EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2022/2554

av 14. desember 2022

om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske sentralbank([1]),

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité([2]),

etter den ordinære regelverksprosedyren([3]) og

ut fra følgende betraktninger:

1) I den digitale tidsalderen støtter informasjons- og kommunikasjonsteknologi (IKT) komplekse systemer som brukes i forbindelse med daglige aktiviteter. Det holder økonomien i gang i viktige sektorer, herunder finanssektoren, og forbedrer det indre markeds virkemåte. Økt digitalisering og innbyrdes forbindelser øker også IKT-risikoen og gjør samfunnet som helhet, og særlig finanssystemet, mer sårbart overfor cybertrusler eller IKT-forstyrrelser. Den allment utbredte bruken av IKT-systemer og en høy grad av digitalisering og konnektivitet er i dag sentrale trekk i den virksomheten som drives av Unionens finansielle enheter, men deres digitale motstandsdyktighet må fortsatt håndteres bedre og integreres i deres bredere operasjonelle rammer.

2) Bruken av IKT har de siste tiårene fått en sentral rolle i leveringen av finansielle tjenester og har nådd det punktet der den i dag er avgjørende for driften av alle finansielle enheters vanlige daglige funksjoner. Digitalisering omfatter i dag for eksempel betalinger som i økende grad har gått fra kontanter og papirbaserte metoder til bruk av digitale løsninger, samt clearing og oppgjør av verdipapirer, elektronisk handel og algoritmehandel, utlån og finansiering, peer-to-peer-finansiering, kredittvurdering, skadebehandling og back-office-funksjoner. Forsikringssektoren har også forandret seg med bruken av IKT, fra framveksten av forsikringsformidlere som tilbyr sine tjenester online ved hjelp av forsikrings-

([1]) EUT C 343 av 26.8 2021, s. 1.
([2]) EUT C 155 av 30.4. 2021, s. 38.
([3]) Europaparlamentets holdning av 10. november 2022 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 28. november 2022.

teknologien InsurTech, til digital tegning av forsikring. Hele finanssektoren er i høy grad blitt digital, og digitaliseringen har også utdypet de innbyrdes forbindelsene og avhengigheten innen finanssektoren og med tredjepartsinfrastruktur og tredjepartsleverandører av tjenester.

3) Det europeiske råd for systemrisiko (ESRB) bekreftet i en rapport fra 2020 om systemrisiko på cyberområdet hvordan det eksisterende høye nivået av innbyrdes forbindelser blant finansielle enheter, finansmarkeder og finansmarkedsinfrastrukturer, og særlig den gjensidige avhengigheten mellom deres IKT-systemer, kan utgjøre en systemisk sårbarhet ettersom lokale cyberhendelser raskt kan spre seg fra en av de nærmere 22 000 finansielle enhetene i Unionen til hele finanssystemet, uhindret av geografiske grenser. Alvorlige IKT-relaterte overtredelser i finanssektoren påvirker ikke bare finansielle enheter isolert sett. De baner også veien for spredning av lokaliserte sårbarheter gjennom de finansielle overføringskanalene og kan få negative konsekvenser for stabiliteten i Unionens finanssystem, for eksempel gjennom likviditetsmangel og generelt tap av tillit til finansmarkedene.

4) I de senere årene har IKT-risiko tiltrukket seg oppmerksomheten til politiske beslutningstakere, reguleringsmyndigheter og standardiseringsorganer på internasjonalt plan, unionsplan og nasjonalt plan i et forsøk på å øke den digitale motstandsdyktigheten, fastsette standarder og koordinere regulerings- eller tilsynsarbeid. På internasjonalt plan har Baselkomiteen for banktilsyn, Komiteen for betalings- og markedsinfrastruktur, Rådet for finansiell stabilitet, Financial Stability Institute samt G7 og G20 som mål å utstyre vedkommende myndigheter og markedsoperatører i ulike jurisdiksjoner med verktøyer for å styrke deres finanssystemers motstandsdyktighet. Dette arbeidet har også vært motivert av behovet for å ta behørig hensyn til IKT-risiko i et globalt finanssystem med sterke innbyrdes forbindelser og for å etterstrebe større samstemmighet når det gjelder relevant beste praksis.

5) Til tross for målrettede politiske og lovgivningsmessige initiativ på unionsplan og nasjonalt plan utgjør IKT-risiko fortsatt en utfordring for den operasjonelle motstandsdyktigheten, ytelsen og stabiliteten i Unionens finanssystem. De reformene som fulgte etter finanskrisen i 2008, styrket først og fremst den finansielle motstandsdyktigheten i Unionens finanssektor og tok sikte på å bevare Unionens konkurranseevne og stabilitet sett fra et økonomisk, tilsynsmessig og markedsmessig perspektiv. Selv om IKT-sikkerhet og digital motstandsdyktighet inngår i den operasjonelle risikoen, har de ikke fått like mye oppmerksomhet på den reguleringsmessige dagsordenen etter finanskrisen og er bare utviklet på noen områder av Unionens politikk og regelverk for finansielle tjenester, eller bare i noen få medlemsstater.

6) I sin kommisjonsmelding av 8. mars 2018 med tittelen «*Handlingsplan for FinTech*: *– et viktig skritt mot en mer konkurransedyktig og innovativ finanssektor i Europa*» understreket Kommisjonen at det er ytterst viktig å gjøre Unionens finanssektor mer motstandsdyktig, herunder sett fra et operasjonelt perspektiv, for å sikre dens teknologiske sikkerhet og at den fungerer godt, samt at den raskt kan gjenopprettes etter IKT-relaterte overtredelser og IKT-relaterte hendelser, noe som til slutt gjør det mulig å levere finansielle tjenester på en effektiv og smidig måte i hele Unionen, herunder i forbindelse med krisesituasjoner, samtidig som forbrukernes og markedets tillit bevares.

7) I april 2019 utstedte Den europeiske tilsynsmyndighet (Den europeiske banktilsynsmyndighet) (EBA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1093/2010([4]), Den europeiske tilsynsmyndighet (Den europeiske tilsynsmyndighet for forsikring og tjenestepensjoner) (EIOPA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1094/2010([5]), og Den europeiske tilsynsmyndighet (Den europeiske verdipapir- og markedstilsynsmyndighet) (ESMA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1095/2010([6])

([4]) Europaparlaments- og rådsforordning (EU) nr. 1093/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske banktilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/78/EF (EUT L 331 av 15.12.2010, s. 12).

([5]) Europaparlaments- og rådsforordning (EU) nr. 1094/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske tilsynsmyndighet for forsikring og tjenestepensjoner), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/79/EF (EUT L 331 av 15.12.2010, s. 48).

([6]) Europaparlaments- og rådsforordning (EU) nr. 1095/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske verdipapir- og markedstilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/77/EF (EUT L 331 av 15.12.2010, s. 84).

(samlet kalt «de europeiske tilsynsmyndighetene» eller «ESMA»), i fellesskap en teknisk uttalelse og etterlyste en sammenhengende tilnærming til IKT-risiko i finanssektoren og anbefalte å styrke finansnæringens digitale operasjonelle motstandsdyktighet på en forholdsmessig måte gjennom et sektorspesifikt initiativ fra Unionen.

8) Unionens finanssektor er regulert av et felles regelverk og underlagt et europeisk finanstilsynssystem. Ikke desto mindre er bestemmelsene om håndtering av digital operasjonell motstandsdyktighet og IKT-sikkerhet ennå ikke fullstendig eller konsekvent harmoniserte, til tross for at den digitale operasjonelle motstandsdyktigheten er avgjørende for å sikre finansiell stabilitet og markedsintegritet i den digitale tidsalderen, og ikke mindre viktige enn for eksempel felles standarder for tilsyn eller markedsatferd. Det felles regelverket og tilsynssystemet bør derfor utvikles slik at det også omfatter digital operasjonell motstandsdyktighet gjennom å styrke vedkommende myndigheters mandat, slik at de får mulighet til å føre tilsyn med styringen av IKT-risiko i finanssektoren for å beskytte det indre markeds integritet og effektivitet, og for å fremme at det fungerer etter hensikten.

9) Lovgivningsmessige forskjeller og ulike nasjonale regulerings- eller tilsynsstrategier for IKT-risiko skaper hindringer for et velfungerende indre marked for finansielle tjenester og hindrer en smidig utøvelse av etableringsadgangen og av retten til fri utveksling av tjenester for finansielle enheter som driver virksomhet over landegrensene. Konkurransen mellom samme type finansielle enheter som driver virksomhet i forskjellige medlemsstater, kan også bli vridd. Dette gjelder særlig for områder der Unionens harmonisering har vært svært begrenset, for eksempel testing av digital operasjonell motstandsdyktighet, eller ikke-eksisterende, for eksempel overvåking av IKT-tredjepartsrisiko. Forskjeller som skyldes planlagt utvikling på nasjonalt plan, kan skape ytterligere hindringer for det indre markeds virkemåte på bekostning av markedsdeltakere og finansiell stabilitet.

10) På grunn av at bestemmelser om IKT-risiko bare delvis er blitt behandlet på unionsplan, er det på det nåværende tidspunktet hull eller overlappinger på viktige områder, for eksempel når det gjelder rapportering av IKT-relaterte hendelser og testing av digital operasjonell motstandsdyktighet, samt manglende konsekvens når nye avvikende nasjonale regler utarbeides, eller overlappende regler anvendes på en kostnadsineffektiv måte. Dette er særlig skadelig for en IKT-intensiv bruker som finanssektoren, ettersom teknologirisikoer ikke kjenner noen grenser og finanssektoren anvender sine tjenester på et bredt grenseoverskridende grunnlag innen og utenfor Unionen. Enkelte finansielle enheter som driver virksomhet over landegrensene, eller som har flere tillatelser (én finansiell enhet kan for eksempel ha tillatelse som bank, verdipapirforetak og betalingsinstitusjon, der hver tillatelse er utstedt av ulike vedkommende myndigheter i en eller flere medlemsstater), står overfor operasjonelle utfordringer når det gjelder å styre IKT-risiko og redusere IKT-hendelsers negative virkninger på egen hånd og på en sammenhengende kostnadseffektiv måte.

11) Ettersom det felles regelverket ikke har vært ledsaget av et omfattende rammeverk for IKT eller operasjonell risiko, er det nødvendig med ytterligere harmonisering av viktige krav til digital operasjonell motstandsdyktighet for alle finansielle enheter. Den IKT-kapasiteten og den generelle motstandsdyktigheten som finansielle enheter med utgangspunkt i disse viktige kravene skal utvikle for å stå imot driftsforstyrrelser, vil bidra til å bevare stabiliteten og integriteten på Unionens finansmarkeder og dermed bidra til å sikre et sterkt investor- og forbrukervern i Unionen. Ettersom denne forordningen har som formål å bidra til at det indre marked virker tilfredsstillende, bør den bygge på artikkel 114 i traktaten om Den europeiske unions virkemåte (TEUV) slik den tolkes i Den europeiske unions domstols rettspraksis.

12) Denne forordningen har som formål å konsolidere og oppgradere kravene til IKT-risiko som en del av kravene til operasjonell risiko, som fram til nå har vært behandlet separat i ulike unionsrettsakter. Selv om disse rettsaktene omfatter hovedkategoriene av finansiell risiko (for eksempel kredittrisiko, markedsrisiko, motpartskredittrisiko, likviditetsrisiko og markedsatferdsrisiko), ble ikke alle komponentene i den operasjonelle motstandsdyktigheten behandlet på en fullstendig måte da disse rettsaktene ble vedtatt. Da reglene om operasjonell risiko ble nærmere utformet i disse unionsrettsaktene, ble det ofte foretrukket en tradisjonell kvantitativ strategi for å styre risiko (nemlig å fastsette et kapitalkrav for å dekke IKT-risiko) i stedet for målrettede kvalitative regler om beskyttelse, påvisning, begrensning, gjenoppretting og avhjelping av IKT-relaterte hendelser, eller om rapporteringskapasitet og digital testkapasitet. Disse rettsaktene skulle først og fremst omfatte og oppdatere grunnleggende regler om tilsyn, markedsintegritet eller atferd. Ved å konsolidere og oppgradere de ulike reglene om IKT-risiko, bør alle bestemmelser om digital risiko i finanssektoren for første gang bli samlet på en konsekvent måte i én enkelt rettsakt. Denne forordningen tetter derfor hullene eller avhjelper manglende

konsekvens i noen av de tidligere rettsaktene, herunder med hensyn til terminologien som brukes i dem, og den viser eksplisitt til IKT-risiko gjennom målrettede regler om kapasitet til IKT-risikostyring, rapportering av hendelser, testing av operasjonell motstandsdyktighet og overvåking av IKT-tredjepartsrisiko. Denne forordningen bør derfor også øke bevisstheten om IKT-risiko og anerkjenne at IKT-hendelser og manglende operasjonell motstandsdyktighet kan utgjøre en fare for finansielle enheters soliditet.

13) Finansielle enheter bør følge den samme tilnærmingen og de samme prinsippbaserte reglene i sin styring av IKT-risiko, samtidig som det tas hensyn til deres størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift. Konsekvens bidrar til å øke tilliten til finanssystemet og bevare dets stabilitet, særlig i tider med høy avhengighet av IKT-systemer, -plattformer og -infrastrukturer, noe som medfører økt digital risiko. Overholdelse av en grunnleggende cyberhygiene bør også hindre at økonomien påføres høye kostnader, ved at virkningene av og kostnadene i forbindelse med IKT-forstyrrelser minimeres.

14) En forordning bidrar til å redusere regelverkets kompleksitet, fremmer tilsynsmessig tilnærming og øker rettssikkerheten, og den bidrar også til å begrense kostnadene for å overholde bestemmelsene, særlig for finansielle enheter som driver virksomhet over landegrensene, og til å redusere konkurransevridninger. Derfor er valget av en forordning med henblikk på å opprette et felles rammeverk for finansielle enheters digitale operasjonelle motstandsdyktighet den mest hensiktsmessige måten for å sikre en homogen og sammenhengende anvendelse av alle de komponentene som inngår i IKT-risikostyring i Unionens finanssektor.

15) Europaparlaments- og rådsdirektiv (EU) 2016/1148([7]) var det første overgripende rammeverket for cybersikkerhet som ble vedtatt på unionsplan, og som også får anvendelse på tre typer av finansielle enheter, nemlig kredittinstitusjoner, handelsplasser og sentrale motparter. Ettersom direktiv (EU) 2016/1148 fastsetter en ordning for identifisering av ytere av samfunnsviktige tjenester på nasjonalt plan, var det imidlertid bare visse kredittinstitusjoner, handelsplasser og sentrale motparter som ble utpekt av medlemsstatene, og som i praksis ble omfattet av direktivets virkeområde, og som derfor skal overholde de aktuelle rapporteringskravene til IKT-sikkerhet og IKT-hendelser som er fastsatt i direktivet. I europaparlaments- og rådsdirektiv (EU) 2022/2555([8]) fastsettes enhetlige kriterier for å bestemme hvilke enheter som er omfattet av direktivets virkeområde (størrelsesbasert regel), samtidig som de tre typene av finansielle enheter fortsatt er omfattet av direktivets virkeområde.

16) Ettersom denne forordningen fører til en økt grad av harmonisering for de ulike komponentene som inngår i digital motstandsdyktighet, gjennom å innføre krav til IKT-risikostyring og rapportering av IKT-relaterte hendelser som er strengere enn dem som er fastsatt i gjeldende unionsregelverk for finansielle tjenester, utgjør imidlertid denne høyere graden en økt harmonisering også sammenlignet med de kravene som er fastsatt i direktiv (EU) 2022/2555. Denne forordningen utgjør derfor *lex specialis* med hensyn til direktiv (EU) 2022/2555. Samtidig er det svært viktig å opprettholde en tett forbindelse mellom finanssektoren og Unionens overgripende rammeverk for cybersikkerhet som for øyeblikket er fastsatt i direktiv (EU) 2022/2555, for å sikre samsvar med de strategiene for cybersikkerhet som er vedtatt av medlemsstatene, og for å gi finansielle tilsynsmyndigheter mulighet til få kjennskap til cyberhendelser som påvirker andre sektorer som er omfattet av det nevnte direktivet.

([7]) Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (EUT L 194 av 19.7.2016, s. 1).

([8]) Europaparlaments- og rådsdirektiv (EU) 2022/2555 av 14. desember 2022 om tiltak for å sikre et høyt felles nivå av cybersikkerhet i hele Unionen, om endring av forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om oppheving av direktiv (EU) 2016/1148 (NIS-2-direktiv) (se EUT L 333 av 27.12.2022, s. 80).

17) I samsvar med artikkel 4 nr. 2 i traktaten om Den europeiske union og uten at det berører Domstolens rettslige overprøving, bør denne forordningen ikke berøre medlemsstatenes ansvar med hensyn til vesentlige statlige funksjoner som gjelder offentlig sikkerhet, forsvar og ivaretakelse av nasjonal sikkerhet, for eksempel vedrørende utlevering av opplysninger som ville være i strid med ivaretakelse av nasjonal sikkerhet.

18) For å muliggjøre læring på tvers av sektorene og for å kunne dra nytte av andre sektorers erfaringer når det gjelder håndtering av cybertrusler, bør de finansielle enhetene som er nevnt i direktiv (EU) 2022/2555, forbli en del av «økosystemet» i det nevnte direktivet (for eksempel samarbeidsgruppen og nettverket av enheter for håndtering av digitale hendelser (CSIRT-enheter)). De europeiske tilsynsmyndighetene og de nasjonale vedkommende myndighetene bør kunne delta i de strategiske politiske drøftingene og det tekniske arbeidet i samarbeidsgruppen i henhold til det nevnte direktivet, og utveksle opplysninger og samarbeide videre med de felles kontaktpunktene som er utpekt eller opprettet i samsvar med det nevnte direktivet. De vedkommende myndighetene i henhold til denne forordningen bør også rådføre seg med og samarbeide med CSIRT-enhetene. De vedkommende myndighetene bør også kunne anmode om en teknisk uttalelse fra de vedkommende myndighetene som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555, og etablere samarbeidsordninger som har til formål å sikre effektive og raske koordineringsordninger.

19) Med tanke på de sterke innbyrdes forbindelsene mellom finansielle enheters digitale motstandsdyktighet og fysiske motstandsdyktighet er det nødvendig med en sammenhengende tilnærming med hensyn til motstandsdyktigheten til kritiske enheter i denne forordningen og i europaparlaments- og rådsdirektiv (EU) 2022/2557([9]). Ettersom finansielle enheters fysiske motstandsdyktighet behandles på en omfattende måte i de forpliktelsene som gjelder IKT-risikostyring og rapportering i denne forordningen, bør forpliktelsene i kapittel III og IV i direktiv (EU) 2022/2557 ikke få anvendelse på finansielle enheter som er omfattet av det nevnte direktivets virkeområde.

20) Leverandører av skytjenester er én kategori av digital infrastruktur som er omfattet av direktiv (EU) 2022/2555. Unionsovervåkingsrammeverket («overvåkingsrammeverket») som er fastsatt ved denne forordningen, får anvendelse på alle kritiske tredjepartsleverandører av IKT-tjenester, herunder leverandører av skytjenester som leverer IKT-tjenester til finansielle enheter, og bør anses som et supplement til det tilsynet som utføres i henhold til direktiv (EU) 2022/2555. Videre bør det overvåkingsrammeverket som er fastsatt ved denne forordningen, omfatte leverandører av skytjenester i fravær av en overgripende unionsramme om opprettelse av en digital overvåkingsmyndighet.

21) For at finansielle enheter skal kunne opprettholde full kontroll over IKT-risiko, må de ha omfattende kapasitet som muliggjør en sterk og effektiv IKT-risikostyring, samt særskilte ordninger og retningslinjer for håndtering av alle IKT-relaterte hendelser og for rapportering av alvorlige IKT-relaterte hendelser. På samme måte bør finansielle enheter ha innført retningslinjer for testing av IKT-systemer, IKT-kontroller og IKT-prosesser, samt for styring av IKT-tredjepartsrisiko. Referansenivået for digital operasjonell motstandsdyktighet hos finansielle enheter bør økes, samtidig som det også skapes mulighet for en forholdsmessig anvendelse av krav til visse finansielle enheter, særlig svært små bedrifter, samt finansielle enheter som er underlagt et forenklet rammeverk for IKT-risikostyring. For å legge til rette for et effektivt tilsyn med tjenestepensjonsforetak som er forholdsmessig og ivaretar behovet for å redusere den administrative byrden for de vedkommende myndighetene, bør de relevante nasjonale tilsynsordningene for slike finansielle enheter ta hensyn til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift, selv når de relevante tersklene fastsatt i artikkel 5 i europaparlaments- og rådsdirektiv (EU) 2016/2341([10]) overskrides. Framfor alt bør tilsynsvirksomheten først og fremst fokusere på behovet for å håndtere alvorlige risikoer i forbindelse med IKT-risikostyringen i en bestemt enhet.

([9]) Europaparlaments- og rådsdirektiv (EU) 2022/2557 av 14. desember 2022 om kritiske enheters motstandsdyktighet og om oppheving av rådsdirektiv 2008/114/EF (se EUT L 333 av 27.12.2022, s. 164).

([10]) Europaparlaments- og rådsdirektiv (EU) 2016/2341 av 14. desember 2016 om virksomhet i og tilsyn med tjenestepensjonsforetak (EUT L 354 av 23.12.2016, s. 37).

De vedkommende myndighetene bør også opprettholde en årvåken, men forholdsmessig tilnærming når det gjelder tilsyn med tjenestepensjonsforetak som, i samsvar med artikkel 31 i direktiv (EU) 2016/2341, utkontrakterer en betydelig del av sin kjernevirksomhet til tjenesteytere, for eksempel kapitalforvaltning, aktuarielle beregninger, regnskap og databehandling.

