deres respektive opgaver i henhold til denne forordning, navnlig i forbindelse med identificerede risici, tilgange og foranstaltninger, der træffes som led i den ledende tilsynsførendes tilsynsopgaver.

Artikel 49

Simuleringsøvelser på tværs af sektorer, kommunikation og samarbejde inden for finans

1. ESA'erne kan via Det Fælles Udvalg og i samarbejde med de kompetente myndigheder, ***afviklingsmyndigheder som omhandlet i artikel 3 i direktiv 2014/59/EU, ECB, Den Fælles Afviklingsinstans for så vidt angår oplysninger vedrørende enheder, der er omfattet af anvendelsesområdet for forordning (EU) nr. 806/2014,*** ESRB ***og ENISA, alt efter hvad der er relevant***, indføre mekanismer, der gør det muligt at udveksle effektive fremgangsmåder på tværs af finansielle sektorer for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

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

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

2. De kompetente myndigheder, ESA'erne og ECB samarbejder tæt med hinanden og udveksler oplysninger med henblik på at varetage deres opgaver i henhold til artikel 47-54. De koordinerer deres tilsyn tæt for at identificere og afhjælpe overtrædelser af 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 50

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 følgende beføjelser til at:

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

b) gennemføre inspektioner eller undersøgelser på stedet, som omfatter, men ***ikke er begrænset til:***

i) at indkalde repræsentanter for de finansielle enheder med henblik på mundtlige eller skriftlige redegørelser for forhold eller dokumenter, der vedrører undersøgelsens genstand og formål, og at optage svarene

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

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

3. Uden at dette berører medlemsstaternes ret til at pålægge strafferetlige sanktioner i overensstemmelse med artikel 52, 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 adfærd, der udgør en overtrædelse af denne forordning, til ophør og afholder sig fra at gentage en sådan adfærd

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

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

d) i det omfang national ret 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 når sådanne optegnelser kan være relevante for en undersøgelse af overtrædelser af denne forordning og

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

5. Såfremt stk. 2, litra c), og 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 som omhandlet i stk. 2, litra c), er behørigt begrundet og kan påklages.

Artikel 51

Udøvelse af beføjelsen til at pålægge administrative sanktioner og afhjælpende foranstaltninger

1. De kompetente myndigheder udøver, hvis det er relevant, beføjelsen til at pålægge de administrative sanktioner og afhjælpende foranstaltninger, der er omhandlet i artikel 50, i overensstemmelse med deres nationale lovrammer på følgende måde:

   a) direkte

   b) i samarbejde med andre myndigheder

   c) under eget ansvar ved delegation til andre myndigheder eller

   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 50, hensyn til, i hvilken grad overtrædelsen er forsætlig eller skyldes uagtsomhed, og alle andre relevante omstændigheder, herunder følgende, 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 opnåede fortjeneste eller undgåede tab, såfremt disse beløb kan beregnes

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

f) i hvilken grad den fysiske eller juridiske person samarbejder med den kompetente myndighed, uden at det dog berører kravet om tilbagebetaling af den pågældende fysiske eller juridiske persons opnåede fortjeneste eller undgåede tab

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

Artikel 52

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 judicielle, 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 53

Meddelelsespligt

Medlemsstaterne giver senest … [***24 måneder*** efter datoen for ***denne forordnings*** ikrafttræden] 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 eventuelle senere ændringer heraf.

Artikel 54

Offentliggørelse af administrative sanktioner

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

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

3. Hvis den kompetente myndighed efter en vurdering i det enkelte tilfælde finder, at offentliggørelse af identiteten, hvis der er tale om juridiske personer, eller af identiteten og personoplysninger, hvis der er tale om fysiske personer, vil være uforholdsmæssig, ***herunder omfatte risici i forbindelse med beskyttelsen af personoplysninger,*** vil bringe de finansielle markeders stabilitet eller gennemførelsen af en igangværende strafferetlig efterforskning i fare eller, i det omfang skaden kan fastslås, vil forvolde uforholdsmæssig stor skade på den involverede person, tager den en af følgende løsninger i anvendelse med hensyn til afgørelsen om at pålægge en administrativ sanktion:

   a) udsætte offentliggørelsen heraf, indtil enhver begrundelse for at undlade offentliggørelse er bortfaldet

b) offentliggøre den anonymt i overensstemmelse med national ret 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 på nogen måde bringes i fare, eller hvis en sådan offentliggørelse ikke står i et rimeligt forhold til den pålagte sanktions mildhed.