22) Terskler og taksonomier for rapportering av IKT-relaterte hendelser varierer vesentlig på nasjonalt plan. Selv om det kan oppnås enighet gjennom det relevante arbeidet som utføres av Den europeiske unions byrå for cybersikkerhet (ENISA), opprettet ved europaparlaments- og rådsforordning (EU) 2019/881([11]), og samarbeidsgruppen i henhold til direktiv (EU) 2022/2555, kan det fortsatt forekomme eller oppstå ulike strategier for terskler og taksonomier for andre finansielle enheter. På grunn av disse forskjellene er det flere krav som finansielle enheter må oppfylle, særlig når de driver virksomhet i flere medlemsstater, og når de inngår i et finanskonsern. Disse forskjellene kan dessuten hindre opprettelsen av ytterligere ensartede eller sentraliserte ordninger på unionsplan som framskynder rapporteringsprosessen og støtter en rask og smidig utveksling av opplysninger mellom vedkommende myndigheter, noe som er svært viktig for å styre IKT-risiko ved storstilte angrep med eventuelle systemiske konsekvenser.

23) For å redusere den administrative byrden og mulige overlappende rapporteringsforpliktelser for visse finansielle enheter bør kravet om rapportering av hendelser i henhold til europaparlaments- og rådsdirektiv (EU) 2015/2366([12]) ikke lenger gjelde for betalingstjenesteytere som er omfattet av virkeområdet for denne forordningen. Derfor bør de kredittinstitusjonene, e-pengeforetakene, betalingsinstitusjonene og yterne av kontoopplysningstjenester som er nevnt i artikkel 33 nr. 1 i det nevnte direktivet, fra denne forordningens anvendelsesdato rapportere i henhold til denne forordningen alle betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser som tidligere er rapportert i henhold til det nevnte direktivet, uavhengig av om slike hendelser er IKT-relaterte.

24) For at de vedkommende myndighetene skal kunne ivareta sin tilsynsrolle gjennom å skaffe seg en fullstendig oversikt over arten, hyppigheten, betydningen og virkningen av IKT-relaterte hendelser, og for å styrke utvekslingen av opplysninger mellom relevante offentlige myndigheter, herunder rettshåndhevende myndigheter og krisehåndteringsmyndigheter, bør denne forordningen fastsette en robust ordning for rapportering av IKT-relaterte hendelser der de relevante kravene bøter på nåværende hull i regelverket for finansielle tjenester, og fjerne eksisterende overlappinger og dobbeltbestemmelser for å redusere kostnadene. Derfor er det viktig å harmonisere ordningen for rapportering av IKT-relaterte hendelser gjennom å kreve at alle finansielle enheter skal rapportere til sine vedkommende myndigheter gjennom et harmonisert rammeverk i samsvar med denne forordningen. I tillegg bør de europeiske tilsynsmyndighetene ha myndighet til ytterligere å spesifisere relevante elementer med hensyn til rammeverket for rapportering av IKT-relaterte hendelser, for eksempel taksonomier, tidsrammer, datasett, maler og gjeldende terskler. For å sikre fullt samsvar med direktiv (EU) 2022/2555 bør finansielle enheter på frivillig grunnlag gis tillatelse til å underrette den berørte vedkommende myndigheten om betydelige cybertrusler, når de anser at cybertrusselen er av relevans for finanssystemet, tjenestebrukerne eller kundene.

25) Det er utarbeidet krav til testing av digital operasjonell motstandsdyktighet i visse finansielle delsektorer med rammer som ikke alltid er fullt ut harmoniserte. Dette fører potensielt til en fordobling av kostnader for finansielle enheter over landegrensene, og gjør en gjensidig anerkjennelse av resultatene av testingen av digital operasjonell motstandsdyktighet komplisert, noe som igjen kan fragmentere det indre marked.

([11]) Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions byrå for cybersikkerhet), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi, og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen) (EUT L 151 av 7.6.2019, s. 15).

([12]) Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF (EUT L 337 av 23.12.2015, s. 35).

26) I de tilfellene der det ikke kreves noen IKT-testing, vil sårbarheter ikke bli oppdaget, hvilket fører til at en finansiell enhet utsettes for en IKT-risiko og til slutt skaper en høyere risiko for stabiliteten og integriteten i finanssektoren. Uten unionstiltak vil testingen av digital operasjonell motstandsdyktighet fortsatt være inkonsekvent, og det vil ikke finnes et system for gjensidig anerkjennelse av IKT-testresultater i ulike jurisdiksjoner. Ettersom det er usannsynlig at andre finansielle delsektorer vil ta i bruk testordninger i et meningsfullt omfang, vil de i tillegg gå glipp av de potensielle fordelene med en testramme, for eksempel å påvise IKT-sårbarheter og IKT-risikoer, og å teste forsvarskapasitet og kontinuitet i virksomheten, hvilket bidrar til å øke tilliten til kunder, leverandører og forretningspartnere. For å utbedre disse overlappingene, forskjellene og hullene er det nødvendig å fastsette regler om koordinering av testordningen og dermed legge til rette for gjensidig anerkjennelse av avanserte tester for finansielle enheter som oppfyller kriteriene i denne forordningen.

27) Finansielle enheters avhengighet av bruken av IKT-tjenester skyldes delvis deres behov for å tilpasse seg en framvoksende konkurransedyktig digital global økonomi, for å effektivisere sin virksomhet og for å imøtekomme forbrukernes etterspørsel. Arten og omfanget av en slik avhengighet har utviklet seg kontinuerlig de siste årene, noe som har bidratt til kostnadsreduksjoner innen finansformidling, muliggjort utvidelse og skalerbarhet av virksomheter i forbindelse med utrullingen av finansielle aktiviteter, og samtidig gitt tilgang til et bredt spekter av IKT-verktøyer for å håndtere komplekse interne prosesser.

28) Den omfattende bruken av IKT-tjenester framgår av komplekse kontraktsregulerte ordninger, der finansielle enheter ofte støter på vanskeligheter med å forhandle om kontraktsvilkår som er tilpasset til de tilsynsstandardene eller andre forskriftsmessige krav som de er omfattet av, eller på annen måte med å håndheve særskilte rettigheter, som for eksempel tilgangs- eller revisjonsrettigheter, selv når sistnevnte er fastsatt i deres kontraktsregulerte ordninger. Mange av disse kontraktsregulerte ordningene inneholder dessuten ikke tilstrekkelige garantier som muliggjør en fullstendig overvåking av utkontrakteringsprosesser, hvilket gjør at den finansielle enheten ikke har mulighet til å vurdere disse risikoene. Ettersom tredjepartsleverandører av IKT-tjenester ofte leverer standardiserte tjenester til ulike typer kunder, kan det dessuten hende at slike kontraktsregulerte ordninger ikke alltid tilgodeser de individuelle eller spesifikke behovene til aktører i finansnæringen.

29) Selv om unionsregelverket for finansielle tjenester inneholder visse generelle regler om utkontraktering, er overvåkingen av den kontraktsregulerte dimensjonen ikke fullt ut forankret i unionsretten. I mangel av klare og skreddersydde EU-standarder som får anvendelse på de kontraktsregulerte ordningene som er inngått med tredjepartsleverandører av IKT-tjenester, er det ikke på en fyllestgjørende måte tatt høyde for den eksterne kilden til IKT-risiko. Derfor er det nødvendig å fastsette visse sentrale prinsipper for å veilede finansielle enheters styring av IKT-tredjepartsrisiko, som er av særlig betydning når finansielle enheter benytter tredjepartsleverandører av IKT-tjenester for å støtte kritiske eller viktige funksjoner. Disse prinsippene bør ledsages av et sett av grunnleggende kontraktfestede rettigheter når det gjelder flere aspekter av gjennomføring og oppsigelse av kontraktsregulerte ordninger, med henblikk på å yte visse minstegarantier for å styrke de finansielle enhetenes evne til effektivt å overvåke alle IKT-risikoer som oppstår hos tredjepartsleverandører av tjenester. Disse prinsippene utfyller den sektorspesifikke lovgivningen som får anvendelse på utkontraktering.

30) I dag er det tydelig at det er en viss mangel på homogenitet og tilnærming når det gjelder overvåking av IKT-tredjepartsrisiko og avhengighet av IKT-tredjeparter. Til tross for innsatsen for å håndtere utkontraktering, som for eksempel EBAs retningslinjer for utkontraktering fra 2019 og ESMAs retningslinjer for utkontraktering til leverandører av skytjenester fra 2021, tas det i unionsretten ikke i tilstrekkelig grad høyde for det bredere spørsmålet om å motvirke systemrisiko som kan utløses av finanssektorens eksponering mot et begrenset antall av kritiske tredjepartsleverandører av IKT-tjenester. Mangelen på regler på unionsplan forsterkes av mangelen på nasjonale regler om mandater og verktøyer som gjør det mulig for finansielle tilsynsmyndigheter å oppnå en god forståelse for avhengighet av IKT-tredjeparter, og foreta en tilstrekkelig overvåking av risikoer som oppstår som følge av konsentrasjoner av avhengighet av IKT-tredjeparter.

31) Med hensyn til den potensielle systemrisikoen som følger av økt bruk av utkontraktering og konsentrasjon av IKT-tredjeparter, og tatt i betraktning de utilstrekkelige nasjonale ordningene med hensyn til å gi finansielle tilsynsmyndigheter tilstrekkelige verktøyer for å kvantifisere, kvalifisere og avhjelpe konsekvensene av IKT-risiko, som oppstår hos kritiske tredjepartsleverandører av IKT-tjenester, er det nødvendig å fastsette et hensiktsmessig overvåkingsrammeverk som gjør det mulig å foreta løpende overvåking av aktivitetene hos tredjepartsleverandører av IKT-tjenester, som er kritiske tredjepartsleverandører av IKT-tjenester til finansielle enheter, samtidig som det sikres at fortroligheten og sikkerheten for andre kunder enn finansielle enheter, bevares. Selv om konsernintern levering av IKT-tjenester innebærer spesifikke risikoer og fordeler, bør den ikke automatisk anses som mindre risikabel enn levering av IKT-tjenester fra leverandører utenfor et finanskonsern, og den bør derfor være omfattet av samme regelverk. Når IKT-tjenester leveres innenfor samme finanskonsern, kan imidlertid finansielle enheter ha en høyere grad av kontroll over konserninterne leverandører, noe som bør tas hensyn til i den samlede risikovurderingen.

32) Med IKT-risiko som blir stadig mer komplisert og sofistikert, er gode tiltak for påvisning og forebygging av IKT-risiko i høy grad avhengig av regelmessig utveksling av etterretninger om trusler og sårbarheter mellom finansielle enheter. Utveksling av opplysninger bidrar til å skape økt bevissthet om cybertrusler. Dette styrker også finansielle enheters evne til å forhindre at cybertrusler blir til virkelige IKT-relaterte hendelser, og det setter finansielle enheter i stand til å begrense virkningen av IKT-relaterte hendelser mer effektivt og til å hente seg inn raskere. I fravær av veiledning på unionsplan synes flere faktorer å ha hindret en slik utveksling av etterretninger, særlig usikkerhet omkring forenligheten med regler om vern av personopplysninger, antitrust og ansvar.

33) I tillegg fører tvil om hvilke typer opplysninger som kan utveksles med andre markedsdeltakere, eller med myndigheter som ikke er tilsynsmyndigheter (som for eksempel ENISA, med henblikk på analytisk underlag, eller Europol, med henblikk på rettshåndheving), til at nyttige opplysninger holdes tilbake. Derfor er omfanget av og kvaliteten på utveksling av opplysninger for tiden fortsatt begrenset og fragmentert, med relevante utvekslinger som for det meste er lokale (gjennom nasjonale initiativ), og ingen enhetlige ordninger for utveksling av opplysninger på unionsplan som er tilpasset behovene til et integrert finanssystem. Derfor er det viktig å styrke disse kommunikasjonskanalene.

34) Finansielle enheter bør derfor oppfordres til å utveksle opplysninger og etterretninger om cybertrusler seg imellom, og til å utnytte i fellesskap individuell kunnskap og praktisk erfaring på strategisk, taktisk og operasjonelt nivå med sikte på å styrke sin kapasitet til i tilstrekkelig grad å vurdere, overvåke, forsvare seg mot og reagere på cybertrusler, gjennom å delta i ordninger for utveksling av opplysninger. Derfor er det nødvendig å gjøre det mulig å opprette frivillige ordninger for utveksling av opplysninger på unionsplan som, når de gjennomføres i pålitelige miljøer, vil hjelpe finansnæringen med å forebygge og reagere i fellesskap på cybertrusler ved raskt å begrense spredningen av IKT-risiko og hindre potensiell smitte gjennom de finansielle kanalene. Disse ordningene bør være i samsvar med gjeldende konkurranseregler i Unionen som fastsatt i kommisjonsmelding av 14. januar 2011 med tittelen «Retningslinjer for anvendelsen av artikkel 101 i traktaten om Den europeiske unions virkemåte på horisontale samarbeidsavtaler», samt med Unionens personvernregler, særlig europaparlaments- og rådsforordning (EU) 2016/679([13]). De bør fungere på grunnlag av et eller flere av de rettsgrunnlagene som er fastsatt i artikkel 6 i den nevnte forordningen, som for eksempel i forbindelse med behandlingen av personopplysninger som er nødvendige for at den dataansvarlige eller en tredjepart kan forfølge en rettmessig interesse i henhold til artikkel 6 nr. 1 bokstav f) i den nevnte forordningen, samt i forbindelse med den behandlingen av personopplysninger som er nødvendig for å oppfylle en rettslig forpliktelse, som påhviler den dataansvarlige, og som er nødvendig for å utføre en oppgave i allmennhetens interesse, eller som et ledd i den dataansvarliges utøvelse av myndighet i henhold til henholdsvis artikkel 6 nr. 1 bokstav c) og e) i den nevnte forordningen.

([13]) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

35) For å opprettholde et høyt nivå av digital operasjonell motstandsdyktighet i hele finanssektoren og samtidig holde tritt med den teknologiske utviklingen bør denne forordningen styre de risikoene som stammer fra alle typer av IKT-tjenester. Med henblikk på dette bør definisjonen av IKT-tjenester i forbindelse med denne forordningen forstås bredt og omfatte digitale tjenester og datatjenester som fortløpende leveres gjennom IKT-systemer, til en eller flere interne eller eksterne brukere. Denne definisjonen bør for eksempel omfatte såkalte «over the top»-tjenester, som faller inn under kategorien elektroniske kommunikasjonstjenester. Den bør bare utelukke den begrensede kategorien av tradisjonelle analoge telefontjenester som kan betegnes som det offentlige telefonnettet («Public Switched Telephone Network» (PSTN)), tjenester innen faste nett, konvensjonelle telefontjenester («Plain Old Telephone Service» (POTS)) eller telefonitjenester innen faste nett.

36) Til tross for den brede dekningen som er fastsatt i denne forordningen, bør det ved anvendelse av reglene om digital operasjonell motstandsdyktighet tas hensyn til de vesentlige forskjellene mellom finansielle enheter når det gjelder deres størrelse og generelle risikoprofil. Som et generelt prinsipp bør finansielle enheter, når de fordeler ressurser og kapasitet for å gjennomføre rammeverket for IKT-risikostyring, på behørig vis veie sine IKT-relaterte behov opp mot sin størrelse og generelle risikoprofil, og arten, omfanget og kompleksiteten av sine tjenester, aktiviteter og drift, mens vedkommende myndigheter bør fortsette å vurdere og gjennomgå tilnærmingen til en slik fordeling.

37) Ytere av kontoopplysningstjenester som nevnt i artikkel 33 nr. 1 i direktiv (EU) 2015/2366 er uttrykkelig omfattet av virkeområdet for denne forordningen, samtidig som det tas hensyn til den spesifikke arten av deres virksomhet og de risikoene som den gir opphav til. Dessuten er e-pengeforetak og betalingsinstitusjoner som er unntatt i henhold til artikkel 9 nr. 1 i europaparlaments- og rådsdirektiv 2009/110/EF([14]) og artikkel 32 nr. 1 i direktiv (EU) 2015/2366, omfattet av denne forordningen, selv om de ikke har fått tillatelse i samsvar med direktiv 2009/110/EF til å utstede elektroniske penger, eller dersom de ikke har fått tillatelse i samsvar med direktiv (EU) 2015/2366 til å yte og utføre betalingstjenester. Postgirokontorer som omhandlet i artikkel 2 nr. 5 punkt 3) i europaparlaments- og rådsdirektiv 2013/36/EU([15]) er imidlertid unntatt fra denne forordningens virkeområde. Den vedkommende myndigheten for betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og ytere av kontoopplysningstjenester som omhandlet i artikkel 33 nr. 1 i direktiv (EU) 2015/2366, bør være den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i direktiv (EU) 2015/2366.

38) Ettersom større finansielle enheter kan ha tilgang til flere ressurser og raskt kan avsette midler til å utvikle styringsstrukturer og innføre ulike foretaksstrategier, er det bare finansielle enheter som ikke er svært små bedrifter i henhold til denne forordningen, som skal pålegges å innføre mer komplekse styringsordninger. Framfor alt er slike enheter bedre rustet til å innføre egne styringsfunksjoner for å føre tilsyn med ordninger med tredjepartsleverandører av IKT-tjenester eller for å ivareta krisehåndtering, organisere sin IKT-risikostyring i henhold til modellen med tre forsvarslinjer eller for å innføre en intern modell for risikostyring og kontroll og underkaste sitt rammeverk for IKT-risikostyring internrevisjon.

39) Noen finansielle enheter drar nytte av unntak eller er underlagt et svært begrenset regelverk i henhold til relevant sektorspesifikk unionsrett. Slike finansielle enheter omfatter forvaltere av alternative investeringsfond som nevnt i artikkel 3 nr. 2 i europaparlaments- og rådsdirektiv 2011/61/EU([16]), forsikrings- og gjenforsikringsforetak som nevnt i artikkel 4 i europaparlaments- og rådsdirektiv 2009/138/EF([17]) og tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen ikke har mer enn 15 medlemmer. I lys av disse unntakene ville det ikke være rimelig å ta med slike finansielle enheter i denne forordningens virkeområde. Dessuten anerkjenner denne forordningen de særtrekkene som gjør seg gjeldende for markedsstrukturen for forsikringsformidling, med det resultatet at forsikringsformidlere, gjenforsikrings-

([14]) Europaparlaments- og rådsdirektiv 2009/110/EU av 16. september 2009 om adgang til å starte og utøve virksomhet som e-pengeforetak og om tilsyn med slik virksomhet, om endring av direktiv 2005/60/EF og 2006/48/EF og om oppheving av direktiv 2000/46/EF (EUT L 267 av 10.10.2009, s. 7).

([15]) Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet som kredittinstitusjon og om tilsyn med kredittinstitusjoner, om endring av direktiv 2002/87/EF og om oppheving av direktiv 2006/48/EF og 2006/49/EF (EUT L 176 av 27.6.2013, s. 338).

([16]) Europaparlaments- og rådsdirektiv 2011/61/EU av 8. juni 2011 om forvaltere av alternative investeringsfond og om endring av direktiv 2003/41/EF og 2009/65/EF og forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 av 1.7.2011, s. 1).

([17]) Europaparlaments- og rådsdirektiv 2009/138/EF av 25. november 2009 om adgang til å starte og utøve virksomhet innen forsikring og gjenforsikring (Solvens II) (EUT L 335 av 17.12.2009, s. 1).

formidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, og som kan regnes som svært små bedrifter eller som små eller mellomstore bedrifter, ikke bør være omfattet av denne forordningen.

40) Ettersom de enhetene som er nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU, er unntatt fra det nevnte direktivets virkeområde, bør medlemsstatene derfor kunne velge å unnta slike enheter som befinner seg på deres respektive territorier, fra denne forordningens anvendelse.

41) For å tilpasse denne forordningen til virkeområdet for europaparlaments- og rådsdirektiv 2014/65/EU([18]) er det også hensiktsmessig å unnta fysiske og juridiske personer som er nevnt i artikkel 2 og 3 i det nevnte direktivet, og som har lov til å levere investeringstjenester uten å måtte innhente tillatelse i henhold til direktiv 2014/65/EU, fra virkeområdet for denne forordningen. I henhold til artikkel 2 i direktiv 2014/65/EU er enheter som anses som finansielle enheter i henhold til denne forordningen, som for eksempel verdipapirsentraler, innretninger for kollektive investeringer eller forsikrings- og gjenforsikringsforetak, imidlertid også unntatt fra dette direktivets virkeområde. Unntak fra denne forordningens virkeområde for personer og enheter nevnt i artikkel 2 og 3 i det nevnte direktivet bør ikke omfatte disse verdipapirsentralene, innretningene for kollektive investeringer eller forsikrings- og gjenforsikringsforetakene.

42) I henhold til sektorspesifikk unionsrett er enkelte finansielle enheter underlagt forenklede krav eller unntak av årsaker knyttet til deres størrelse eller de tjenestene de leverer. Denne kategorien av finansielle enheter omfatter små verdipapirforetak uten innbyrdes forbindelser, små tjenestepensjonsforetak som kan unntas fra virkeområdet for direktiv (EU) 2016/2341 på vilkårene fastsatt av den berørte medlemsstaten i artikkel 5 i det nevnte direktivet, og som forvalter pensjonsordninger som til sammen ikke har mer enn 100 medlemmer, samt institusjoner som er unntatt i henhold til direktiv 2013/36/EU. I samsvar med forholdsmessighetsprinsippet og for å bevare ånden i den sektorspesifikke unionsretten er det derfor også hensiktsmessig å underlegge disse finansielle enhetene et forenklet rammeverk for IKT-risikostyring i henhold til denne forordningen. Den forholdsmessige karakteren av rammeverket for IKT-risikostyring som omfatter disse finansielle enhetene, bør ikke endres av de tekniske reguleringsstandardene som skal utarbeides av de europeiske tilsynsmyndighetene. I samsvar med forholdsmessighetsprinsippet er det dessuten hensiktsmessig også å underlegge betalingsinstitusjoner omhandlet i artikkel 32 nr. 1 i direktiv (EU) 2015/2366 og e-pengeforetak omhandlet i artikkel 9 i direktiv 2009/110/EF som er unntatt i samsvar med nasjonal rett, som innarbeider disse unionsrettsaktene, et forenklet rammeverk for IKT-risikostyring i henhold til denne forordningen, mens betalingsinstitusjoner og e-pengeforetak som ikke er unntatt i samsvar med sin respektive nasjonale rett, som innarbeider sektorspesifikk unionsrett, bør overholde det generelle rammeverket fastsatt i denne forordningen.

43) På samme måte bør finansielle enheter som anses som svært små bedrifter, eller som er underlagt det forenklede rammeverket for IKT-risikostyring i henhold til denne forordningen, ikke være forpliktet til å opprette en funksjon for å overvåke de ordningene som de har inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester; eller til å utpeke et medlem av den øverste ledelsen som skal være ansvarlig for å føre tilsyn med den tilhørende risikoeksponeringen og relevant dokumentasjon; til å overføre ansvaret for å styre og overvåke IKT-risiko til en kontrollfunksjon og sikre et passende nivå av uavhengighet for den kontrollfunksjonen for å unngå interessekonflikter; til å dokumentere og gjennomgå minst én gang i året rammeverket for IKT-risikostyring; til regelmessig å underlegge rammeverket for IKT-risikostyring internrevisjon; til å foreta grundige vurderinger etter store endringer i deres infrastruktur og prosesser for nettverk og informasjon; til regelmessig å foreta risikoanalyser av eldre IKT-systemer; til å underkaste gjennomføringen av planer for IKT-respons og -gjenoppretting uavhengig internrevisjon; til å ha en krisestyringsfunksjon, til å utvide testingen av kontinuitet i virksomheten og respons- og gjenopprettingsplaner for å fange opp scenarioer med overflytting mellom den primære IKT-infrastrukturen og redundante anlegg; til å innberette til vedkommende myndigheter, på deres anmodning, et overslag over samlede årlige kostnader og tap forårsaket av alvorlige IKT-relaterte hendelser, til å opprettholde redundant IKT-kapasitet; til å informere nasjonale vedkommende myndigheter om gjennomførte endringer etter gjennomgåelsen av IKT-relaterte hendelser; til fortløpende å overvåke relevant teknologisk utvikling, til å etablere et omfattende program for testing av digital operasjonell motstandsdyktig-

([18]) Europaparlaments- og rådsdirektiv 2014/65/EU av 15. mai 2014 om markeder for finansielle instrumenter og om endring av direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 av 12.6.2014, s. 349).

het som en integrert del av det rammeverket for IKT-risikostyring som er fastsatt i denne forordningen, eller til å vedta og regelmessig gjennomgå en strategi for IKT-tredjepartsrisiko. I tillegg bør svært små bedrifter bare være forpliktet til å vurdere behovet for å opprettholde slik redundant IKT-kapasitet på grunnlag av hvilken risikoprofil de har. Svært små bedrifter bør dra nytte av en mer fleksibel ordning når det gjelder programmer for testing av digital operasjonell motstandsdyktighet. Når de overveier hvilken type og hyppighet av testing som skal utføres, bør de på en passende måte skape balanse mellom målet om å opprettholde en høy digital operasjonell motstandsdyktighet, de tilgjengelige ressursene og sin generelle risikoprofil. Svært små bedrifter og finansielle enheter som er underlagt det forenklede rammeverket for IKT-risikostyring i henhold til denne forordningen, bør unntas fra kravet om å utføre avansert testing av IKT-verktøyer, IKT-systemer og IKT-prosesser på grunnlag av trusselbasert penetrasjonstesting (TLPT), ettersom bare finansielle enheter som oppfyller kriteriene fastsatt i denne forordningen, bør være forpliktet til å utføre slik testing. På bakgrunn av sin begrensede kapasitet bør svært små bedrifter kunne bli enige med tredjepartsleverandøren av IKT-tjenester om å delegere den finansielle enhetens rett til tilgang, inspeksjon og revisjon til en uavhengig tredjepart, som skal utpekes av tredjepartsleverandøren av IKT-tjenester, forutsatt at den finansielle enheten når som helst kan anmode den respektive uavhengige tredjeparten om alle relevante opplysninger og garantier når det gjelder de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår.

44) Ettersom bare de finansielle enhetene som er utpekt med henblikk på avansert testing av digital motstandsdyktighet, bør være forpliktet til å utføre trusselbaserte penetrasjonstester, bør de administrative prosessene og de finansielle kostnadene som er forbundet med gjennomføringen av slike tester, overføres til en liten prosentdel av finansielle enheter.

45) For å sikre full tilpasning av og overordnet sammenheng mellom de finansielle enhetenes forretningsstrategier på den ene side og gjennomføringen av IKT-risikostyring på den annen side, bør de finansielle enhetenes ledelsesorganer være forpliktet til å ha en sentral og aktiv rolle i styringen og tilpasningen av rammeverket for IKT-risikostyring og den samlede strategien for digital operasjonell motstandsdyktighet. Ledelsesorganenes strategi bør ikke bare fokusere på hvordan IKT-systemenes motstandsdyktighet sikres, men bør også omfatte mennesker og prosesser gjennom et sett av retningslinjer som, på hvert foretaksnivå og for alle ansatte, fremmer en sterk følelse av bevissthet om cyberrisikoer og et tilsagn om å overholde en streng cyberhygiene på alle nivåer. Ledelsesorganets endelige ansvar for å styre en finansiell enhets IKT-risiko bør være et overordnet prinsipp for denne helhetlige strategien og omsettes i et fortløpende engasjement hos ledelsesorganet for å kontrollere overvåkingen av IKT-risikostyringen.

46) Dessuten går prinsippet om ledelsesorganets fulle og endelige ansvar for styringen av den finansielle enhetens IKT-risiko hånd i hånd med behovet for å sikre et nivå av IKT-relaterte investeringer og et samlet budsjett for den finansielle enheten som vil gjøre det mulig for den finansielle enheten å oppnå et høyt nivå av digital operasjonell motstandsdyktighet.

47) Med inspirasjon fra relevant beste praksis og relevante retningslinjer, anbefalinger og strategier på internasjonalt og nasjonalt plan samt på sektorplan når det gjelder styring av cyberrisiko, fremmer denne forordningen et sett av prinsipper som letter den overordnede strukturen for IKT-risikostyring. Så lenge finansielle enheters hovedsakelige kapasitet oppfyller de ulike funksjonene for IKT-risikostyring (identifisering, beskyttelse og forebygging, påvisning, respons og gjenoppretting, læring og utvikling samt kommunikasjon) som er fastsatt i denne forordningen, bør finansielle enheter stå fritt til å bruke modeller for IKT-risikostyring som er utformet eller kategorisert på en annen måte.

48) For å holde tritt med et cybertrusselbilde som er i utvikling, bør finansielle enheter opprettholde oppdaterte IKT-systemer som er pålitelige og egnede til ikke bare å garantere den databehandlingen som er nødvendig for deres tjenester, men også for å sikre tilstrekkelig teknologisk motstandsdyktighet, slik at de i tilstrekkelig grad kan håndtere ytterligere behandlingsrelaterte behov på grunn av stressede markedsforhold eller andre vanskelige situasjoner.

49) Effektive planer for kontinuitet i virksomheten og gjenopprettingsplaner er nødvendige for at finansielle enheter omgående og raskt kan finne en løsning på IKT-relaterte hendelser, særlig cyberangrep, gjennom å begrense skaden og prioritere gjenopptakelse av aktiviteter og tiltak for gjenoppretting i samsvar med sine beredskapsplaner. En slik gjenopptakelse bør imidlertid på ingen måte sette integriteten og sikkerheten i nettverks- og informasjonssystemene eller dataenes tilgjengelighet, autentisitet, integritet eller fortrolighet i fare.

50) Selv om denne forordningen gir finansielle enheter mulighet til å fastsette sine mål for gjenopprettingstid og gjenopprettingspunkt på en fleksibel måte og dermed fullt ut ta hensyn til de relevante funksjonenes egenskaper og kritiske verdi og til eventuelle spesifikke forretningsmessige behov, bør den likevel kreve at de foretar en vurdering av den eventuelle samlede innvirkningen på markedseffektiviteten når slike mål fastsettes.

51) Bakmennene bak cyberangrep har en tendens til å søke å oppnå økonomiske gevinster direkte fra kilden og dermed utsette finansielle enheter for vesentlige konsekvenser. For å forhindre at IKT-systemer mister integritet eller blir utilgjengelige, og dermed unngå datainnbrudd og skade på fysisk IKT-infrastruktur, bør finansielle enheters rapportering av alvorlige IKT-relaterte hendelser forbedres betydelig og forenkles. Rapportering av IKT-relaterte hendelser bør harmoniseres gjennom å innføre et krav om at alle finansielle enheter skal rapportere direkte til sine berørte vedkommende myndigheter. Dersom en finansiell enhet er underlagt tilsyn av mer enn én nasjonal vedkommende myndighet, bør medlemsstatene utpeke én enkelt vedkommende myndighet som mottaker av slik rapportering. Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i rådsforordning (EU) nr. 1024/2013([19]), skal legge fram slik rapportering for de nasjonale vedkommende myndighetene, og disse bør deretter oversende rapporten til Den europeiske sentralbank (ESB).

52) Direkte rapportering bør gjøre det mulig for finansielle tilsynsmyndigheter å få umiddelbar tilgang til opplysninger om alvorlige IKT-relaterte hendelser. Finansielle tilsynsmyndigheter bør i sin tur videreformidle opplysninger om alvorlige IKT-relaterte hendelser til offentlige myndigheter som ikke er finansielle myndigheter (som for eksempel vedkommende myndigheter og felles kontaktpunkter i henhold til direktiv (EU) 2022/2555, nasjonale personvernmyndigheter og rettshåndhevende myndigheter i forbindelse med alvorlige IKT-relaterte hendelser av kriminell karakter) for å øke disse myndighetenes bevissthet om slike hendelser og, når det gjelder CSIRT-enheter, for å fremme hurtig bistand, alt etter hva som er relevant. Medlemsstatene bør dessuten kunne bestemme at finansielle enheter selv bør gi slike opplysninger til offentlige myndigheter utenfor området for finansielle tjenester. Disse informasjonsstrømmene bør gi finansielle enheter mulighet til raskt å dra nytte av eventuelle relevante tekniske innspill, råd om avhjelpende tiltak og påfølgende oppfølgning fra slike myndigheter. Opplysninger om alvorlige IKT-relaterte hendelser bør sendes begge veier: Finansielle tilsynsmyndigheter bør gi alle nødvendige tilbakemeldinger eller veiledning til den finansielle enheten, mens de europeiske tilsynsmyndighetene bør dele anonymiserte opplysninger om cybertrusler og sårbarheter knyttet til en hendelse for å bidra til et bredere kollektivt forsvar.

53) Selv om det bør kreves at alle finansielle enheter rapporterer hendelser, forventes det at dette kravet ikke vil påvirke dem alle på samme måte. Relevante vesentlighetsterskler og rapporteringsfrister bør således behørig tilpasses gjennom delegerte rettsakter basert på de tekniske reguleringsstandardene som skal utarbeides av de europeiske tilsynsmyndighetene, med henblikk på å dekke bare alvorlige IKT-relaterte hendelser. I tillegg bør det tas hensyn til de finansielle enhetenes særtrekk når det fastsettes tidsfrister for rapporteringsforpliktelser.

54) Denne forordningen bør fastsette et krav om at kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak skal rapportere alle betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser – som tidligere er rapportert i henhold til direktiv (EU) 2015/2366 – uavhengig av hendelsens IKT-karakter.

([19]) Rådsforordning (EU) nr. 1024/2013 av 15. oktober 2013 om tildeling av særskilte oppgaver til Den europeiske sentralbank i forbindelse med politikken for tilsyn med kredittinstitusjoner (EUT L 287 av 29.10.2013, s. 63).

55) De europeiske tilsynsmyndighetene bør ha til oppgave å vurdere gjennomførbarheten og vilkårene for en mulig sentralisering av rapporter om IKT-relaterte hendelser på unionsplan. En slik sentralisering kan bestå av et felles EU-knutepunkt for rapportering av alvorlige IKT-relaterte hendelser, som enten direkte mottar de relevante rapportene og automatisk underretter nasjonale vedkommende myndigheter, eller som bare sentraliserer relevante rapporter fra de nasjonale vedkommende myndighetene, og dermed oppfyller en koordineringsrolle. De europeiske tilsynsmyndighetene bør ha til oppgave å utarbeide, i samråd med ESB og ENISA, en felles rapport som undersøker muligheten for å opprette et felles EU-knutepunkt.

56) For å oppnå et høyt nivå av digital operasjonell motstandsdyktighet, og i tråd med både de relevante internasjonale standardene (for eksempel G7 Fundamental Elements for Threat-Led Penetration Testing) og med de rammeverkene som anvendes i Unionen, som for eksempel TIBER-EU, bør finansielle enheter regelmessig teste sine IKT-systemer og ansatte som har IKT-relatert ansvar, med hensyn til hvor effektiv deres kapasitet er for forebygging, påvisning, respons og gjenoppretting, for å påvise og håndtere potensielle IKT-sårbarheter. For å gjenspeile de forskjellene som eksisterer på tvers av og innenfor de ulike finansielle delsektorene når det gjelder finansielle enheters nivå av cybersikkerhetsberedskap, bør testing omfatte et bredt spekter av verktøyer og tiltak, alt fra vurderingen av grunnleggende krav (for eksempel sårbarhetsvurderinger og -analyser, analyser av åpen kildekode, vurderinger av nettsikkerhet, mangelanalyser, fysiske sikkerhetsvurderinger, spørreskjemaer og programvareløsninger for skanning, gjennomgåelse av kildekoder dersom det er mulig, scenariobaserte tester, kompatibilitetstesting, ytelsestesting eller ende-til-ende-testing) til mer avansert testing ved hjelp av TLPT. Slike avanserte tester bør bare kreves av finansielle enheter som utfra et IKT-perspektiv er modne nok til å kunne gjennomføre dem på en rimelig måte. Den testingen av den digitale operasjonelle motstandsdyktigheten som kreves i henhold til denne forordningen, bør derfor være mer krevende for de finansielle enhetene som oppfyller kriteriene fastsatt i denne forordningen (for eksempel store, systemiske og IKT-modne kredittinstitusjoner, børser, verdipapirsentraler og sentrale motparter), enn for andre finansielle enheter. Samtidig bør testing av digital operasjonell motstandsdyktighet ved hjelp av TLPT være mer relevant for finansielle enheter som driver virksomhet innenfor sentrale delsektorer for finansielle tjenester, og som spiller en systemisk rolle (for eksempel betalinger, bankvirksomhet samt clearing og oppgjør), og mindre relevant for andre delsektorer (for eksempel kapitalforvaltere og kredittvurderingsbyråer).

57) Finansielle enheter som er involvert i virksomhet over landegrensene, og som utøver etableringsadgang eller tjenesteyting i Unionen, bør oppfylle et felles sett av krav til avansert testing (TLPT) i hjemstaten, som bør omfatte IKT-infrastrukturer i alle jurisdiksjoner der det grenseoverskridende finanskonsernet driver virksomhet i Unionen, hvilket innebærer at slike grenseoverskridende finanskonsern bare kan pådra seg relaterte IKT-testkostnader i én jurisdiksjon.

58) For å utnytte den ekspertisen som allerede er ervervet av visse vedkommende myndigheter, særlig med hensyn til gjennomføringen av TIBER-EU-rammeverket, bør denne forordningen gi medlemsstatene mulighet til å utpeke en felles offentlig myndighet som ansvarlig i finanssektoren på nasjonalt plan for alle TLPT-relaterte spørsmål eller, dersom ingen slik myndighet utpekes, å utpeke vedkommende myndigheter til å delegere utførelsen av TLPT-relaterte oppgaver til en annen nasjonal finansiell vedkommende myndighet.

59) Ettersom denne forordningen ikke krever at finansielle enheter skal dekke alle kritiske eller viktige funksjoner i én enkelt trusselbasert penetrasjonstest, bør finansielle enheter stå fritt til å bestemme hvilke og hvor mange kritiske eller viktige funksjoner som bør være omfattet av en slik test.

60) Samlet testing som definert i denne forordningen, som innebærer deltakelse av flere finansielle enheter i en TLPT, og for hvilke en tredjepartsleverandør av IKT-tjenester kan inngå kontraktsregulerte ordninger direkte med en ekstern tester, bør bare tillates dersom kvaliteten eller sikkerheten for de tjenestene som tredjepartsleverandør av IKT-tjenester leverer til kunder som er enheter som faller utenfor virkeområdet for denne forordningen, eller for fortroligheten for data som er knyttet til slike tjenester, med rimelighet kan forventes å bli negativt påvirket. Samlet testing bør også være omfattet av garantier (under ledelse av én utpekt finansiell enhet, kalibrering av antall deltakende finansielle enheter) for å sikre en streng testprosess for de involverte finansielle enhetene som oppfyller målene for TLPT i henhold til denne forordningen.

61) For å utnytte interne ressurser som er tilgjengelige på foretaksnivå, bør denne forordningen tillate bruk av interne testere for å utføre TLPT, forutsatt at tilsynsmyndigheten godkjenner det, at det ikke foreligger noen interessekonflikter, og at anvendelsen av interne og eksterne testere alternerer regelmessig (hver tredje test), samtidig som formidleren av trusseletterretninger i TLPT alltid skal være ekstern i forhold til den finansielle enheten. Ansvaret for å utføre en TLPT bør fullt ut ligge hos den finansielle enheten. Erklæringer fra myndighetene bør utelukkende ha til formål å sikre gjensidig anerkjennelse og bør ikke utelukke eventuelle oppfølgingstiltak som er nødvendige for å håndtere den IKT-risikoen som den finansielle enheten er eksponert for, og de bør heller ikke ses på som en tilsynsmessig godkjenning av en finansiell enhets kapasitet til å styre og begrense IKT-risiko.

62) For å sikre en forsvarlig overvåking av IKT-tredjepartsrisiko i finanssektoren er det nødvendig å fastsette en rekke prinsippbaserte regler for å veilede finansielle enheter når de overvåker risiko som oppstår i forbindelse med funksjoner som er utkontraktert til tredjepartsleverandører av IKT-tjenester, særlig for IKT-tjenester som støtter kritiske eller viktige funksjoner, samt mer generelt i forbindelse med avhengighet av IKT-tredjeparter.

63) For å håndtere kompleksiteten i de ulike kildene til IKT-risiko, samtidig som det tas hensyn til mangfoldet av leverandører av teknologiske løsninger som muliggjør en smidig levering av finansielle tjenester, bør denne forordningen omfatte et bredt spekter av tredjepartsleverandører av IKT-tjenester, herunder leverandører av skytjenester, programvare, dataanalysetjenester og leverandører av datasentertjenester. Ettersom finansielle enheter på en effektiv og sammenhengende måte bør identifisere og styre alle typer risiko, herunder i forbindelse med IKT-tjenester som anskaffes innenfor et finanskonsern, bør det likeledes presiseres at foretak som er en del av et finanskonsern og hovedsakelig leverer IKT-tjenester til morforetaket, eller til datterforetak eller filialer av morforetaket, samt finansielle enheter som leverer IKT-tjenester til andre finansielle enheter, også bør anses som tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen. Endelig, på bakgrunn av at markedet for betalingstjenester i stadig større grad blir avhengig av komplekse tekniske løsninger, og med hensyn til nye typer betalingstjenester og betalingsrelaterte løsninger, bør deltakere i økosystemet for betalingstjenester som leverer betalingsbehandlingstjenester, eller som driver betalingsinfrastrukturer, også anses som tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen, med unntak av sentralbanker når de driver betalings- eller verdipapiroppgjørssystemer, og offentlige myndigheter når de leverer IKT-relaterte tjenester i forbindelse med utførelsen av statlige funksjoner.

64) En finansiell enhet bør til enhver tid fortsatt være fullt ansvarlig for å overholde sine forpliktelser i henhold til denne forordningen. Finansielle enheter bør anvende en forholdsmessig tilnærming i forbindelse med overvåkingen av de risikoene som oppstår hos tredjepartsleverandører av IKT-tjenester, gjennom å ta behørig hensyn til karakteren på og omfanget av, kompleksiteten hos og betydningen av sin IKT-relaterte avhengighet, tjenestenes kritiske verdi eller betydningen av de prosessene eller funksjonene som er omfattet av de kontraktsregulerte ordningene, og, i siste instans, på grunnlag av en grundig vurdering av en eventuell potensiell innvirkning på kontinuiteten og kvaliteten til finansielle tjenester på individuelt nivå og på konsernnivå, alt etter hva som er relevant.