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 ***kun*** er tilgængelig på deres officielle websted ***i den periode, der er nødvendig af hensyn til denne artikel. Denne periode må ikke overstige fem år efter offentliggørelsen.***

Artikel 55

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***, herunder udveksling af oplysninger mellem kompetente myndigheder i henhold til denne forordning og kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) …/…[+], må*** ikke videregives til nogen anden person eller myndighed, medmindre der er hjemmel dertil i bestemmelser fastsat i EU-ret eller national ret ***;***

[+] EUT: Indsæt venligst i teksten nummeret på direktivet i dokument PE-CONS 32/22 (2020/0359(COD)).

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.

Artikel 56

Databeskyttelse

1. ESA'erne og de kompetente myndigheder må kun behandle personoplysninger, hvis det er nødvendigt for, at de kan opfylde deres respektive forpligtelser og udføre deres opgaver i henhold til denne forordning, navnlig med hensyn til undersøgelse, inspektion, anmodning om oplysninger, kommunikation, offentliggørelse, evaluering, efterprøvning, vurdering og udarbejdelse af tilsynsplaner. Personoplysninger behandles i overensstemmelse med forordning (EU) 2016/679 eller (EU) 2018/1725, alt efter hvilken der finder anvendelse.

2. Medmindre andet er fastsat i andre sektorspecifikke retsakter, opbevares de personoplysninger, der er omhandlet i stk. 1, indtil de relevante tilsynsopgaver er udført, og under alle omstændigheder i en periode på højst 15 år, undtagen i tilfælde af verserende retssager, der kræver yderligere opbevaring af sådanne oplysninger.

Kapitel VIII

Delegerede retsakter

Artikel 57

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 31, stk. 6, og artikel 43, stk. 2, tillægges Kommissionen for en periode på fem år fra den … [***12 måneder*** efter datoen for denne forordnings ikrafttræden]. ***Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. 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 i artikel 31, stk. 6, og artikel 43, stk. 2, omhandlede delegation af beføjelser 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 31, stk. 6, og artikel 43, 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 underrettet 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 58

Revisionsklausul

1. Senest den … [5 år efter datoen for denne forordnings ikrafttræden] foretager Kommissionen efter høring af ESA'erne og ESRB, alt efter hvad der er relevant, en gennemgang og forelægger en rapport for Europa-Parlamentet og Rådet, eventuelt ledsaget af et lovgivningsmæssigt forslag. ***Gennemgangen skal som minimum omfatte følgende:***

   a) kriterierne for udpegelse af kritiske tredjepartsudbydere af IKT-tjenester i overensstemmelse med artikel 31, stk. 2

   b) den frivillige karakter af underretningen om væsentlige cybertrusler, der er omhandlet i artikel 19

   c) den ordning, der er omhandlet i artikel 31, stk. 12, og de beføjelser, som tillægges den ledende tilsynsførende, som er fastsat i artikel 35, stk. 1, litra d), nr. iv), første led, med henblik på at evaluere nævnte bestemmelsers effektivitet med hensyn til at sikre effektivt tilsyn med kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland og nødvendigheden af at etablere en dattervirksomhed i Unionen.

Med henblik på dette litras første afsnit skal gennemgangen indeholde en analyse af den ordning, der er omhandlet i artikel 31, stk. 12, herunder for så vidt angår adgang for Unionens finansielle enheder til tjenester fra tredjelande og tilgængeligheden af sådanne tjenester på Unionens marked, og den skal tage hensyn til den yderligere udvikling på markederne for tjenester, der er omfattet af denne forordning, de finansielle enheders og de finansielle tilsynsmyndigheders praktiske erfaring med hensyn til henholdsvis brugen af og tilsynet med nævnte ordning og enhver relevant reguleringsmæssig og tilsynsmæssig udvikling, der finder sted på internationalt plan.

d) det hensigtsmæssige i at lade de finansielle enheder, der er omhandlet i artikel 2, stk. 3, litra e), og som gør brug af automatiske salgssystemer, være omfattet af denne forordnings anvendelsesområde i lyset af den fremtidige markedsudvikling i brugen af sådanne systemer

e) det fælles tilsynsnetværks funktion og effektivitet med hensyn til at støtte tilsynets konsekvens og informationsudvekslingens effektivitet inden for tilsynsrammen.

2. I forbindelse med revisionen af direktiv (EU) 2015/2366 vurderer Kommissionen behovet for øget cyberrobusthed i betalingssystemer og betalingsbehandlingsaktiviteter og hensigtsmæssigheden af at udvide denne forordnings anvendelsesområde til operatører af betalingssystemer og enheder, der er involveret i betalingsbehandlingsaktiviteter. I lyset af denne vurdering forelægger Kommissionen som led i revisionen af direktiv (EU) 2015/2366 en rapport for Europa-Parlamentet og Rådet senest den ... [6 måneder efter datoen for denne forordnings ikrafttræden].