65) Gjennomføringen av en slik overvåking bør følge en strategisk tilnærming til IKT-tredjepartsrisiko som formaliseres ved at den finansielle enhetens ledelsesorgan vedtar en særlig strategi for IKT-tredjepartsrisiko, som tar utgangspunkt i en løpende screening av all avhengighet av IKT-tredjeparter. For å øke tilsynsmyndighetens bevissthet om avhengighet av IKT-tredjeparter og ytterligere støtte arbeidet i forbindelse med overvåkingsrammeverket som fastsatt i henhold til denne forordningen, bør alle finansielle enheter være forpliktet til å føre et register over opplysninger om alle kontraktsregulerte ordninger som gjelder bruken av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester. Finansielle tilsynsmyndigheter bør kunne anmode om tilgang til hele registret eller be om bestemte avsnitt av registeret, og dermed innhente vesentlige opplysninger for å få en bredere forståelse av finansielle enheters IKT-avhengighet.

66) En grundig analyse før kontraktinngåelse bør underbygge og gå forut for den formelle inngåelsen av kontraktsregulerte ordninger, særlig gjennom å fokusere på elementer som kritisk verdi eller betydningen av de tjenestene som støttes av den påtenkte IKT-kontrakten, de nødvendige tilsynsgodkjenningene eller andre forhold, den mulige konsentrasjonsrisikoen som følger med, samt å anvende tilbørlig aktsomhet i prosessen med utvelgelse og vurdering av tredjepartsleverandører av IKT-tjenester og vurdering av potensielle interessekonflikter. I forbindelse med kontraktsregulerte ordninger som gjelder kritiske eller viktige funksjoner, bør finansielle enheter ta hensyn til hvorvidt tredjepartsleverandører av IKT-tjenester bruker de nyeste og høyeste standardene om informasjonssikkerhet. Oppsigelse av kontraktsregulerte ord-

ninger kan som et minimum være forårsaket av en rekke omstendigheter som viser mangler hos tredjepartsleverandøren av IKT-tjenester, særlig vesentlige overtredelser av lover eller kontraktsvilkår, omstendigheter som avslører en potensiell endring i utførelsen av de funksjonene som er fastsatt i kontraktsregulerte ordninger, tegn på svakheter hos tredjepartsleverandøren av IKT-tjenester i den samlede IKT-risikostyringen eller omstendigheter som tyder på at den berørte vedkommende myndigheten ikke er i stand til å føre effektivt tilsyn med den finansielle enheten.

67) For å håndtere den systemiske virkningen av den konsentrasjonsrisikoen som er forbundet med IKT-tredjeparter, fremmer denne forordningen en balansert løsning ved hjelp av en fleksibel og gradvis tilnærming til en slik konsentrasjonsrisiko, ettersom innføringen av strenge tak eller strenge begrensninger kan hindre utøvelsen av virksomhet og begrense kontraktsfriheten. Finansielle enheter bør foreta en grundig vurdering av sine påtenkte kontraktsregulerte ordninger for å fastslå sannsynligheten for at en slik risiko oppstår, herunder ved hjelp av inngående analyser av underleverandøravtaler, særlig når de inngås med tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland. På det nåværende tidspunktet, og med henblikk på å finne en rimelig balanse mellom nødvendigheten av å bevare kontraktsfriheten og å sikre den finansielle stabiliteten, anses det ikke som hensiktsmessig å fastsette regler om strenge tak og strenge begrensninger for eksponeringer mot IKT-tredjeparter. I forbindelse med overvåkingsrammeverket bør en hovedovervåker som er utpekt i henhold til denne forordningen, med hensyn til kritiske tredjepartsleverandører av IKT-tjenester, være særlig oppmerksom på å oppnå full forståelse for omfanget av gjensidig avhengighet, påvise særlige tilfeller der en høy grad av konsentrasjon av kritiske tredjepartsleverandører av IKT-tjenester i Unionen sannsynligvis vil legge press på stabiliteten og integriteten i Unionens finanssystem, og opprettholde en dialog med kritiske tredjepartsleverandører av IKT-tjenester der denne spesifikke risikoen er identifisert.

68) For regelmessig å vurdere og overvåke hvorvidt en tredjepartsleverandør av IKT-tjenester har evnen til å levere tjenester på en sikker måte til en finansiell enhet, og uten at dette har negative virkninger på en finansiell enhets digitale operasjonelle motstandsdyktighet, bør flere viktige kontraktsmessige elementer med tredjepartsleverandører av IKT-tjenester harmoniseres. En slik harmonisering bør omfatte minst de områdene som er svært viktige for at den finansielle enheten skal kunne gjennomføre en fullstendig overvåking av de risikoene som kan oppstå gjennom tredjepartsleverandøren av IKT-tjenester, sett i lys av en finansiell enhets behov for å sikre sin digitale motstandsdyktighet ettersom den er helt avhengig av de mottatte IKT-tjenestenes stabilitet, funksjonalitet, tilgjengelighet og sikkerhet.

69) Når finansielle enheter og tredjepartsleverandører av IKT-tjenester reforhandler kontraktsregulerte ordninger med henblikk på oppnå samsvar med kravene i denne forordningen, bør de sikre at de viktige kontraktsbestemmelsene som er fastsatt i denne forordningen, er omfattet.

70) Definisjonen av «kritisk eller viktig funksjon» i denne forordningen omfatter de «kritiske funksjonene» som er definert i artikkel 2 nr. 1 punkt 35) i europaparlaments- og rådsdirektiv 2014/59/EU([20]). Funksjoner som anses som kritiske i henhold til direktiv 2014/59/EU, er derfor tatt med i definisjonen av kritiske funksjoner i henhold til denne forordningen.

71) Uavhengig av hvor kritisk eller viktig den funksjonen som støttes av IKT-tjenestene, er, bør kontraktsregulerte ordninger særlig inneholde en spesifikasjon av de fullstendige beskrivelsene av funksjoner og tjenester, av stedene der slike funksjoner leveres, og hvor dataene skal behandles, samt beskrivelser av tjenestenivå. Andre grunnleggende elementer for å muliggjøre en finansiell enhets overvåking av IKT-tredjepartsrisiko er kontraktsbestemmelser som spesifiserer hvordan adgang, tilgjengelighet, integritet, sikkerhet og vern av personopplysninger sikres av tredjepartsleverandøren av IKT-tjenester, bestemmelser som fastsetter de relevante garantiene for å muliggjøre tilgang til, gjenoppretting og tilbakeføring av data ved insolvens, krisehåndtering eller opphør av virksomheten til tredjepartsleverandøren av IKT-tjenester, samt bestemmelser som krever at tredjepartsleverandøren av IKT-tjenester skal yte bistand i tilfelle av IKT-

([20]) Europaparlaments- og rådsdirektiv 2014/59/EU av 15. mai 2014 om fastsettelse av en ramme for gjenoppretting og krisehåndtering av kredittinstitusjoner og verdipapirforetak og om endring av rådsdirektiv 82/891/EØF, europaparlaments- og rådsdirektiv 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 og europaparlaments- og rådsforordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 av 12.6.2014, s. 190).

hendelser i forbindelse med tjenestene som leveres, uten ekstra kostnad eller til en kostnad som er fastsatt på forhånd, bestemmelser om forpliktelsen for tredjepartsleverandøren av IKT-tjenester til å samarbeide fullt ut med vedkommende myndigheter og krisehåndteringsmyndigheter i den finansielle enheten og bestemmelser om oppsigelsesrett og tilhørende minste oppsigelsesfrist for kontraktsregulerte ordninger i samsvar med forventningene til vedkommende myndigheter og krisehåndteringsmyndigheter.

72) I tillegg til slike kontraktsbestemmelser, og med henblikk på å sikre at finansielle enheter fortsatt har full kontroll over all utvikling som skjer på tredjepartsnivå, og som kan svekke deres IKT-sikkerhet, bør kontraktene om levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, også inneholde bestemmelser om følgende: En fullstendig beskrivelse av tjenestenivået, med nøyaktige kvantitative og kvalitative ytelsesmål, for å muliggjøre uten unødig forsinkelse egnede korrigerende tiltak dersom de avtalte tjenestenivåene ikke overholdes, relevante oppsigelsesfrister og rapporteringsforpliktelser for tredjepartsleverandøren av IKT-tjenester for hendelser som kan ha en vesentlig innvirkning på hvorvidt tredjepartsleverandøren av IKT-tjenester har evnen til å levere de respektive IKT-tjenestene på en effektiv måte, et krav om at tredjepartsleverandøren av IKT-tjenester skal gjennomføre og teste beredskapsplaner for virksomheten og innføre IKT-sikkerhetstiltak, IKT-verktøyer og IKT-retningslinjer som muliggjør sikker levering av tjenester, samt delta og samarbeide fullt ut i den TLPT-en som utføres av den finansielle enheten.

73) Kontrakter om levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, bør også inneholde bestemmelser som gir den finansielle enheten, eller en utpekt tredjepart, rett til tilgang, inspeksjon og revisjon, og rett til å ta kopier som avgjørende verktøyer i de finansielle enhetenes løpende overvåking av de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår, kombinert med sistnevntes fulle samarbeid i forbindelse med inspeksjonene. Tilsvarende bør den finansielle enhetens vedkommende myndighet ha rett til, som følge av varsler, å inspisere og foreta revisjon av tredjepartsleverandøren av IKT-tjenester, med forbehold om vern av fortrolige opplysninger.

74) Slike kontraktsregulerte ordninger bør også inneholde særskilte exit-strategier som særlig muliggjør obligatoriske overgangsperioder der tredjepartsleverandører av IKT-tjenester bør fortsette å levere de relevante tjenestene med henblikk på å redusere risikoen for forstyrrelser i den finansielle enheten, eller for å gi sistnevnte mulighet til å bytte til andre tredjepartsleverandører av IKT-tjenester på en effektiv måte, eller alternativt bytte til interne løsninger som er forenlige med den leverte IKT-tjenestens kompleksitet. Finansielle enheter som er omfattet av direktiv 2014/59/EU, bør dessuten sikre at de relevante kontraktene for IKT-tjenester er robuste og kan håndheves fullt ut ved krisehåndtering av disse finansielle enhetene. I samsvar med krisehåndteringsmyndighetenes forventninger bør disse finansielle enhetene derfor sikre at de relevante kontraktene for IKT-tjenester er motstandsdyktige mot krisehåndtering. Så lenge disse finansielle enhetene fortsetter å oppfylle sine betalingsforpliktelser, bør de blant annet sikre at de relevante kontraktene for IKT-tjenester inneholder bestemmelser om at de ikke kan sies opp, ikke kan oppheves midlertidig og ikke kan endres på grunn av omstrukturering eller krisehåndtering.

75) Videre kan frivillig bruk av standardavtalevilkår som offentlige myndigheter eller Unionens institusjoner har utarbeidet, særlig bruken av kontraktsvilkår som Kommisjonen har utarbeidet for skytjenester, gi de finansielle enhetene og tredjepartsleverandørene av IKT-tjenester mer trygghet gjennom å øke rettssikkerheten når det gjelder bruken av skytjenester i finanssektoren, i fullt samsvar med de kravene og forventningene som er fastsatt i unionsregelverket for finansielle tjenester. Utarbeidingen av standardavtalevilkår bygger på tiltak som allerede var planlagt i handlingsplanen for FinTech fra 2018, som kunngjorde Kommisjonens hensikt om å fremme og tilrettelegge for utarbeidingen av standardavtalevilkår for finansielle enheters utkontraktering av skytjenester, basert på den tverrsektorielle innsatsen fra berørte parter på området for skytjenester, som Kommisjonen har bidratt til med deltakelse fra finanssektoren.

76) For å fremme tilnærming og effektivitet med hensyn til tilsynsstrategier når det gjelder styring av IKT-tredjepartsrisiko i finanssektoren, samt for å styrke den digitale operasjonelle motstandsdyktigheten i finansielle enheter som er avhengige av kritiske tredjepartsleverandører av IKT-tjenester for levering av IKT-tjenester som støtter leveringen av finansielle tjenester, og dermed bidra til å bevare stabiliteten i Unionens finanssystem og integriteten på det indre marked for finansielle tjenester, bør kritiske tredjepartsleverandører av IKT-tjenester være underlagt Unionens overvåkingsrammeverk.

Selv om opprettelsen av overvåkingsrammeverket er begrunnet i merverdien av å treffe tiltak på unionsplan og av de særlige forholdene som gjør seg gjeldende for bruken av IKT-tjenester, og den rollen de spiller i forbindelse med levering av finansielle tjenester, bør det samtidig bemerkes at denne løsningen virker å være egnet bare innenfor rammen av denne forordningen som spesifikt omhandler digital operasjonell motstandsdyktighet i finanssektoren. Et slikt overvåkingsrammeverk bør imidlertid ikke anses som en ny modell for Unionens tilsyn på andre områder av finansielle tjenester og finansiell virksomhet.

77) Overvåkingsrammeverket bør bare få anvendelse på kritiske tredjepartsleverandører av IKT-tjenester. Det bør derfor være en utpekingsordning som tar hensyn til omfanget og arten av finanssektorens avhengighet av slike tredjepartsleverandører av IKT-tjenester. Denne ordningen bør innebære et sett av kvantitative og kvalitative kriterier for å fastsette parametrer for kritisk verdi som grunnlag for inkludering i overvåkingsrammeverket. For å sikre at denne vurderingen er nøyaktig, og uavhengig av foretaksstrukturen til tredjepartsleverandøren av IKT-tjenester, bør slike kriterier, når det gjelder en tredjepartsleverandør av IKT-tjenester som er en del av et større konsern, ta hensyn til hele konsernstrukturen hos tredjepartsleverandøren av IKT-tjenester. På den ene side bør kritiske tredjepartsleverandører av IKT-tjenester som ikke automatisk utpekes i henhold til disse kriteriene, ha mulighet til å delta i overvåkingsrammeverket på frivillig basis, men på den annen side bør tredjepartsleverandører av IKT-tjenester som allerede er omfattet av overvåkingsrammer som støtter utførelsen av oppgavene til Det europeiske system av sentralbanker som nevnt i artikkel 127 nr. 2 i TEUV, unntas.

78) På samme måte bør finansielle enheter som leverer IKT-tjenester til andre finansielle enheter, selv om de tilhører kategorien av tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen, også unntas fra overvåkingsrammeverket ettersom de allerede er omfattet av tilsynsordninger som er opprettet gjennom det relevante unionsregelverket for finansielle tjenester. Dersom det er relevant, bør vedkommende myndigheter i forbindelse med sin tilsynsvirksomhet ta hensyn til den IKT-risikoen som finansielle enheter som leverer IKT-tjenester, utgjør for finansielle enheter. På samme måte bør det på grunn av de eksisterende ordningene for risikoovervåking på konsernnivå innføres samme unntak for tredjepartsleverandører av IKT-tjenester som leverer tjenester hovedsakelig til enheter i sitt egen konsern. Tredjepartsleverandører av IKT-tjenester som utelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheter som bare er aktive i denne medlemsstaten, bør også unntas fra utpekingsordningen på grunn av sin begrensede virksomhet og manglende innvirkning over landegrensene.

79) Den digitale omstillingen av finansielle tjenester har ført til et helt enestående nivå når det gjelder bruk og avhengighet av IKT-tjenester. Ettersom det er blitt utenkelig å levere finansielle tjenester uten bruk av skytjenester, programvareløsninger og datarelaterte tjenester, har Unionens finansielle økosystem blitt uløselig forbundet med visse IKT-tjenester som leveres av tredjepartsleverandører av IKT-tjenester. Noen av disse leverandørene er innovatører når det gjelder å utvikle og anvende IKT-basert teknologi, og spiller en viktig rolle i leveringen av finansielle tjenester eller er blitt integrert i verdikjeden for finansielle tjenester. De er dermed blitt avgjørende for stabiliteten og integriteten i Unionens finanssystem. Denne utbredte avhengigheten av tjenester levert av kritiske tredjepartsleverandører av IKT-tjenester, i kombinasjon med den gjensidige avhengigheten mellom informasjonssystemene til ulike markedsoperatører, skaper en direkte og potensielt alvorlig risiko for Unionens system for finansielle tjenester og for kontinuiteten i leveringen av finansielle tjenester dersom kritiske tredjepartsleverandører av IKT-tjenester skulle bli påvirket av driftsforstyrrelser eller alvorlige cyberhendelser. Cyberhendelser har en særegen evne til å formere seg og spre seg i hele finanssystemet i et betydelig raskere tempo enn andre typer risikoer som overvåkes i finanssektoren, og kan strekke seg over sektorer og utover geografiske grenser. De har potensial til å utvikle seg til en systemisk krise der tilliten til finanssystemet uthules på grunn av forstyrrelser av funksjoner som støtter realøkonomien, eller på grunn av betydelige finansielle tap som når et nivå som finanssystemet ikke kan klare, eller som krever omfattende tiltak for å absorbere kraftige sjokk. For å hindre at disse scenarioene inntreffer og dermed setter Unionens finansielle stabilitet og integritet i fare, er det viktig å sikre tilnærming av tilsynspraksis for IKT-tredjepartsrisiko i finanssektoren, særlig gjennom nye regler som gjør det mulig for Unionen å ha oversyn med kritiske tredjepartsleverandører av IKT-tjenester.

80) Overvåkingsrammeverket avhenger for en stor del av graden av samarbeid mellom hovedovervåkeren og den kritiske tredjepartsleverandøren av IKT-tjenester som leverer tjenester til finansielle enheter, som påvirker leveransen av finansielle tjenester. Vellykket overvåking er blant annet basert på hovedovervåkerens evne til effektivt å gjennomføre overvåkingsoppdrag og inspeksjoner for å vurdere de reglene, kontrollene og prosessene som brukes av de kritiske tredjepartsleverandørene av IKT-tjenester, samt å vurdere den potensielle kumulative virkningen av deres aktiviteter på den finansielle stabiliteten og finanssystemets integritet. Samtidig er det svært viktig at kritiske tredjepartsleverandører av IKT-tjenester følger hovedovervåkerens anbefalinger og imøtekommer dennes betenkeligheter. Ettersom manglende samarbeid fra en kritisk tredjepartsleverandør av IKT-tjenester som leverer tjenester som påvirker leveringen av finansielle tjenester, som for eksempel avslag på å gi tilgang til sine lokaler eller å sende inn opplysninger, til slutt vil frata hovedovervåkeren dens viktige verktøyer for å vurdere IKT-tredjepartsrisiko og kan ha en negativ innvirkning på finanssystemets finansielle stabilitet og integritet, er det også nødvendig å innføre en passende sanksjonsordning.

81) På denne bakgrunn bør hovedovervåkerens behov for å ilegge overtredelsesgebyr for å tvinge kritiske tredjepartsleverandører av IKT-tjenester til å oppfylle forpliktelsene om åpenhet og tilgang som fastsatt i denne forordningen, ikke trues av vanskeligheter som oppstår som følge av håndhevingen av disse overtredelsesgebyrene i forbindelse med kritiske tredjepartsleverandører av IKT-tjenester som er etablert i tredjeland. For å sikre at slike sanksjoner kan håndheves, og for å muliggjøre en rask innføring av framgangsmåter som opprettholder retten til forsvar for de kritiske tredjepartsleverandørene av IKT-tjenester i forbindelse med utpekingsordningen og utstedelsen av anbefalinger, bør det kreves at disse kritiske tredjepartsleverandørene av IKT-tjenester som leverer tjenester til finansielle enheter, som påvirker leveringen av finansielle tjenester, skal være forpliktet til å opprettholde en tilstrekkelig virksomhet i Unionen. På grunn av tilsynets karakter og mangelen på sammenlignbare ordninger i andre jurisdiksjoner finnes det ingen egnede alternative ordninger for å nå dette målet gjennom et effektivt samarbeid med finansielle tilsynsmyndigheter i tredjeland om overvåkingen av virkninger av de digitale operasjonelle risikoene som systemviktige tredjepartsleverandører av IKT-tjenester, som anses som kritiske tredjepartsleverandører av IKT-tjenester etablert i tredjeland, utgjør. For å fortsette å levere IKT-tjenester til finansielle enheter i Unionen bør derfor en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med denne forordningen, senest tolv måneder etter utpekingen, treffe alle nødvendige tiltak for å sikre sin registrering som foretak i Unionen gjennom å opprette et datterforetak som definert i gjeldende unionsregelverk, nærmere bestemt i europaparlaments- og rådsdirektiv 2013/34/EU([21]).

82) Kravet om å opprette et datterforetak i Unionen bør ikke hindre den kritiske tredjepartsleverandøren av IKT-tjenester fra å levere IKT-tjenester og tilhørende teknisk støtte fra anlegg og infrastruktur som ligger utenfor Unionen. Denne forordningen innfører ikke noen plikt om datalokalisering ettersom den ikke krever at datalagring eller databehandling skal finne sted i Unionen.

83) Kritiske tredjepartsleverandører av IKT-tjenester bør kunne tilby IKT-tjenester fra hvor som helst i verden, ikke nødvendigvis eller ikke bare fra lokaler i Unionen. Overvåkingsvirksomheten bør først gjennomføres i lokaler som ligger i Unionen, og gjennom samhandling med enheter lokalisert i Unionen, herunder datterforetak etablert av kritiske tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen. Slike tiltak i Unionen kan imidlertid være utilstrekkelige for at hovedovervåkeren fullt ut og på en effektiv måte skal kunne utføre sine oppgaver i henhold til denne forordningen. Hovedovervåkeren bør derfor også kunne utøve sin relevante myndighet i tredjeland. Utøvelsen av denne myndigheten i tredjeland bør gjøre det mulig for hovedovervåkeren å undersøke de fasilitetene fra hvilke IKT-tjenestene eller de tekniske supporttjenestene faktisk leveres eller forvaltes av den kritiske tredjepartsleverandøren av IKT-tjenester, og bør gi hovedovervåkeren omfattende og operasjonell forståelse av IKT-risikostyringen hos den kritiske tredjepartsleverandøren av IKT-tjenester. Hovedovervåkerens mulighet, i egenskap av unionsbyrå, til å utøve myndighet utenfor Unionens territorium bør være behørig avgrenset av relevante vilkår, særlig samtykke fra den berørte kritiske tredjepartsleverandøren av IKT-tjenester. På samme måte bør de berørte myndighetene i tredjelandet underrettes om, og ikke ha innvendinger mot, at hovedovervåkerens virksomhet utøves på tredjelandets eget territorium. For å sikre en effektiv gjennomføring, og uten at det berører den respektive myndigheten til Unionens institusjoner og medlemsstatene, må imidlertid slik myndighet også være fullt forankret i inngåelsen av ordninger om administrativt samarbeid med de berørte myndighetene i det berørte tredjelandet. Denne forordningen bør derfor gjøre det mulig for de europeiske til-

([21]) Europaparlaments- og rådsdirektiv 2013/34/EU av 26. juni 2013 om årsregnskaper, konsernregnskaper og tilhørende rapporter for visse typer foretak, om endring av europaparlaments- og rådsdirektiv 2006/43/EF og om oppheving av rådsdirektiv 78/660/EØF og 83/349/EØF (EUT L 182 av 29.6.2013, s. 19).

synsmyndighetene å inngå ordninger om administrativt samarbeid med de berørte myndighetene i tredjeland som ikke på annen måte bør skape rettslige forpliktelser for Unionen og dens medlemsstater.

84) For å lette kommunikasjonen med hovedovervåkeren og for å sikre tilstrekkelig representasjon, bør kritiske tredjepartsleverandører av IKT-tjenester som er en del av et konsern, utpeke en juridisk person som sitt koordineringspunkt.

85) Overvåkingsrammeverket bør ikke berøre medlemsstatenes myndighet til å gjennomføre sine egne overvåkings- eller monitoreringsoppdrag med hensyn til tredjepartsleverandører av IKT-tjenester som ikke er utpekt som kritiske i henhold til denne forordningen, men som anses som viktige på nasjonalt plan.

86) For å utnytte den institusjonelle flerlagsarkitekturen på området finansielle tjenester bør Felleskomiteen for de europeiske tilsynsmyndighetene fortsette å sikre en samlet koordinering på tvers av sektorer i alle spørsmål som gjelder IKT-risiko, i samsvar med sine oppgaver når det gjelder cybersikkerhet. Dette arbeidet bør støttes av en ny underkomité («overvåkingsforumet») som utfører forberedende arbeid både for de enkelte beslutningene rettet til kritiske tredjepartsleverandører av IKT-tjenester, og for utstedelse av kollektive anbefalinger, særlig i forbindelse med referansemåling av overvåkingsprogrammene for kritiske tredjepartsleverandører av IKT-tjenester, og identifisering av beste praksis for håndtering av spørsmål om IKT-konsentrasjonsrisiko.

87) For å sikre at kritiske tredjepartsleverandører av IKT-tjenester overvåkes på en hensiktsmessig og effektiv måte på unionsplan, fastsetter denne forordningen at hver og en av de tre europeiske tilsynsmyndighetene kan utpekes som hovedovervåker. Den individuelle tildelingen av en kritisk tredjepartsleverandør av IKT-tjenester til en av de tre europeiske tilsynsmyndighetene bør være et resultat av en vurdering av den overveiende andelen av finansielle enheter som driver virksomhet i finanssektorene, som den europeiske tilsynsmyndigheten har ansvaret for. Denne tilnærmingen bør føre til en balansert fordeling av oppgaver og ansvar mellom de tre europeiske tilsynsmyndighetene i forbindelse med utøvelsen av overvåkingsfunksjonene og bør på beste måte utnytte de menneskelige ressursene og den tekniske ekspertisen som finnes i hver av de tre europeiske tilsynsmyndighetene.

88) Hovedovervåkere bør tildeles nødvendig myndighet til å foreta undersøkelser, gjennomføre stedlige inspeksjoner og eksterne inspeksjoner i lokaler og på driftssteder hos kritiske tredjepartsleverandører av IKT-tjenester samt å innhente fullstendige og oppdaterte opplysninger. Denne myndigheten bør gjøre det mulig for hovedovervåkeren å få reell innsikt i typen, omfanget og virkningen av IKT-tredjepartsrisikoen for finansielle enheter og til syvende og sist for Unionens finanssystem. Å gi de europeiske tilsynsmyndighetene den ledende overvåkerrollen er en forutsetning for å forstå og håndtere den systemiske dimensjonen av IKT-risiko i finanssektoren. Den innvirkningen som kritiske tredjepartsleverandører av IKT-tjenester har på Unionens finanssektor, og de potensielle problemene som skyldes den derav følgende IKT-konsentrasjonsrisikoen, krever en kollektiv tilnærming på unionsplan. Samtidig gjennomføring av flere revisjoner og tilgangsrettigheter som utføres separat av mange vedkommende myndigheter med liten eller ingen innbyrdes koordinering, vil forhindre finansielle tilsynsmyndigheter i å få en fullstendig og omfattende oversikt over IKT-tredjepartsrisiko i Unionen, samtidig som det innebærer redundans, byrde og kompleksitet for kritiske tredjepartsleverandører av IKT-tjenester, dersom de er gjenstand for mange anmodninger om overvåking og inspeksjon.

89) Ettersom utpekingen som kritisk har en betydelig innvirkning, bør denne forordningen sikre at rettighetene til kritiske tredjepartsleverandører av IKT-tjenester overholdes gjennom hele gjennomføringen av overvåkingsrammeverket. Før slike leverandører utpekes som kritiske, bør de for eksempel ha rett til å sende en begrunnet uttalelse til hovedovervåkeren som inneholder alle opplysninger som er relevante for den vurderingen som gjelder utpekingen. Ettersom hovedovervåkeren bør ha myndighet til å legge fram anbefalinger om spørsmål som gjelder IKT-risiko og egnede tiltak for håndtering av disse, som omfatter myndigheten til å motsette seg visse kontraktsregulerte ordninger som i siste instans påvirker stabiliteten til den finansielle enheten eller finanssystemet, bør kritiske tredjepartsleverandører av IKT-tjenester

også gis mulighet til, før disse anbefalingene ferdigstilles, å gi forklaringer på hvilken innvirkning de foreslåtte løsningene i anbefalingene forventes å ha på kunder som er enheter som faller utenfor virkeområdet for denne forordningen, og til å utarbeide løsninger for å begrense risikoene. Kritiske tredjepartsleverandører av IKT-tjenester som er uenige med anbefalingene, bør sende inn en begrunnet redegjørelse for sin hensikt om ikke å slutte seg til anbefalingen. Dersom en slik begrunnet redegjørelse ikke sendes inn, eller dersom den anses å være utilstrekkelig, bør hovedovervåkeren sende ut en kunngjøring som kort beskriver problemet med manglende overholdelse.

90) De vedkommende myndighetene bør på behørig vis la oppgaven med å kontrollere at anbefalinger fra hovedovervåkeren faktisk overholdes, inngå i deres oppdrag med hensyn til tilsyn med finansielle enheter. De vedkommende myndighetene bør kunne kreve at finansielle enheter treffer ytterligere tiltak for å styre de risikoene som er identifisert i hovedovervåkerens anbefalinger, og bør i god tid utstede meldinger om dette. Dersom hovedovervåkeren retter anbefalinger til kritiske tredjepartsleverandører av IKT-tjenester som er underlagt tilsyn i henhold til direktiv (EU) 2022/2555, bør de vedkommende myndighetene, på frivillig grunnlag og før de vedtar ytterligere tiltak, kunne høre de vedkommende myndighetene i henhold til det nevnte direktivet for å fremme en koordinert strategi for håndtering av de aktuelle kritiske tredjepartsleverandørene av IKT-tjenester.

91) Utøvelsen av overvåkingen bør styres av tre operasjonelle prinsipper som har til formål å sikre a) tett koordinering mellom de europeiske tilsynsmyndighetene i deres roller som hovedovervåker gjennom et felles overvåkingsnettverk, b) samsvar med det rammeverket som er fastsatt i henhold til direktiv (EU) 2022/2555 (gjennom en frivillig høring av organer i henhold til det nevnte direktivet for å unngå overlapping av tiltak rettet mot kritiske tredjepartsleverandører av IKT-tjenester), og c) aktsomhet for å minimere den potensielle risikoen for forstyrrelser i tjenester levert av kritiske tredjepartsleverandører av IKT-tjenester til kunder som er enheter som faller utenfor virkeområdet for denne forordningen.

92) Overvåkingsrammeverket bør ikke erstatte eller på noen måte eller i noen del anvendes i stedet for kravet om at finansielle enheter selv skal styre de risikoene som følger av anvendelsen av tredjepartsleverandører av IKT-tjenester, herunder deres forpliktelse til å opprettholde en løpende overvåking av kontraktsregulerte ordninger som er inngått med kritiske tredjepartsleverandører av IKT-tjenester. Overvåkingsrammeverket bør heller ikke berøre de finansielle enhetenes fulle ansvar for å overholde og oppfylle alle rettslige forpliktelser fastsatt i denne forordningen og i det relevante regelverket for finansielle tjenester.

93) For å unngå dobbeltbestemmelser og overlappinger bør vedkommende myndigheter avstå fra å treffe individuelle tiltak som tar sikte på å overvåke risiko hos den kritiske tredjepartsleverandøren av IKT-tjenester, og bør i den forbindelse stole på den relevante hovedovervåkerens vurdering. Alle tiltak bør under alle omstendigheter koordineres og avtales på forhånd med hovedovervåkeren som ledd i utførelsen av oppgaver innenfor overvåkingsrammeverket.

94) For å fremme tilnærming på internasjonalt plan når det gjelder anvendelse av beste praksis for gjennomgåelse og overvåking av den digitale risikostyringen som foretas av tredjepartsleverandører av IKT-tjenester, bør de europeiske tilsynsmyndighetene oppfordres til å inngå samarbeidsordninger med relevante tilsyns- og reguleringsmyndigheter i tredjeland.

95) For å utnytte den spesifikke kompetansen, de tekniske ferdighetene og ekspertisen til personale som spesialiserer seg på operasjonell risiko og IKT-risiko hos de vedkommende myndighetene, de tre europeiske tilsynsmyndighetene og, på frivillig grunnlag, de vedkommende myndighetene i henhold til direktiv (EU) 2022/2555, bør hovedovervåkeren benytte seg av nasjonal tilsynskapasitet og -kunnskap og opprette særskilte granskningsgrupper for hver kritisk tredjepartsleverandør av IKT-tjenester, for å samle tverrfaglige grupper til støtte for utarbeiding og gjennomføring av overvåkingsvirksomhet, herunder generelle undersøkelser og inspeksjoner av kritiske tredjepartsleverandører av IKT-tjenester, samt for eventuell nødvendig oppfølging av dem.

96) Mens kostnader som oppstår som følge av overvåkingsoppgaver vil bli fullt ut finansiert av avgifter pålagt kritiske tredjepartsleverandører av IKT-tjenester, er det imidlertid sannsynlig at de europeiske tilsynsmyndighetene vil pådra seg, før overvåkingsrammeverket får anvendelse, kostnader for gjennomføring av særskilte IKT-systemer som støtter den kommende overvåkingen, ettersom særskilte IKT-systemer må utvikles og innføres på forhånd. Denne forordningen inneholder bestemmelser om en hybrid finansieringsmodell, der overvåkingsrammeverket som sådan vil være fullt ut finansiert gjennom avgifter, mens utviklingen av de europeiske tilsynsmyndighetenes IKT-systemer vil bli finansiert gjennom bidrag fra Unionen og de nasjonale vedkommende myndighetene.

97) De vedkommende myndighetene bør ha all nødvendig tilsyns-, undersøkelses- og sanksjonsmyndighet for å sikre at de utøver sine oppgaver i henhold til denne forordningen. De bør i prinsippet offentliggjøre kunngjøringer om de administrative sanksjonene de pålegger. Ettersom finansielle enheter og tredjepartsleverandører av IKT-tjenester kan etableres i ulike medlemsstater og overvåkes av ulike vedkommende myndigheter, bør anvendelsen av denne forordningen lettes ved på den ene side et nært samarbeid mellom berørte vedkommende myndigheter, herunder Den europeiske sentralbank, med hensyn til særlige oppgaver som den er tildelt i henhold til rådsforordning (EU) nr. 1024/2013, og ved på den annen side høring av de europeiske tilsynsmyndighetene gjennom gjensidig utveksling av opplysninger og levering av bistand i forbindelse med den relevante tilsynsvirksomheten.

98) For ytterligere å kvantifisere og kvalifisere kriteriene for utpeking av tredjepartsleverandører av IKT-tjenester som kritiske og for å harmonisere overvåkingsavgiftene bør myndigheten til å vedta rettsakter i samsvar med artikkel 290 i TEUV delegeres til Kommisjonen for å utfylle denne forordningen med nærmere spesifisering av den systemiske virkningen som en svikt eller en driftsstans hos en tredjepartsleverandør av IKT-tjenester skulle kunne få på de finansielle enhetene som den leverer IKT-tjenester til, antall globale systemviktige institusjoner eller andre systemviktige institusjoner som er avhengige av den aktuelle tredjepartsleverandøren av IKT-tjenester, antall tredjepartsleverandører av IKT-tjenester som er aktive på et gitt marked, kostnadene ved å overføre data og IKT-arbeidsbelastningen til andre tredjepartsleverandører av IKT-tjenester, samt størrelsen på avgiftsbeløpene og hvordan de skal betales. Det er særlig viktig at Kommisjonen gjennomfører hensiktsmessige høringer under sitt forberedende arbeid, herunder på ekspertnivå, og at disse høringene gjennomføres i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming([22]). For å sikre lik deltakelse ved utarbeidingen av delegerte rettsakter er det særlig viktig at Europaparlamentet og Rådet mottar alle dokumenter samtidig som medlemsstatenes eksperter, og deres eksperter bør ha systematisk adgang til møter i Kommisjonens ekspertgrupper som er med på utarbeidingen av delegerte rettsakter.

99) Tekniske reguleringsstandarder bør sikre en ensartet harmonisering av kravene fastsatt i denne forordningen. De europeiske tilsynsmyndighetene bør i egenskap av organ med høyt spesialisert sakkunnskap derfor få i oppdrag å utarbeide utkast til tekniske reguleringsstandarder som ikke innebærer politiske valg, med sikte på framlegging for Kommisjonen. Det bør utvikles tekniske reguleringsstandarder på områdene IKT-risikostyring, rapportering av alvorlige IKT-relaterte hendelser, testing, samt i forbindelse med sentrale krav til en forsvarlig overvåking av IKT-tredjepartsrisiko. Kommisjonen og de europeiske tilsynsmyndighetene bør sikre at disse standardene og kravene kan anvendes av alle finansielle enheter på en måte som står i forhold til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift. Kommisjonen bør gis myndighet til å vedta slike tekniske reguleringsstandarder ved hjelp av delegerte rettsakter i henhold til artikkel 290 i TEUV og i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

100) For å gjøre det lettere å sammenligne rapporter om alvorlige IKT-relaterte hendelser og alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, samt for å sikre åpenhet om kontraktsregulerte ordninger for bruk av IKT-tjenester som leveres av tredjepartsleverandører av IKT-tjenester, bør de europeiske tilsynsmyndighetene utarbeide utkast til tekniske gjennomføringsstandarder som fastsetter standardiserte maler, skjemaer og framgangsmåter, slik at finansielle enheter kan rapportere en alvorlig IKT-relatert hendelse og en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshetshendelse, samt standardiserte maler for registrering av opplysninger. Når de europeiske tilsynsmyndighetene utarbeider disse standardene, bør de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift. Kommisjonen bør gis myndighet til å vedta slike tekniske gjennomføringsstandarder ved hjelp av en gjennomføringsrettsakt i henhold til artikkel 291 i TEUV og i samsvar med artikkel 15 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

([22]) EUT L 123 av 12.5.2016, s. 1.

101) Ettersom det allerede er fastsatt ytterligere krav gjennom delegerte rettsakter og gjennomføringsrettsakter basert på tekniske reguleringsstandarder og tekniske gjennomføringsstandarder i europaparlaments- og rådsforordning (EF) nr. 1060/2009([23]), (EU) nr. 648/2012([24]), (EU) nr. 600/2014([25]) og (EU) nr. 909/2014([26]), er det hensiktsmessig å gi de europeiske tilsynsmyndighetene mandat til, enten individuelt eller i fellesskap gjennom Felleskomiteen, å legge fram tekniske reguleringsstandarder og tekniske gjennomføringsstandarder for Kommisjonen for vedtakelse av delegerte rettsakter og gjennomføringsrettsakter om overføring og oppdatering av eksisterende regler om IKT-risikostyring.

102) Ettersom denne forordningen, sammen med europaparlaments- og rådsdirektiv (EU) 2022/2556([27]), innebærer en konsolidering av bestemmelser om IKT-risikostyring i flere forordninger og direktiver i Unionens regelverk for finansielle tjenester, herunder forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014, og europaparlaments- og rådsforordning (EU) 2016/1011([28]), bør disse forordningene endres for å sikre fullt samsvar og tydeliggjøre at gjeldende IKT-risikorelaterte bestemmelser er fastsatt i denne forordningen.

103) Derfor bør virkeområdet for de relevante artiklene knyttet til operasjonell risiko, for hvilke delegerte rettsakter og gjennomføringsrettsakter skal vedtas i henhold til den myndigheten som er fastsatt i forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011, begrenses slik at alle bestemmelser som omfatter aspekter av digital operasjonell motstandsdyktighet, og som i dag inngår i disse forordningene, overføres til denne forordningen.

104) Den potensielle systemrisikoen på cyberområdet knyttet til bruken av IKT-infrastrukturer som muliggjør drift av betalingssystemer og levering av betalingsbehandlingstjenester, bør håndteres på behørig vis på unionsplan gjennom harmoniserte regler om digital motstandsdyktighet. Kommisjonen bør derfor raskt vurdere behovet for å gjennomgå virkeområdet for denne forordningen, samtidig som en slik gjennomgåelse tilpasses til resultatet av den omfattende gjennomgåelsen som er planlagt i henhold til direktiv (EU) 2015/2366. Mange storstilte angrep i løpet av det siste tiåret viser hvordan betalingssystemer er blitt utsatt for cybertrusler. Med en sentral plassering i betalingstjenestekjeden og sterke innbyrdes forbindelser til finanssystemet som en helhet har betalingssystemer og betalingsbehandlingstjenester fått en avgjørende betydning for finansmarkedenes virkemåte i Unionen. Cyberangrep på slike systemer kan forårsake alvorlige driftsforstyrrelser med direkte konsekvenser for viktige økonomiske funksjoner, som for eksempel tilrettelegging av betalinger og indirekte virkninger på relaterte økonomiske prosesser. Inntil det er innført en harmonisert ordning og tilsyn med operatører av betalingssystemer og behandlingsenheter på unionsplan, kan medlemsstatene, med sikte på å anvende en lignende markedspraksis, la seg inspirere av de kravene til digital operasjonell motstandsdyktighet som er fastsatt i denne forordningen, når de anvender regler på operatører av betalingssystemer og behandlingsenheter som er underlagt tilsyn i deres egne jurisdiksjoner.

([23]) Europaparlaments- og rådsforordning (EF) nr. 1060/2009 av 16. september 2009 om kredittvurderingsbyråer (EUT L 302 av 17.11.2009, s. 1).

([24]) Europaparlaments- og rådsforordning (EU) nr. 648/2012 av 4. juli 2012 om OTC-derivater, sentrale motparter og transaksjonsregistre (EUT L 201 av 27.7.2012, s. 1).

([25]) Europaparlaments- og rådsforordning (EU) nr. 600/2014 av 15. mai 2014 om markeder for finansielle instrumenter og om endring av forordning (EU) nr. 648/2012 (EUT L 173 av 12.6.2014, s. 84).

([26]) Europaparlaments- og rådsforordning (EU) nr. 909/2014 av 23. juli 2014 om forbedring av verdipapiroppgjør i Den europeiske union og om verdipapirsentraler samt om endring av direktiv 98/26/EF og 2014/65/EU og forordning (EU) nr. 236/2012 (EUT L 257 av 28.8.2014, s. 1).

([27]) Europaparlaments- og rådsdirektiv (EU) 2022/256 av 14. desember 2022 om endring av 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 med hensyn til digital operasjonell motstandsdyktighet i finanssektoren (se EUT L 333 av 27.12.2022, s. 153).

([28]) Europaparlaments- og rådsforordning (EU) 2016/1011 av 8. juni 2016 om indekser som brukes som referanseverdier for finansielle instrumenter og finansielle kontrakter eller for å måle investeringsfonds resultater, og om endring av direktiv 2008/48/EF og 2014/17/EU og forordning (EU) nr. 596/2014 (EUT L 171 av 29.6.2016, s. 1).

105) Ettersom målet for denne forordningen, som er å oppnå et høyt nivå av digital operasjonell motstandsdyktighet for regulerte finansielle enheter, ikke kan nås i tilstrekkelig grad av medlemsstatene ettersom det krever harmonisering av flere ulike regler i unionsretten og nasjonal rett, og derfor på grunn av tiltakets omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i den nevnte artikkelen går denne forordningen ikke lenger enn det som er nødvendig for å nå dette målet.

106) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 42 nr. 1 i europaparlaments- og rådsforordning (EU) 2018/1725([29]) og avga uttalelse 10. mai 2021([30]).