På grundlag af denne revisionsrapport og efter høring af ESA'erne, ECB og ESRB kan Kommissionen, hvor det er relevant og som led i det lovgivningsmæssige forslag, som den kan vedtage i henhold til artikel 108, stk. 2, i direktiv (EU) 2015/2366, forelægge et forslag, der sikrer, at alle operatører af betalingssystemer og enheder, der er involveret i betalingsbehandlingsaktiviteter, er omfattet af passende tilsyn, samtidig med at der tages hensyn til centralbankens eksisterende tilsyn.

3. ***Senest den ...*** [***tre år efter datoen for denne forordnings ikrafttræden***] foretager Kommissionen ***efter høring af ESA'erne og Udvalget af Europæiske Revisionstilsynsmyndigheder*** en gennemgang og forelægger en rapport for Europa-Parlamentet og Rådet, eventuelt ledsaget af et lovgivningsmæssigt forslag vedrørende det ***hensigtsmæssige i skærpede krav til lovpligtige revisorer og revisionsfirmaer for så vidt angår digital operationel modstandsdygtighed ved at lade revisorer og revisionsfirmaer blive omfattet af denne forordnings anvendelsesområde eller gennem ændringer af Europa-Parlamentets og Rådets direktiv 2006/43/EF***[44]***.***

[44] Europa-Parlamentets og Rådets direktiv 2006/43/EF af 17. maj 2006 om lovpligtig revision af årsregnskaber og konsoliderede regnskaber, om ændring af Rådets direktiv 78/660/EØF og 83/349/EØF og om ophævelse af Rådets direktiv 84/253/EØF (EUT L 157 af 9.6.2006, s. 87).

Afdeling II

Ændringer

Artikel 59

Ændringer af forordning (EF) nr. 1060/2009

I forordning (EF) nr. 1060/2009 foretages følgende ændringer:

1) Bilag I, afsnit A, punkt 4, første afsnit, 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 i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) .../…[*+].

---

[*] Europa-Parlamentets og Rådets forordning (EU) .../… af … 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, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L … af …, s. …)."

2) Bilag III, punkt 12, affattes således:

"***12. Kreditvurderingsbureauet overtræder artikel 6, stk. 2, sammenholdt med bilag I, afsnit A, punkt 4, ved at undlade at 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 i overensstemmelse med forordning (EU) …/… [++], eller ved at undlade at gennemføre eller opretholde beslutningsprocedurer eller organisatoriske strukturer som påkrævet i henhold til nævnte punkt."***

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)), og indsæt nummer, dato og EUT-henvisning for nævnte forordning i fodnoten.

[++] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

Artikel 60

Ændringer af forordning (EU) nr. 648/2012

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

1) I artikel 26 foretages følgende ændringer:

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) …/…[*+].

_____

[*] Europa-Parlamentets og Rådets forordning (EU) .../… af … 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, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L … af …, s. …)."

b) Stk. 6 udgår.

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)), og indsæt nummer, dato og EUT-henvisning for nævnte forordning i fodnoten.

2) I artikel 34 foretages følgende ændringer:

a) Stk. 1 affattes således:

"1. En CCP udarbejder, gennemfører og opretholder en passende forretningskontinuitetsplan og en katastrofeberedskabsplan, som omfatter ***en politik*** for IKT-driftsstabilitet og planer for ***IKT-indsats og*** -genopretning, der indføres og gennemføres i overensstemmelse med forordning (EU) …/…[+], og som har til formål at sikre opretholdelsen af dens funktioner, sikre rettidig genopretning af transaktioner og opfyldelse af CCP'ens forpligtelser.***"***

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

"3. 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 ***en politik*** for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner.***"***

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

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, 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) .../…[+].

2. Et transaktionsregister udarbejder, gennemfører og opretholder en hensigtsmæssig forretningskontinuitetsplan og en katastrofeberedskabsplan, herunder ***en politik*** for IKT-driftsstabilitet og planer for ***IKT-indsats og*** -genopretning udarbejdet i overensstemmelse med forordning (EU) .../…[+] , 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.