VEDTATT DENNE FORORDNINGEN:

KAPITTEL I

Alminnelige bestemmelser

Artikkel 1

Formål

1. For å oppnå et høyt felles nivå av digital operasjonell motstandsdyktighet fastsetter denne forordningen ensartede krav til sikkerheten i nettverks- og informasjonssystemer som støtter finansielle enheters forretningsprosesser på følgende måte:

a) Krav som får anvendelse på finansielle enheter i forbindelse med

   i) risikostyring i forbindelse med informasjons- og kommunikasjonsteknologi (IKT),

   ii) rapportering av alvorlige IKT-relaterte hendelser og underretning på frivillig grunnlag om betydelige cybertrusler til de vedkommende myndighetene,

   iii) rapportering av alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser til de vedkommende myndighetene fra finansielle enheter som nevnt i artikkel 2 nr. 1 bokstav a)–d),

   iv) testing av digital operasjonell motstandsdyktighet,

   v) utveksling av opplysninger og etterretninger i forbindelse med cybertrusler og sårbarheter,

   vi) tiltak for forsvarlig styring av IKT-tredjepartsrisiko.

b) Krav i forbindelse med kontraktsregulerte ordninger inngått mellom tredjepartsleverandører av IKT-tjenester og finansielle enheter.

c) Regler om opprettelse og gjennomføring av overvåkingsrammeverket for kritiske tredjepartsleverandører av IKT-tjenester når de leverer tjenester til finansielle enheter.

d) Krav om samarbeid mellom vedkommende myndigheter og regler om vedkommende myndigheters tilsyn og håndheving i forbindelse med alle forhold som er omfattet av denne forordningen.

2. Når det gjelder finansielle enheter som er identifisert som vesentlige eller viktige enheter i henhold til nasjonale regler som innarbeider artikkel 3 i direktiv (EU) 2022/2555, skal denne forordningen anses som en sektorspesifikk unionsrettsakt med hensyn til artikkel 4 i det nevnte direktivet.

3. Denne forordningen berører ikke medlemsstatenes ansvar for vesentlige statlige funksjoner som gjelder offentlig sikkerhet, forsvar og nasjonal sikkerhet i samsvar med unionsretten.

([29]) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

([30]) EUT C 229 av 15.6.2021, s. 16.

Artikkel 2

Virkeområde

1. Med forbehold for nr. 3 og 4 får denne forordningen anvendelse på følgende enheter:

a) Kredittinstitusjoner

b) Betalingsinstitusjoner, herunder betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366.

c) Ytere av kontoopplysningstjenester.

d) E-pengeforetak, herunder e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF.

e) Verdipapirforetak.

f) Tilbydere av kryptoeiendeler som er meddelt tillatelse i henhold til europaparlaments- og rådsforordning om markeder for kryptoeiendeler, og om endring av forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937 («forordningen om markeder for kryptoeiendeler») og utstedere av kryptoeiendeler,

g) Verdipapirsentraler.

h) Sentrale motparter.

i) Handelsplasser.

j) Transaksjonsregistre.

k) Forvaltere av alternative investeringsfond.

l) Forvaltningsselskaper.

m) Leverandører av datarapporteringstjenester.

n) Forsikrings- og gjenforsikringsforetak.

o) Forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet.

p) Tjenestepensjonsforetak.

q) Kredittvurderingsbyråer.

r) Administratorer av kritiske referanseverdier.

s) Tilbydere av folkefinansieringstjenester.

t) Verdipapiriseringsregistre.

u) tredjepartsleverandører av IKT-tjenester.

2. I denne forordningen skal enheter nevnt i nr. 1 bokstav a)–t) samlet kalles «finansielle enheter».

3. Denne forordningen får ikke anvendelse på

a) forvaltere av alternative investeringsfond som nevnt i artikkel 3 nr. 2 i direktiv 2011/61/EF,

b) forsikrings- og gjenforsikringsforetak som nevnt i artikkel 4 i direktiv 2009/138/EF,

c) tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen ikke har mer enn 15 medlemmer i alt,

d) fysiske eller juridiske personer som er unntatt i henhold til artikkel 2 og 3 i direktiv 2014/65/EU,

e) forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, som er svært små, små eller mellomstore bedrifter,

f) postgirokontorer som nevnt i artikkel 2 nr. 5 punkt 3) i direktiv 2013/36/EU.

4. Medlemsstatene kan unnta enheter nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU som befinner seg på deres respektive territorier, fra denne forordningens virkeområde. Dersom en medlemsstat gjør bruk av denne muligheten, skal den underrette Kommisjonen om dette og om eventuelle senere endringer. Kommisjonen skal offentliggjøre opplysningene på sitt nettsted eller på en annen lett tilgjengelig måte.

Artikkel 3

Definisjoner

I denne forordningen menes med

1) «digital operasjonell motstandsdyktighet» en finansiell enhets evne til å bygge opp, sikre og gjennomgå sin operasjonelle integritet og pålitelighet gjennom å sikre, enten direkte eller indirekte gjennom bruk av tjenester levert av tredjepartsleverandører av IKT-tjenester, hele spekteret av IKT-relatert kapasitet som er nødvendig for å håndtere sikkerheten i de nettverks- og informasjonssystemene som en finansiell enhet bruker, og som støtter fortløpende levering av finansielle tjenester og deres kvalitet, herunder i forbindelse med forstyrrelser,

2) «nettverks- og informasjonssystem» et nettverks- og informasjonssystem som definert i artikkel 6 punkt 1) i direktiv (EU) 2022/2555,

3) «eldre IKT-system» et IKT-system som har nådd slutten av sin livssyklus (end-of-life), og som av teknologiske eller kommersielle årsaker ikke er egnet til oppgraderinger eller utbedringer, eller som ikke lenger støttes av sin tredjepartsleverandør av IKT-tjenester, men som fortsatt er i bruk og støtter den finansielle enhetens funksjoner,

4) «sikkerhet i nettverks- og informasjonssystemer» sikkerhet i nettverks- og informasjonssystemer som definert i artikkel 6 punkt 2) i direktiv (EU) 2022/2555,

5) «IKT-risiko» enhver omstendighet som med rimelighet kan identifiseres i forbindelse med bruk av nettverks- og informasjonssystemer som, dersom den oppstår, kan svekke sikkerheten i nettverks- og informasjonssystemer, i verktøyer eller prosesser som er teknologiavhengige, i funksjoner og prosesser eller i forbindelse med levering av tjenester gjennom å skape negative virkninger i det digitale eller fysiske miljøet,

6) «informasjonsressurs» en samling av opplysninger, både materielle og immaterielle, som det er verdt å beskytte,

7) «IKT-ressurs» en programvare- eller maskinvareressurs i nettverks- og informasjonssystemene som brukes av den finansielle enheten,

8) «IKT-relatert hendelse» én enkelt hendelse eller en rekke tilknyttede hendelser som ikke er planlagt av den finansielle enheten, og som går ut over sikkerheten i nettverks- og informasjonssystemene, og har en negativ innvirkning på tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene eller på de tjenestene som leveres av den finansielle enheten,

9) «betalingsrelatert operasjonell hendelse eller sikkerhetshendelse» én enkelt hendelse eller en rekke tilknyttede hendelser som ikke er planlagt av de finansielle enhetene nevnt i artikkel 2 nr. 1 bokstav a)–d), uansett om de er IKT-relaterte eller ikke, og som har en negativ innvirkning på tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til betalingsrelaterte opplysninger, eller på de betalingsrelaterte tjenestene som leveres av den finansielle enheten,

10) «alvorlig IKT-relatert hendelse» en IKT-relatert hendelse som har en stor negativ innvirkning på nettverks- og informasjonssystemene som støtter den finansielle enhetens kritiske eller viktige funksjoner,

11) «alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse» en betalingsrelatert operasjonell hendelse eller sikkerhetshendelse som har stor negativ innvirkning på de betalingsrelaterte tjenestene som leveres,

12) «cybertrussel» cybertrussel som definert i artikkel 2 punkt 8) i forordning (EU) 2019/881,

13) «betydelig cybertrussel» en cybertrussel hvis tekniske egenskaper tilsier at den kan føre til en alvorlig IKT-relatert hendelse eller en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse,

14) «cyberangrep» en ondsinnet IKT-relatert hendelse forårsaket av en trusselaktørs forsøk på å ødelegge, eksponere, endre, deaktivere, stjele eller få uautorisert tilgang til eller uautorisert bruk av en eiendel,

15) «trusseletterretning» opplysninger som er aggregert, omdannet, analysert, tolket eller beriket for å skape den sammenhengen som kreves for beslutningstaking, og for å muliggjøre relevant og tilstrekkelig forståelse med henblikk på å redusere virkningene av en IKT-relatert hendelse eller en cybertrussel, herunder de tekniske detaljene om et cyberangrep, de ansvarlige for angrepet og deres framgangsmåte og motiv,

16) «sårbarhet» en svakhet, mottakelighet eller feil i en eiendel, et system, en prosess eller en kontroll som kan utnyttes,

17) «trusselbasert penetrasjonstesting (TLPT)» et rammeverk som etterligner de taktikkene, teknikkene og framgangsmåtene som brukes av virkelige trusselaktører og oppfattes som en ekte cybertrussel, og som gir en kontrollert, skreddersydd og etterretningsbasert («red team») test av de kritiske produksjonssystemene som er i drift hos den finansielle enheten,

18) «IKT-tredjepartsrisiko» en IKT-risiko som kan oppstå for en finansiell enhet i forbindelse med dens bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester eller av underleverandører til slike leverandører, herunder gjennom ordninger for utkontraktering,

19) «tredjepartsleverandør av IKT-tjenester» et foretak som leverer IKT-tjenester,

20) «konsernintern leverandør av IKT-tjenester» et foretak som er en del av et finanskonsern, og som hovedsakelig leverer IKT-tjenester til finansielle enheter innenfor samme konsern eller til finansielle enheter som tilhører samme institusjonelle beskyttelsesordning, herunder til deres morforetak, datterforetak, filialer eller andre enheter som er under felles eierskap eller kontroll,

21) «IKT-tjenester» digitale tjenester og datatjenester som fortløpende leveres gjennom IKT-systemer til en eller flere interne eller eksterne brukere, herunder maskinvare som en tjeneste og maskinvaretjenester som omfatter maskinvareleverandørens levering av teknisk støtte via oppdateringer av programvare eller fastvare, med unntak av tradisjonelle analoge telefonitjenester,

22) «kritisk eller viktig funksjon» en funksjon hvis forstyrrelser i vesentlig grad vil forringe en finansiell enhets finansielle inntjening, eller soliditeten eller kontinuiteten i dens tjenester og aktiviteter, eller som, dersom den aktuelle funksjonen avbrytes, er mangelfull eller mislykkes, i vesentlig grad kan forringe en finansiell enhets oppfyllelse av de vilkårene og forpliktelsene som er forbundet med dens tillatelse, eller av dens øvrige forpliktelser i henhold til gjeldende regelverk for finansielle tjenester,

23) «kritisk tredjepartsleverandør av IKT-tjenester» en tredjepartsleverandør av IKT-tjenester som er klassifisert som kritisk i samsvar med artikkel 31,

24) «tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland» en tredjepartsleverandør av IKT-tjenester som er en juridisk person som er etablert i et tredjeland, og som har inngått en kontraktsregulert ordning med en finansiell enhet om levering av IKT-tjenester,

25) «datterforetak» et datterforetak i henhold til artikkel 2 punkt 10) og artikkel 22 i direktiv 2013/34/EU,

26) «konsern» et konsern som definert i artikkel 2 punkt 11) i direktiv 2013/34/EU,

27) «morforetak» et morforetak i henhold til artikkel 2 punkt 9) og artikkel 22 i direktiv 2013/34/EU,

28) «IKT-underleverandør som er etablert i et tredjeland» en IKT-underleverandør som er en juridisk person som er etablert i et tredjeland, og som har inngått en kontraktsregulert ordning enten med en tredjepartsleverandør av IKT-tjenester eller med en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland,

29) «IKT-konsentrasjonsrisiko» en eksponering mot enkelte eller flere tilknyttede kritiske tredjepartsleverandører av IKT-tjenester som skaper en grad av avhengighet av slike leverandører, slik at manglende tilgjengelighet, feil eller annen type svikt hos en slik leverandør kan sette en finansiell enhets evne til å levere kritiske eller viktige funksjoner i fare, eller føre til at den rammes av andre former for negative virkninger, herunder store tap, eller sette den finansielle stabiliteten i Unionen som helhet i fare,

30) «ledelsesorgan» et ledelsesorgan som definert i artikkel 4 nr. 1 punkt 36) i direktiv 2014/65/EU, artikkel 3 nr. 1 punkt 7) i direktiv 2013/36/EU, artikkel 2 nr. 1 bokstav s) i europaparlaments- og rådsdirektiv 2009/65/EF([31]), artikkel 2 nr. 1 punkt 45) i forordning (EU) nr. 909/2014, artikkel 3 nr. 1 punkt 20) i forordning (EU) 2016/1011 og i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler, eller tilsvarende personer som i praksis leder enheten eller har nøkkelfunksjoner i samsvar med relevant unionsrett eller nasjonal rett,

31) «kredittinstitusjon» en kredittinstitusjon som definert i artikkel 4 nr. 1 punkt 1) i europaparlaments- og rådsforordning (EU) nr. 575/2013([32]),

32) «institusjon unntatt i henhold til direktiv 2013/36/EU» en enhet som nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU,

33) «verdipapirforetak» et verdipapirforetak som definert i artikkel 4 nr. 1 punkt 1) i direktiv 2014/65/EU,

34) «lite verdipapirforetak uten innbyrdes forbindelser» et verdipapirforetak som oppfyller vilkårene i artikkel 12 nr. 1 i europaparlaments- og rådsforordning (EU) 2019/2033([33]),

35) «betalingsinstitusjon» en betalingsinstitusjon som definert i artikkel 4 nr. 4 i direktiv (EU) 2015/2366,

36) «betalingsinstitusjon som er unntatt i henhold til direktiv (EU) 2015/2366» en betalingsinstitusjon som er unntatt i henhold til artikkel 32 nr. 1 i direktiv (EU) 2015/2366,

37) «yter av kontoopplysningstjenester» en yter av kontoopplysningstjenester som nevnt i artikkel 33 nr. 1 i direktiv (EU) 2015/2366,

38) «e-pengeforetak» et e-pengeforetak som definert i artikkel 2 punkt 1) i europaparlaments- og rådsdirektiv 2009/110/EF,

39) «e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF» et e-pengeforetak som er omfattet av et unntak som omhandlet i artikkel 9 nr. 1 i direktiv 2009/110/EF,

40) «sentral motpart» en sentral motpart som definert i artikkel 2 punkt 1) i forordning (EU) nr. 648/2012,

41) «transaksjonsregister» et transaksjonsregister som definert i artikkel 2 punkt 2) i forordning (EU) nr. 648/2012,

42) «verdipapirsentral» en verdipapirsentral som definert i artikkel 2 nr. 1 punkt 1) i forordning (EU) nr. 909/2014,

43) «handelsplass» en handelsplass som definert i artikkel 4 nr. 1 punkt 24) i direktiv 2014/65/EU,

44) «forvalter av alternative investeringsfond» en forvalter av alternative investeringsfond som definert i artikkel 4 nr. 1 bokstav b) i direktiv 2011/61/EU,

45) «forvaltningsselskap» et forvaltningsselskap som definert i artikkel 2 nr. 1 bokstav b) i direktiv 2009/65/EF,

46) «leverandør av datarapporteringstjenester» en leverandør av datarapporteringstjenester i henhold til forordning (EU) nr. 600/2014, som nevnt i artikkel 2 nr. 1 punkt 34)–36) i samme forordning,

47) «forsikringsforetak» et forsikringsforetak som definert i artikkel 13 punkt 1) i direktiv 2009/138/EF,

48) «gjenforsikringsforetak» et gjenforsikringsforetak som definert i artikkel 13 punkt 4) i direktiv 2009/138/EF,

([31]) Europaparlaments- og rådsdirektiv 2009/65/EF av 13. juli 2009 om samordning av lover og forskrifter om foretak for kollektiv investering i omsettelige verdipapirer (UCITS) (EUT L 302 av 17.11.2009, s. 32).

([32]) Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og om endring av forordning (EU) nr. 648/2012 (EUT L 176 av 27.6.2013, s. 1).

([33]) Europaparlaments- og rådsforordning (EU) 2019/2033 av 27. november 2019 om tilsynskrav for verdipapirforetak og om endring av forordning (EU) nr. 1093/2010, (EU) nr. 575/2013, (EU) nr. 600/2014 og (EU) nr. 806/2014 (EUT L 314 av 5.12.2019, s. 1).

49) «forsikringsformidler» en forsikringsformidler som definert i artikkel 2 nr. 1 punkt 3) i europaparlaments- og rådsforordning (EU) 2016/97([34]),

50) «forsikringsformidler som har forsikringsformidling som tilleggsvirksomhet» en forsikringsformidler som har forsikringsformidling som tilleggsvirksomhet, som definert i artikkel 2 nr. 1 punkt 4) i direktiv (EU) 2016/97,

51) «gjenforsikringsformidler» en gjenforsikringsformidler som definert i artikkel 2 nr. 1 punkt 5) i direktiv (EU) 2016/97,

52) «tjenestepensjonsforetak» et tjenestepensjonsforetak som definert i artikkel 6 punkt 1) i direktiv (EU) 2016/2341,

53) «lite tjenestepensjonsforetak» et tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen har mindre enn 100 medlemmer,

54) «kredittvurderingsbyrå» et kredittvurderingsbyrå som definert i artikkel 3 nr. 1 bokstav b) i forordning (EF) nr. 1060/2009,

55) «tilbyder av kryptoeiendelstjenester» en tilbyder av kryptoeiendelstjenester som definert i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler,

56) «utsteder av kryptoeiendeler» en utsteder av kryptoeiendeler som definert i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler,

57) «administrator av kritiske referanseverdier» en administrator av kritiske referanseverdier som definert i artikkel 3 nr. 1 punkt 25) i forordning (EU) 2016/1011,

58) «tilbyder av folkefinansieringstjenester» en tilbyder av folkefinansieringstjenester som definert i artikkel 2 nr. 1 bokstav e) i europaparlaments- og rådsforordning (EU) 2020/1503([35]),

59) «verdipapiriseringsregister» et verdipapiriseringsregister som definert i artikkel 2 punkt 23) i europaparlaments- og rådsforordning (EU) 2017/2402([36]),

60) «svært liten bedrift» en finansiell enhet, som ikke er en handelsplass, en sentral motpart, et transaksjonsregister eller en verdipapirsentral, og som sysselsetter færre enn ti personer og har en årsomsetning og/eller en samlet årsbalanse som ikke overstiger 2 millioner euro,

61) «hovedovervåker» den europeiske tilsynsmyndigheten som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b) i denne forordningen,

62) «felleskomité» den komiteen som er nevnt i artikkel 54 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010,

63) «liten bedrift» en finansiell enhet som sysselsetter ti eller flere personer, men færre enn 50 personer, og som har en årsomsetning og/eller en samlet årsbalanse som overstiger 2 millioner euro, men som ikke overstiger 10 millioner euro,

64) «mellomstor bedrift» en finansiell enhet som ikke er en liten bedrift, og som sysselsetter færre enn 250 personer og har en årsomsetning som ikke overstiger 50 millioner euro og/eller en årsbalanse som ikke overstiger 43 millioner euro,

65) «offentlig myndighet» enhver offentlig myndighet eller andre enheter innen offentlig forvaltning, herunder nasjonale sentralbanker.

([34]) Europaparlaments- og rådsdirektiv (EU) 2016/97 av 20. januar 2016 om forsikringsdistribusjon (EUT L 26 av 2.2.2016, s. 19).

([35]) Europaparlaments- og rådsforordning (EU) 2020/1503 av 7. oktober 2020 om europeiske tilbydere av folkefinansieringstjenester til næringsvirksomhet og om endring av forordning (EU) 2017/1129 og direktiv (EU) 2019/1937 (EUT L 347 av 20.10.2020, s. 1).

([36]) Europaparlaments- og rådsforordning (EU) 2017/2402 av 12. desember 2017 om fastsettelse av en generell ramme for verdipapirisering og en særskilt ramme for enkel, gjennomsiktig og standardisert verdipapirisering, og om endring av 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 av 28.12.2017, s. 35).

Artikkel 4

Forholdsmessighetsprinsippet

1. Finansielle enheter skal gjennomføre reglene fastsatt i kapittel II i samsvar med forholdsmessighetsprinsippet, samtidig som det tas hensyn til deres størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift.

2. I tillegg skal finansielle enheters anvendelse av kapittel III, IV og V avsnitt I, stå i et rimelig forhold til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift, slik det er spesifisert i de relevante reglene i disse kapitlene.

3. De vedkommende myndighetene skal vurdere finansielle enheters anvendelse av forholdsmessighetsprinsippet når de gjennomgår sammenhengen i rammeverket for IKT-risikostyring på grunnlag av de rapportene som framlegges på anmodning fra vedkommende myndigheter i henhold til artikkel 6 nr. 5 og artikkel 16 nr. 2.

KAPITTEL II

IKT-RISIKOSTYRING

Avsnitt I

Artikkel 5

Styring og organisering

1. Finansielle enheter skal ha innført et intern rammeverk for styring og kontroll som sikrer en effektiv og forsvarlig styring av IKT-risiko, i samsvar med artikkel 6 nr. 4, for å oppnå et høyt nivå av digital operasjonell motstandsdyktighet.

2. Ledelsesorganet i den finansielle enheten skal definere, godkjenne, føre tilsyn med og ha ansvar for gjennomføringen av alle ordninger knyttet til rammeverket for IKT-risikostyring nevnt i artikkel 6 nr. 1.

Ved anvendelse av første ledd skal organet

a) ha det endelige ansvaret for å styre den finansielle enhetens IKT-risiko,

b) innføre retningslinjer som tar sikte på å sikre opprettholdelse av høye standarder for tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene,

c) fastsette klare roller og ansvarsområder for alle IKT-relaterte funksjoner og etablere hensiktsmessige styringsordninger for å sikre effektiv og rettidig kommunikasjon, samarbeid og koordinering mellom disse funksjonene,

d) ha det endelige ansvaret for å fastsette og godkjenne strategien for digital operasjonell motstandsdyktighet som nevnt i artikkel 6 nr. 8, herunder fastsette et passende risikotoleransenivå for den finansielle enhetens IKT-risiko, som nevnt i artikkel 6 nr. 8 bokstav b),

e) godkjenne, føre tilsyn med og regelmessig gjennomgå gjennomføringen av den finansielle enhetens retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting som nevnt i henholdsvis artikkel 11 nr. 1 og 3, som kan vedtas som egne spesifikke retningslinjer som utgjør en integrert del av den finansielle enhetens overordnede retningslinjer for kontinuitet i virksomheten og respons- og gjenopprettingsplan,

f) godkjenne og regelmessig gjennomgå den finansielle enhetens interne IKT-revisjonsplaner, IKT-revisjoner og vesentlige endringer i dem,

g) tildele og regelmessig gjennomgå et passende budsjett for å oppfylle den finansielle enhetens behov i forbindelse med digital operasjonell motstandsdyktighet med hensyn til alle typer ressurser, herunder relevante IKT-programmer for å bevisstgjøre om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet nevnt i artikkel 13 nr. 6, og IKT-ferdigheter for alle ansatte,

h) godkjenne og regelmessig gjennomgå den finansielle enhetens retningslinjer for ordninger når det gjelder bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester,

i) innføre, på foretaksnivå, rapporteringskanaler som gjør det mulig å bli behørig underrettet om

i) ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester,

ii) alle relevante planlagte vesentlige endringer med hensyn til tredjepartsleverandører av IKT-tjenester,

iii) potensielle virkninger av slike endringer på de kritiske eller viktige funksjonene som omfattes av disse ordningene, herunder et sammendrag av risikoanalysen for å vurdere virkningene av disse endringene, og som et minimum alvorlige IKT-relaterte hendelser og deres virkninger, samt respons- og gjenopprettingstiltak og korrigerende tiltak.

3. Andre finansielle enheter enn svært små bedrifter skal opprette en funksjon for å overvåke ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester, eller skal utpeke et medlem av den øverste ledelsen som ansvarlig for å føre tilsyn med tilhørende risikoeksponering og relevant dokumentasjon.

4. Medlemmene av den finansielle enhetens ledelsesorgan skal hele tiden holde seg oppdatert med tilstrekkelig kunnskap og ferdigheter slik at de kan forstå og vurdere IKT-risikoen og dens innvirkning på den finansielle enhetens drift, herunder ved regelmessig å gjennomgå spesifikk opplæring som står i et rimelig forhold til den IKT-risikoen som styres.

Avsnitt II

Artikkel 6

Ramme for IKT-risikostyring

1. Finansielle enheter skal ha et forsvarlig, omfattende og veldokumentert rammeverk for IKT-risikostyring som en del av sitt overordnede risikostyringssystem, slik at de kan håndtere IKT-risiko på en rask, effektiv og grundig måte og sikre et høyt nivå av digital operasjonell motstandsdyktighet.

2. Rammeverket for IKT-risikostyring skal som et minimum omfatte strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer som er nødvendige for på behørig vis og i tilstrekkelig grad å beskytte alle informasjonsressurser og IKT-ressurser, herunder programvare, maskinvare, servere, samt for å beskytte alle relevante fysiske komponenter og infrastrukturer, som for eksempel lokaler, datasentre og følsomme utpekte områder, for å sikre at alle informasjonsressurser og IKT-ressurser er tilstrekkelig beskyttet mot risiko, herunder skade og uautorisert tilgang eller bruk.

3. I samsvar med sitt rammeverk for IKT-risikostyring skal finansielle enheter minimere virkningen av IKT-risiko gjennom å innføre egnede strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer. De skal gi fullstendige og oppdaterte opplysninger om IKT-risiko og om sitt rammeverk for IKT-risikostyring til de vedkommende myndighetene når de anmoder om det.

4. Andre finansielle enheter enn svært små bedrifter skal tildele ansvaret for å styre og føre tilsyn med IKT-risiko til en kontrollfunksjon og sikre et passende nivå av uavhengighet for en slik kontrollfunksjon for å unngå interessekonflikter. Finansielle enheter skal sikre et passende skille og uavhengighet av IKT-risikostyringsfunksjoner, kontrollfunksjoner og interne revisjonsfunksjoner i henhold til modellen med tre forsvarslinjer eller en intern modell for risikostyring og kontroll.

5. Rammeverket for IKT-risikostyring skal dokumenteres og gjennomgås minst én gang i året, eller regelmessig når det gjelder svært små bedrifter, samt når det forekommer alvorlige IKT-relaterte hendelser, og i henhold til tilsynsinstrukser eller konklusjoner fra relevante tester av digital operasjonell motstandsdyktighet eller fra revisjonsprosesser. Rammeverket skal forbedres kontinuerlig på grunnlag av erfaringer fra gjennomføring og overvåking. En rapport om gjennomgåelsen av rammeverket for IKT-risikostyring skal legges fram for den vedkommende myndigheten når den anmoder om det.

6. Rammeverket for IKT-risikostyring for andre finansielle enheter enn svært små bedrifter skal regelmessig være gjenstand for internrevisjon av revisorer i tråd med den finansielle enhetens revisjonsplan. Disse revisorene skal ha tilstrekkelig kunnskap, ferdigheter og ekspertise med hensyn til IKT-risiko samt være tilstrekkelig uavhengige. Hyppigheten av IKT-revisjoner og deres fokus skal stå i et rimelig forhold til den finansielle enhetens IKT-risiko.

7. De finansielle enhetene skal på grunnlag av konklusjonene fra internrevisjonen opprette en formell oppfølgingsprosess, herunder regler om rettidig verifisering og utbedring av kritiske resultater fra IKT-revisjonen.

8. Rammeverket for IKT-risikostyring skal omfatte en strategi for digital operasjonell motstandsdyktighet som fastsetter hvordan rammeverket skal gjennomføres. For dette formålet skal strategien for digital operasjonell motstandsdyktighet omfatte metoder for å håndtere IKT-risiko og oppfylle spesifikke IKT-mål gjennom å

a) redegjøre for hvordan rammeverket for IKT-risikostyring støtter den finansielle enhetens forretningsstrategi og mål,

b) fastsette risikotoleransenivået for IKT-risiko i samsvar med den finansielle enhetens risikovillighet og analysere toleransen mot virkninger av IKT-forstyrrelser,

c) redegjøre for klare mål for informasjonssikkerhet, herunder nøkkelindikatorer og viktige risikoparametrer,

d) redegjøre for IKT-referansearkitekturen og eventuelle endringer som er nødvendige for å nå spesifikke forretningsmål,

e) beskrive de ulike ordningene som er innført for å påvise IKT-relaterte hendelser, forebygge deres innvirkning og gi beskyttelse mot den,

f) dokumentere den nåværende situasjonen for den digitale operasjonelle motstandsdyktigheten på grunnlag av antall alvorlige IKT-relaterte hendelser som er rapportert, og effektiviteten av de forebyggende tiltakene,

g) gjennomføre testing av digital operasjonell motstandsdyktighet i samsvar med kapittel IV i denne forordningen,

h) utarbeide en kommunikasjonsstrategi i tilfelle av IKT-relaterte hendelser hvis offentliggjøring er påkrevd i samsvar med artikkel 14.

9. Finansielle enheter kan i forbindelse med strategien for digital operasjonell motstandsdyktighet som nevnt i nr. 8 utforme en helhetlig strategi med flere ulike leverandører av IKT-tjenester på konsern- eller enhetsnivå som viser hvor det er stor avhengighet av tredjepartsleverandører av IKT-tjenester, og forklare logikken bak den valgte sammensetningen av tredjepartsleverandører av IKT-tjenester.

10. Finansielle enheter kan i samsvar med unionsretten og nasjonal sektorspesifikk lovgivning utkontraktere oppgavene med å kontrollere overholdelsen av kravene til IKT-risikostyring til konserninterne eller eksterne foretak. Ved slik utkontraktering er den finansielle enheten fortsatt fullt ansvarlig for å kontrollere at kravene til IKT-risikostyring overholdes.

Artikkel 7

IKT-systemer, -protokoller og -verktøyer

For å håndtere og styre IKT-risiko skal de finansielle enhetene bruke og opprettholde oppdaterte IKT-systemer, -protokoller og -verktøyer som er

a) hensiktsmessige med hensyn til omfanget av transaksjoner som ligger til grunn for deres virksomhet, i samsvar med forholdsmessighetsprinsippet som nevnt i artikkel 4,

b) pålitelige,

c) utstyrt med tilstrekkelig kapasitet med henblikk på en korrekt behandling av de opplysningene som er nødvendige for å utføre aktiviteter og rettidig levering av tjenester, og for å håndtere toppbelastning med hensyn til ordre-, meldings- eller transaksjonsvolum etter behov, herunder når det innføres ny teknologi,

d) teknologisk motstandsdyktige for i tilstrekkelig grad å håndtere ytterligere behov for informasjonsbehandling som kreves under stressede markedsforhold eller andre vanskelige situasjoner.

Artikkel 8

Identifisering

1. Som en del av det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter identifisere, klassifisere og på en hensiktsmessig måte dokumentere alle IKT-støttede forretningsfunksjoner, roller og ansvarsområder, de informasjonsressursene og IKT-ressursene som støtter disse funksjonene, og deres roller og avhengighet med hensyn til IKT-risiko. Finansielle enheter skal ved behov og minst én gang i året vurdere hvorvidt denne klassifiseringen og all relevant dokumentasjon er tilstrekkelig.

2. Finansielle enheter skal fortløpende identifisere alle kilder til IKT-risiko, særlig risikoeksponeringen mot og fra andre finansielle enheter, og vurdere cybertrusler og IKT-sårbarheter som er relevante for deres IKT-støttede forretningsfunksjoner, informasjonsressurser og IKT-ressurser. Finansielle enheter skal regelmessig og minst én gang i året gjennomgå de risikoscenarioene som påvirker dem.

3. Andre finansielle enheter enn svært små bedrifter skal foreta en risikovurdering etter hver større endring av infrastrukturen i nettverks- og informasjonssystemene, i de prosessene eller framgangsmåtene som påvirker deres IKT-støttede forretningsfunksjoner, informasjonsressurser eller IKT-ressurser.

4. De finansielle enhetene skal identifisere alle informasjonsressurser og IKT-ressurser, herunder på eksterne steder, nettverksressurser og maskinvareutstyr, og de skal kartlegge de som anses som kritiske. De skal kartlegge konfigurasjonen til informasjonsressursene og IKT-ressursene samt forbindelsene og den gjensidige avhengigheten mellom de ulike informasjonsressursene og IKT-ressursene.

5. De finansielle enhetene skal identifisere og dokumentere alle prosesser som er avhengige av tredjepartsleverandører av IKT-tjenester, og skal identifisere innbyrdes forbindelser med tredjepartsleverandører av IKT-tjenester som leverer tjenester som støtter kritiske eller viktige funksjoner.

6. Ved anvendelse av nr. 1, 4 og 5 skal finansielle enheter føre relevante varefortegnelser og oppdatere dem regelmessig og hver gang det skjer en større endring som nevnt i nr. 3.

7. Andre finansielle enheter enn svært små bedrifter skal regelmessig og minst én gang i året foreta en særskilt IKT-risikovurdering av alle eldre IKT-systemer og i hvert tilfelle før og etter sammenkopling av teknologier, applikasjoner eller systemer.

Artikkel 9

Beskyttelse og forebygging

1. For å sikre tilstrekkelig beskyttelse av IKT-systemer og organisere mottiltak skal finansielle enheter kontinuerlig overvåke og kontrollere IKT-systemers og -verktøyers sikkerhet og virkemåte, og minimere virkningen av IKT-risiko på IKT-systemer gjennom å innføre egnede sikkerhetsverktøyer, retningslinjer og prosedyrer for IKT-sikkerhet.

2. Finansielle enheter skal utforme, anskaffe og gjennomføre IKT-relaterte sikkerhetsstrategier, -prosedyrer, -protokoller og -verktøyer som har til formål å sikre IKT-systemers motstandsdyktighet, kontinuitet og tilgjengelighet, særlig for de systemene som støtter kritiske eller viktige funksjoner, og å opprettholde høye standarder for tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, enten de er inaktive, i bruk eller under overføring.

3. For å nå målene nevnt i nr. 2 skal finansielle enheter bruke IKT-løsninger og -prosesser som er hensiktsmessige i samsvar med artikkel 4. Disse IKT-løsningene og -prosessene skal

a) sikre sikkerheten for metoden ved overføring av data,

b) minimere risikoen for korrumpering eller tap av data, uautorisert tilgang og tekniske feil som kan hemme forretningsvirksomheten,

c) forhindre mangel på tilgjengelighet, svekkelse av autentisiteten og integriteten, brudd på regler om fortrolighet og tap av data,

d) sikre at opplysningene er beskyttet mot risikoer som oppstår i forbindelse med databehandling, herunder dårlig forvaltning, prosessrelaterte risikoer og menneskelige feil.

4. Som en del av det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter

a) utarbeide og dokumentere retningslinjer for informasjonssikkerhet der det er fastsatt regler for å beskytte tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, informasjonsressurser og IKT-ressurser, herunder hos deres kunder, dersom det er relevant,

b) ved å følge en risikobasert tilnærming, innføre en forsvarlig forvaltningsstruktur for nettverk og infrastrukturer ved hjelp av passende teknikker, metoder og protokoller som kan omfatte gjennomføring av automatiserte ordninger for å isolere berørte informasjonsressurser ved cyberangrep,

c) gjennomføre retningslinjer som begrenser den fysiske eller logiske tilgangen til informasjonsressurser og IKT-ressurser til bare det som kreves for legitime og godkjente funksjoner og aktiviteter, og innføre en rekke retningslinjer, framgangsmåter og kontroller som omhandler tilgangsrettigheter, og sikre en forsvarlig forvaltning av disse,

d) gjennomføre retningslinjer og protokoller for sterke systemer for autentisering på grunnlag av relevante standarder og særskilte kontrollsystemer, og beskyttelsestiltak for kryptonøkler der data krypteres på grunnlag av resultatene av godkjente prosesser for dataklassifisering og IKT-risikovurdering,

e) gjennomføre dokumenterte retningslinjer, framgangsmåter og kontroller for håndtering av IKT-endringer, herunder endringer av programvare, maskinvare, fastvarekomponenter, systemer eller sikkerhetsparametrer, som bygger på en risikovurderingsmetode og er en integrert del av den finansielle enhetens overordnede prosess for endringsstyring, for å sikre at alle endringer av IKT-systemer registreres, testes, vurderes, godkjennes, gjennomføres og verifiseres på en kontrollert måte,

f) sørge for at det innføres hensiktsmessige og omfattende dokumenterte retningslinjer for programvareutbedringer og oppdateringer.

Ved anvendelse av første ledd bokstav b) skal finansielle enheter utforme infrastrukturen for nettilkopling på en måte som gjør det mulig å avbryte eller segmentere den øyeblikkelig for å minimere og forhindre spredning, særlig i forbindelse med innbyrdes forbundne finansielle prosesser.

Ved anvendelse av første ledd bokstav e) skal prosessen for håndtering av IKT-endringer godkjennes av passende ledelsesnivåer og omfatte spesifikke protokoller.

Artikkel 10

Påvisning

1. De finansielle enhetene skal ha ordninger for rask påvisning av anormal virksomhet i samsvar med artikkel 17, herunder problemer med IKT-nettverkets yteevne og IKT-relaterte hendelser, og for å identifisere potensielle vesentlige svake punkter («single points of failure»).

Alle ordninger for påvisning omhandlet i første ledd skal testes regelmessig i samsvar med artikkel 25.

2. Ordningene for påvisning nevnt i nr. 1 skal muliggjøre flere kontrollnivåer, inneholde fastsatte varslingsterskler og varslingskriterier for å utløse og iverksette IKT-relaterte hendelser, herunder automatiske varslingsordninger for det relevante personalet som har ansvar for håndtering av IKT-relaterte hendelser.

3. De finansielle enhetene skal avsette tilstrekkelig med ressurser og kapasitet for å overvåke brukeraktivitet, forekomsten av IKT-avvik og IKT-relaterte hendelser, særlig cyberangrep.

4. Leverandørene av datarapporteringstjenester skal i tillegg ha systemer som på en effektiv måte kan kontrollere om handelsrapportene er fullstendige, identifisere utelatelser og åpenbare feil og anmode om at disse rapportene overføres på nytt.

Artikkel 11

Respons og gjenoppretting

1. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1 og på grunnlag av kravene til identifisering som er fastsatt i artikkel 8, skal finansielle enheter innføre omfattende retningslinjer for IKT-kontinuitet i virksomheten, som kan vedtas som egne spesifikke retningslinjer, og som utgjør en integrert del av den finansielle enhetens overordnede retningslinjer for kontinuitet i virksomheten.

2. De finansielle enhetene skal gjennomføre retningslinjer for IKT-kontinuitet i virksomheten gjennom særskilte, hensiktsmessige og dokumenterte ordninger, planer, framgangsmåter og ordninger som tar sikte på

a) å sikre kontinuiteten i den finansielle enhetens kritiske eller viktige funksjoner,

b) å reagere på og løse alle IKT-relaterte hendelser raskt, riktig og effektivt på en måte som begrenser skade og prioriterer gjenopptakelse av virksomhet og gjenopprettingstiltak,

c) å aktivere omgående særskilte planer som muliggjør begrensningstiltak, prosesser og teknologier tilpasset hver type av IKT-relatert hendelse, og som forhindrer ytterligere skader, samt skreddersydde framgangsmåter for respons og gjenoppretting som fastsatt i samsvar med artikkel 12,

d) å beregne foreløpige virkninger, skader og tap,

e) å fastsette kommunikasjons- og krisehåndteringstiltak som sikrer at oppdaterte opplysninger overføres til alt berørt internt personale og eksterne berørte parter i samsvar med artikkel 14, og at de rapporteres til de vedkommende myndighetene i samsvar med artikkel 19.

3. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter gjennomføre tilhørende planer for IKT-respons og -gjenoppretting som, når det gjelder andre finansielle enheter enn svært små bedrifter, skal gjennomgås av uavhengige internrevisjoner.

4. De finansielle enhetene skal innføre, opprettholde og regelmessig teste hensiktsmessige planer for IKT-kontinuitet i virksomheten, særlig med hensyn til kritiske eller viktige funksjoner som er utkontraktert eller kontrahert gjennom ordninger inngått med tredjepartsleverandører av IKT-tjenester.

5. De finansielle enhetene skal som en del av sine overordnede retningslinjer for kontinuitet i virksomheten foreta en driftskonsekvensanalyse av hvor eksponerte de er mot alvorlige driftsforstyrrelser. De finansielle enhetene skal i forbindelse med driftskonsekvensanalysen vurdere potensielle virkninger av alvorlige driftsforstyrrelser ved hjelp av kvantitative og kvalitative kriterier ved anvendelse av interne og eksterne data og scenarioanalyse, alt etter hva som er relevant. Driftskonsekvensanalysen skal ta hensyn til den kritiske verdien til identifiserte og kartlagte forretningsfunksjoner, støtteprosesser, avhengighet av tredjeparter og informasjonsressurser og deres gjensidige avhengighet. De finansielle enhetene skal sikre at IKT-ressurser og IKT-tjenester utformes og anvendes helt i tråd med driftskonsekvensanalysen, særlig når det gjelder å sikre i tilstrekkelig grad alle kritiske komponenters redundans.

6. De finansielle enhetene skal som en del av sin omfattende IKT-risikostyring

a) teste planene for IKT-kontinuitet i virksomheten og planene for IKT-respons og -gjenoppretting i forbindelse med IKT-systemer som støtter alle funksjoner minst én gang i året, samt ved eventuelle vesentlige endringer av IKT-systemer som støtter kritiske eller viktige funksjoner,

b) teste de krisekommunikasjonsplanene som er utarbeidet i samsvar med artikkel 14.

Ved anvendelse av første ledd bokstav a) skal andre finansielle enheter enn svært små bedrifter ta med i testplanene scenarioer for cyberangrep og overflytting mellom den primære IKT-infrastrukturen og den redundante kapasiteten, sikkerhetskopier og de redundante anleggene som er nødvendige for å oppfylle forpliktelsene fastsatt i artikkel 12.

De finansielle enhetene skal regelmessig gjennomgå sine retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting, samtidig som det tas hensyn til resultatene av de testene som er utført i samsvar med første ledd, og anbefalinger som bygger på revisjonskontroller eller tilsynskontroller.

7. Andre finansielle enheter enn svært små bedrifter skal ha en krisehåndteringsfunksjon som, dersom deres planer for IKT-kontinuitet i virksomheten eller planer for IKT-respons og -gjenoppretting aktiveres, blant annet skal inneholde tydelige framgangsmåter for å håndtere intern og ekstern krisekommunikasjon i samsvar med artikkel 14.

8. De finansielle enhetene skal føre lett tilgjengelige registre over aktiviteter som pågår før og ved driftsforstyrrelser, når deres planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting aktiveres.