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

6) Bilag I, afsnit II, ændres således:

a) Litra a) og b) affattes således:

"a) et transaktionsregister overtræder bestemmelserne i artikel 79, stk. 1, ved at undlade at identificere kilder til operationelle risici eller ved at undlade at reducere disse risici ved at udvikle passende systemer, kontroller og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) .../…[+]

b) et transaktionsregister overtræder bestemmelserne i artikel 79, stk. 2, ved at undlade at udarbejde, gennemføre eller opretholde en hensigtsmæssig forretningskontinuitetsplan og en katastrofeberedskabsplan udarbejdet i overensstemmelse med forordning (EU) .../…[+]*, som har til formål at sikre opretholdelse af registrets funktioner, sikre rettidig genopretning af transaktioner og opfyldelse af transaktionsregistrets forpligtelser".*

b) Litra c) udgår.

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

7) Bilag III ændres således:

a) Afsnit II ændres således:

i) litra c) affattes således:

"c) en niveau 2-CCP overtræder artikel 26, stk. 3, ved at undlade at opretholde eller anvende en organisatorisk struktur, som sikrer kontinuitet og regelmæssighed i leveringen af dens tjenesteydelser og udøvelsen af dens aktiviteter, eller ved at undlade at anvende hensigtsmæssige og forholdsmæssigt afpassede systemer, ressourcer og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) .../…[+]".

ii) litra f) udgår.

b) Afsnit III, litra a), affattes således:

"a) en niveau 2-CCP overtræder artikel 34, stk. 1, ved at undlade at udarbejde, gennemføre eller opretholde en passende forretningskontinuitetsplan og en indsats- og genopretningsplan udarbejdet i overensstemmelse med forordning (EU) .../…[+], som har til formål at sikre opretholdelsen af CCP'ens funktioner, sikre rettidig genopretning af alle transaktioner og opfyldelse af CCP'ens forpligtelser, og som mindst giver mulighed for at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, for at give den pågældende CCP mulighed for at opretholde driftssikkerheden og gennemføre afvikling på den planlagte dato".

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

Artikel 61

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 IKT-værktøjer, kontroller og procedurer, som er oprettet og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) .../…[*+], 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) .../… af … 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, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L … af …, s. …)."

2) Stk. 2 udgår.

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)), og indsæt nummer, dato og EUT-henvisning for nævnte forordning i fodnoten.

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 ***en politik*** for IKT-driftsstabilitet og planer for ***IKT-indsats og*** -genopretning udarbejdet i overensstemmelse med forordning (EU) .../…[+], som har til formål at sikre opretholdelsen 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 12, stk. 5 og 7, i forordning (EU) .../…[+]."

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

4) ▌Stk. 6▐ affattes således:

"6. CSD'er identificerer, overvåger og forvalter de risici, som de vigtigste deltagere i de værdipapirafviklingssystemer, de driver, samt serviceydere og andre CSD'er eller andre markedsinfrastrukturer kan indebære for deres transaktioner. De giver efter anmodning de kompetente og relevante myndigheder oplysninger om sådanne risici, der identificeres. De underretter også omgående den kompetente myndighed og relevante myndigheder om eventuelle operationelle hændelser som følge af sådanne risici, dog ikke om IKT-risikoen."

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

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

Artikel 62

Ændringer af forordning (EU) nr. 600/2014

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

1) Artikel 27g ændres således:

a) Stk. 4 ***affattes således:***

4. "En APA skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) .../…*[+].

---

* Europa-Parlamentets og Rådets forordning (EU) .../… af … 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, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L … af …, s. …)."

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

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

2) Artikel 27h ændres således:

a) Stk. 5 ***affattes således:***

"5. En CTP skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i forordning (EU) .../…[++]."

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)), og indsæt nummer, dato og EUT-henvisning for nævnte forordning i fodnoten.

[++] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

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 ***affattes således:***

"3. En ARM skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i forordning (EU) .../…[+]."

b) Stk. 5, litra b), affattes således:

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

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)).

Artikel 63

Ændring af forordning (EU) 2016/1011

I artikel 6 i forordning (EU) 2016/1011 tilføjes følgende stykke:

"6. For kritiske benchmarks skal en administrator have solide administrative og regnskabsmæssige procedurer, interne kontrolmekanismer, effektive procedurer til risikovurdering og effektive kontrol- og sikkerhedsforanstaltninger med henblik på styring af sine IKT-systemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) .../…*[*+]*.

_____

[*] Europa-Parlamentets og Rådets forordning (EU) .../… af … 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, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L … af …, s. …)."

Artikel 64

Ikrafttræden og anvendelse

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

Den finder anvendelse fra den … [***24*** måneder efter datoen for ***denne forordnings*** ikrafttræden].

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

Udfærdiget i ..., den …

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

[+] EUT: Indsæt venligst i teksten nummeret på den forordning, der er indeholdt i dokument PE-CONS 41/22 (2020/0266(COD)), og indsæt nummer, dato og EUT-henvisning for nævnte forordning i fodnoten.