9. Verdipapirsentraler skal legge fram kopier av resultatene av testene av IKT-kontinuitet i virksomheten eller av lignende aktiviteter for de vedkommende myndighetene.

10. Andre finansielle enheter enn svært små bedrifter skal på anmodning fra de vedkommende myndighetene innberette et overslag over samlede årlige kostnader og tap forårsaket av alvorlige IKT-relaterte hendelser.

11. I samsvar med artikkel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 skal de europeiske tilsynsmyndighetene gjennom Felleskomiteen innen 17. juli 2024 utarbeide felles retningslinjer for overslaget over de samlede årlige kostnadene og tapene nevnt i nr. 10.

Artikkel 12

Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting

1. For å sikre gjenskapelse av IKT-systemer og data med minimal nedetid, begrensede forstyrrelser og tap skal finansielle enheter som en del av sitt rammeverk for IKT-risikostyring utarbeide og dokumentere

a) retningslinjer og framgangsmåter for sikkerhetskopiering som angir omfanget av de dataene som skal sikkerhetskopieres, og minste hyppighet for sikkerhetskopiering, basert på opplysningenes kritiske verdi eller fortrolighetsnivået for opplysningene,

b) framgangsmåter og metoder for gjenskapelse og gjenoppretting.

2. De finansielle enhetene skal sette opp systemer for sikkerhetskopiering som kan aktiveres i samsvar med retningslinjene og framgangsmåtene for sikkerhetskopiering, samt framgangsmåter og metoder for gjenskapelse og gjenoppretting. Aktiveringen av systemer for sikkerhetskopiering skal ikke sette sikkerheten til nettverks- og informasjonssystemene eller tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene i fare. Testing av framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting skal gjennomføres med jevne mellomrom.

3. Når finansielle enheter gjenskaper sikkerhetskopierte data ved bruk av egne systemer, skal de bruke IKT-systemer som er fysisk og logisk atskilt fra det IKT-systemet som er kilden. IKT-systemene skal ha en sikker beskyttelse mot enhver form for uautorisert tilgang eller IKT-korrumpering og gjøre det mulig å gjenskape tjenester ved hjelp av sikkerhetskopiering av data og systemer etter behov.

For sentrale motparter skal gjenopprettingsplaner gjøre det mulig å gjenopprette alle transaksjoner fra det tidspunktet da de ble avbrutt, slik at den sentrale motpartens virksomhet fortsatt er sikker og avviklingen kan fullføres på den planlagte datoen.

Leverandørene av datarapporteringstjenester skal dessuten ha tilstrekkelige ressurser og fasiliteter for sikkerhetskopiering og gjenskapelse, slik at de kan tilby og opprettholde sine tjenester til enhver tid.

4. Andre finansielle enheter enn svært små bedrifter skal opprettholde redundant IKT-kapasitet med ressurser, evne og funksjoner som er tilstrekkelige for å sikre virksomhetens behov. Svært små bedrifter skal vurdere behovet for å opprettholde en slik redundant IKT-kapasitet på grunnlag av hvilken risikoprofil de har.

5. Verdipapirsentraler skal ha minst ett sekundært driftssted utstyrt med tilstrekkelige ressurser, evne, funksjoner og personalmessige ordninger for å sikre virksomhetens behov.

Det sekundære driftsstedet skal

a) være plassert tilstrekkelig langt fra det primære driftsstedet for å sikre at det har en annen risikoprofil, og for å forhindre at det påvirkes av den hendelsen som påvirker det primære driftsstedet,

b) kunne sikre kontinuiteten for kritiske eller viktige funksjoner som er identiske med det primære driftsstedet, eller opprettholde det tjenestenivået som er nødvendig for å sikre at den finansielle enheten kan utføre sin kritiske virksomhet innenfor rammen av gjenopprettingsmålene,

c) være tilgjengelig umiddelbart for den finansielle enhetens personale for å sikre kontinuiteten for kritiske eller viktige funksjoner dersom det primære driftsstedet ikke er tilgjengelig.

6. Når finansielle enheter fastsetter mål for gjenopprettingstid og gjenopprettingspunkt for hver funksjon, skal de ta hensyn til om det er en kritisk eller viktig funksjon, og til den mulige samlede innvirkningen på markedets effektivitet. Slike tidsmål skal sikre at de avtalte tjenestenivåene oppnås i ekstreme scenarioer.

7. Når de finansielle enhetene gjenoppretter virksomheten etter en IKT-relatert hendelse, skal de utføre nødvendige kontroller, herunder eventuelt flere kontroller og avstemminger, for å sikre at dataintegriteten holder høyeste nivå. Disse kontrollene skal også utføres når data fra eksterne berørte parter rekonstrueres, for å sikre at alle dataene til systemene er sammenhengende.

Artikkel 13

Læring og utvikling

1. De finansielle enhetene skal sørge for å ha kapasitet og personale som kan samle inn opplysninger om sårbarheter og cybertrusler, IKT-relaterte hendelser, særlig cyberangrep, og analysere hvilken innvirkning de forventes å ha på deres digitale operasjonelle motstandsdyktighet.

2. De finansielle enhetene skal gjennomgå IKT-relaterte hendelser etter at en alvorlig IKT-relatert hendelse forstyrrer deres kjernevirksomhet, analysere årsakene til forstyrrelsen og identifisere nødvendige forbedringer av IKT-virksomheten eller av de retningslinjene for IKT-kontinuitet i virksomheten som er nevnt i artikkel 11.

Andre finansielle enheter enn svært små bedrifter skal, på anmodning, underrette de vedkommende myndighetene om endringene som ble gjennomført etter gjennomgåelsen av IKT-relaterte hendelser som nevnt i første ledd.

Gjennomgåelsene etter IKT-relaterte hendelser nevnt i første ledd skal avgjøre om de fastsatte framgangsmåtene ble fulgt, og om de tiltakene som ble truffet, var effektive, blant annet når det gjelder

a) svartiden for å reagere på sikkerhetsvarsler og fastslå virkningen av IKT-relaterte hendelser og alvorlighetsgraden av dem,

b) kvaliteten og hastigheten i forbindelse med utførelse av en kriminalteknisk analyse, dersom det anses som hensiktsmessig,

c) effektiviteten av den finansielle enhetens håndtering av feilhendelser,

d) effektiviteten av intern og ekstern kommunikasjon.

3. Erfaringer fra testing av den digitale operasjonelle motstandsdyktigheten som er utført i samsvar med artikkel 26 og 27, og fra faktiske IKT-relaterte hendelser, særlig cyberangrep, samt utfordringer som oppstår i forbindelse med aktiveringen av planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting, skal sammen med relevante opplysninger som utveksles med motparter, og som vurderes i forbindelse med tilsynskontroller, fortløpende innarbeides i IKT-risikovurderingsprosessen. Disse resultatene skal danne grunnlag for hensiktsmessige gjennomgåelser av relevante komponenter i det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1.

4. De finansielle enhetene skal overvåke effektiviteten av gjennomføringen av den strategien for digital operasjonell motstandsdyktighet som er fastsatt i artikkel 6 nr. 8. De skal kartlegge IKT-risikoens utvikling over tid, analysere hyppigheten, typene, omfanget og utviklingen av IKT-relaterte hendelser, særlig cyberangrep og deres mønstre, med henblikk på å forstå graden av IKT-risikoeksponering, særlig når det gjelder kritiske eller viktige funksjoner, og forbedre den finansielle enhetens cybermodenhet og cyberberedskap.

5. Ledende IKT-ansatte skal minst én gang i året rapportere til ledelsesorganet om de resultatene som er nevnt i nr. 3, og legge fram anbefalinger.

6. De finansielle enhetene skal utarbeide bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet som obligatoriske moduler i sine ordninger for personalopplæring. Disse programmene og denne opplæringen skal gjelde for alle ansatte og for personer i den øverste ledelsen, og skal ha en grad av kompleksitet som tilsvarer deres oppgavers ansvarsområde. Dersom det er relevant, skal finansielle enheter også inkludere tredjepartsleverandører av IKT-tjenester i sine relevante opplæringsordninger i samsvar med artikkel 30 nr. 2 bokstav i).

7. Andre finansielle enheter enn svært små bedrifter skal overvåke den relevante teknologiske utviklingen fortløpende, også for å forstå hvilken virkning innføringen av slike nye teknologier kan få på kravene til IKT-sikkerhet og digital operasjonell motstandsdyktighet. De skal holde seg oppdatert om de seneste prosessene for IKT-risikostyring for å bekjempe aktuelle eller nye former for cyberangrep på en effektiv måte.

Artikkel 14

Kommunikasjon

1. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter ha krisekommunikasjonsplaner som gjør det mulig å informere kunder og motparter samt allmennheten på en ansvarsfull måte om minst alvorlige IKT-relaterte hendelser eller sårbarheter, alt etter hva som er relevant.

2. Som en del av rammeverket for IKT-risikostyring skal finansielle enheter gjennomføre kommunikasjonsstrategier for internt ansatte og eksterne berørte parter. I kommunikasjonsstrategiene for de ansatte skal det tas hensyn til behovet for å skille mellom ansatte som deltar i IKT-risikostyring, særlig ansatte som har ansvar for respons og gjenoppretting, og ansatte som har behov for opplysninger.

3. Minst én person i den finansielle enheten skal ha i oppgave å gjennomføre kommunikasjonsstrategien for IKT-relaterte hendelser og fungere som talsperson overfor allmennheten og mediene for dette formålet.

Artikkel 15

Ytterligere harmonisering av verktøyer, metoder, framgangsmåter og retningslinjer for IKT-risikostyring

De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med Den europeiske unions cybersikkerhetsbyrå (ENISA) utarbeide felles utkast til tekniske reguleringsstandarder for å

a) spesifisere hvilke ytterligere elementer som skal inngå i retningslinjene, protokollene og verktøyene for IKT-sikkerhet som nevnt i artikkel 9 nr. 2, med henblikk på å garantere sikkerheten i nettverkene, sikre tilstrekkelige garantier mot inntrengning og misbruk av data, bevare tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, herunder krypteringsteknikker, og garantere en nøyaktig og rask dataoverføring uten større forstyrrelser og unødige forsinkelser,

b) utvikle ytterligere komponenter i den håndteringen av kontroll med tilgangsrettigheter som er nevnt i artikkel 9 nr. 4 bokstav c), og tilhørende personalpolitikk som angir tilgangsrettigheter, framgangsmåter for tildeling og tilbakekalling av rettigheter, overvåking av anormal atferd i forbindelse med IKT-risiko ved hjelp av egnede indikatorer, herunder mønstre for nettbruk, tidspunkter, IT-aktivitet og ukjent utstyr,

c) videreutvikle de ordningene som er angitt i artikkel 10 nr. 1, og som muliggjør umiddelbar påvisning av anormal virksomhet, og de kriteriene som er fastsatt i artikkel 10 nr. 2, for å utløse IKT-relaterte prosesser for påvisning av og håndtering av hendelser,

d) spesifisere nærmere komponentene i de retningslinjene for IKT-kontinuitet i virksomheten som er nevnt i artikkel 11 nr. 1,

e) spesifisere nærmere testingen av IKT-kontinuitet i virksomheten som nevnt i artikkel 11 nr. 6 for å sikre at slik testing tar behørig hensyn til scenarioer der kvaliteten på leveringen av en kritisk eller viktig funksjon forverres til et uakseptabelt nivå eller mislykkes, og tar behørig hensyn til den potensielle virkningen av insolvens eller andre feil forårsaket av en eventuell berørt tredjepartsleverandør av IKT-tjenester og, dersom det er relevant, de politiske risikoene i de respektive leverandørenes jurisdiksjoner,

f) spesifisere nærmere komponentene i planene for IKT-respons og -gjenoppretting som nevnt i artikkel 11 nr. 3,

g) spesifisere nærmere innholdet i og formatet for rapporten om gjennomgåelse av rammeverket for IKT-risikostyring som nevnt i artikkel 6 nr. 5.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift, samtidig som de skal ta behørig hensyn til eventuelle særtrekk som følge av den særskilte arten av aktiviteter i ulike sektorer for finansielle tjenester.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 16

Forenklet rammeverk for IKT-risikostyring

1. Artikkel 5–15 i denne forordningen får ikke anvendelse på små verdipapirforetak uten innbyrdes forbindelser, betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, foretak som er unntatt i henhold til direktiv 2013/36/EU, og for hvilke medlemsstatene har besluttet ikke å anvende den muligheten som er nevnt i artikkel 2 nr. 4 i denne forordningen, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og små tjenestepensjonsforetak.

Med forbehold for første ledd skal enhetene som er oppført i første ledd,

a) innføre og opprettholde et forsvarlig og dokumentert rammeverk for IKT-risikostyring som spesifiserer de ordningene og tiltakene som skal muliggjøre en rask, effektiv og omfattende styring av IKT-risiko, herunder for beskyttelse av relevante fysiske komponenter og infrastrukturer,

b) kontinuerlig overvåke alle IKT-systemers sikkerhet og virkemåte,

c) minimere virkningen av IKT-risiko gjennom bruk av forsvarlige, robuste og oppdaterte IKT-systemer, -protokoller og -verktøyer som er egnet til å støtte utførelsen av deres aktiviteter og levering av tjenester og i tilstrekkelig grad beskytte tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene i nettverks- og informasjonssystemene,

d) gjøre det mulig raskt å identifisere og oppdage kilder til IKT-risiko og avvik i nettverks- og informasjonssystemene, og raskt håndtere IKT-relaterte hendelser,

e) identifisere stor avhengighet av tredjepartsleverandører av IKT-tjenester,

f) sikre kontinuiteten for kritiske eller viktige funksjoner gjennom planer for kontinuitet i virksomheten og respons- og gjenopprettingstiltak, som minst omfatter tiltak for sikkerhetskopiering og gjenoppretting,

g) regelmessig teste planene og tiltakene nevnt i bokstav f), samt effektiviteten av kontrollene som er gjennomført i samsvar med bokstav a) og c),

h) gjennomføre, alt etter hva som er relevant, de relevante operasjonelle konklusjonene som følger av de testene som er nevnt i bokstav g), og av analysen etter hendelsen i IKT-risikovurderingsprosessen, og etter behov og IKT-risikoprofil utarbeide bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet for de ansatte og ledelsen.

2. Rammeverket for IKT-risikostyring nevnt i nr. 1 andre ledd bokstav a) skal dokumenteres og gjennomgås regelmessig og når det forekommer alvorlige IKT-relaterte hendelser i samsvar med tilsynsinstruksene. Rammeverket skal forbedres kontinuerlig på grunnlag av erfaringer fra gjennomføring og overvåking. En rapport om gjennomgåelsen av rammeverket for IKT-risikostyring skal legges fram for den vedkommende myndigheten når den anmoder om det.

3. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ENISA utarbeide felles utkast til tekniske reguleringsstandarder for å

a) spesifisere nærmere hvilke elementer som skal inngå i rammeverket for IKT-risikostyring nevnt i nr. 1 andre ledd bokstav a),

b) spesifisere nærmere elementene i forbindelse med systemer, protokoller og verktøyer for å minimere virkningen av IKT-risiko som nevnt i nr. 1 andre ledd bokstav c), med henblikk på å garantere sikkerheten i nettverkene, sikre tilstrekkelige garantier mot inntrengning og misbruk av data og bevare tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene,

c) spesifisere nærmere komponentene i planene for IKT-kontinuitet i virksomheten som nevnt i nr. 1 andre ledd bokstav f),

d) spesifisere nærmere reglene om testing av planer for kontinuitet i virksomheten og sikre at de kontrollene som er nevnt i nr. 1 andre ledd bokstav g), er effektive, og sikre at det ved slik testing tas behørig hensyn til scenarioer der kvaliteten på leveringen av en kritisk eller viktig funksjon forverres til et uakseptabelt nivå eller mislykkes,

e) spesifisere nærmere innholdet i og formatet for rapporten om gjennomgåelsen av rammeverket for IKT-risikostyring som nevnt i nr. 2.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

KAPITTEL III

HÅNDTERING, KLASSIFISERING OG RAPPORTERING AV IKT-RELATERTE hendelser

Artikkel 17

Prosess for håndtering av IKT-relaterte hendelser

1. De finansielle enhetene skal fastsette, opprette og gjennomføre en prosess for håndtering av IKT-relaterte hendelser for å påvise, håndtere og innberette IKT-relaterte hendelser.

2. De finansielle enhetene skal registrere alle IKT-relaterte hendelser og betydelige cybertrusler. De finansielle enhetene skal opprette hensiktsmessige framgangsmåter og prosesser for å sikre en ensartet og integrert overvåking, håndtering og oppfølging av IKT-relaterte hendelser, for å sikre at de grunnleggende årsakene identifiseres, dokumenteres og håndteres for å hindre at slike hendelser inntreffer.

3. Som ledd i prosessen for håndtering av IKT-relaterte hendelser nevnt i nr. 1

a) innføres indikatorer for tidlig varsling,

b) fastsettes framgangsmåter for å identifisere, spore, logge, kategorisere og klassifisere IKT-relaterte hendelser, alt etter deres prioritet og alvorlighetsgrad og i henhold til hvor kritiske de berørte tjenestene er, i samsvar med kriteriene fastsatt i artikkel 18 nr. 1,

c) tildeles roller og ansvarsområder som må aktiveres for ulike IKT-relaterte hendelsestyper og IKT-relaterte scenarioer,

d) utarbeides planer for kommunikasjon til ansatte, eksterne berørte parter og medier i samsvar med artikkel 14 og planer for underretning av kunder, planer for interne eskaleringsprosedyrer, herunder IKT-relaterte kundeklager, samt planer for formidling av opplysninger til finansielle enheter som opptrer som motparter, alt etter hva som er relevant,

e) sikres det at alvorlige IKT-relaterte hendelser som et minimum blir rapportert til den relevante øverste ledelsen, og at ledelsesorganet som et minimum underrettes om alvorlige IKT-relaterte hendelser, med en redegjørelse for virkningene, tiltakene og ytterligere kontroller som skal fastsettes som følge av slike IKT-relaterte hendelser,

f) treffes det framgangsmåter for tiltak i forbindelse med IKT-relaterte hendelser for å begrense virkningene og sikre at tjenestene raskt blir operasjonelle og sikre.

Artikkel 18

Klassifisering av IKT-relaterte hendelser og cybertrusler

1. De finansielle enhetene skal klassifisere IKT-relaterte hendelser og fastsette deres innvirkning på grunnlag av følgende kriterier:

a) Antallet og/eller betydningen av kunder eller finansielle motparter som er berørt, og, dersom det er relevant, mengden eller antallet av transaksjoner som er berørt av den IKT-relaterte hendelsen, og om den IKT-relaterte hendelsen har påvirket omdømmet.

b) Varigheten av den IKT-relaterte hendelsen, herunder tjenestens nedetid.

c) Den geografiske spredningen med hensyn til områdene som påvirkes av den IKT-relaterte hendelsen, særlig dersom den påvirker mer enn to medlemsstater.

d) Datatap som den IKT-relaterte hendelsen medfører, når det gjelder tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene.

e) De berørte tjenestenes kritiske verdi, herunder den finansielle enhetens transaksjoner og virksomhet.

f) De økonomiske virkningene, særlig direkte og indirekte kostnader og tap, av den IKT-relaterte hendelsen i både absolutte og relative tall.

2. De finansielle enhetene skal klassifisere cybertrusler som betydelige på grunnlag av de utsatte tjenestenes kritiske verdi, herunder den finansielle enhetens transaksjoner og virksomhet, antallet og/eller betydningen av kunder eller finansielle motparter som rammes, og den geografiske spredningen av de områdene som er utsatt for risiko.

3. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ESB og ENISA utarbeide felles utkast til tekniske reguleringsstandarder som spesifiserer følgende nærmere:

a) Kriteriene fastsatt i nr. 1, herunder vesentlighetsterskler for å fastslå alvorlige IKT-relaterte hendelser eller, dersom det er relevant, alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, som er omfattet av rapporteringsforpliktelsen fastsatt i artikkel 19 nr. 1.

b) Kriteriene som skal anvendes av vedkommende myndigheter for å vurdere betydningen av alvorlige IKT-relaterte hendelser eller, dersom det er relevant, av alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, for berørte vedkommende myndigheter i andre medlemsstater, og de nærmere opplysningene i rapportene om alvorlige IKT-relaterte hendelser eller, dersom det er relevant, alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, som skal deles med andre vedkommende myndigheter i henhold til artikkel 19 nr. 6 og 7.

c) Kriteriene fastsatt i nr. 2 i denne artikkelen, herunder høye vesentlighetsterskler for å fastslå betydelige cybertrusler.

4. Når de europeiske tilsynsmyndighetene utarbeider det felles utkastet til tekniske reguleringsstandarder nevnt i nr. 3 i denne artikkelen, skal de ta hensyn til kriteriene fastsatt i artikkel 4 nr. 2, samt til internasjonale standarder, veiledninger og spesifikasjoner som ENISA har utarbeidet og offentliggjort, herunder, dersom det er relevant, spesifikasjoner for andre økonomiske sektorer. Ved anvendelse av kriteriene angitt i artikkel 4 nr. 2 skal de europeiske tilsynsmyndighetene ta behørig hensyn til behovet for at svært små, små og mellomstore bedrifter mobiliserer tilstrekkelige ressurser og kapasitet til å sikre at IKT-relaterte hendelser håndteres raskt.

De europeiske tilsynsmyndighetene skal framlegge disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i nr. 3 i denne artikkelen, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 19

Rapportering av alvorlige IKT-relaterte hendelser og frivillig underretning om betydelige cybertrusler

1. De finansielle enhetene skal rapportere alvorlige IKT-relaterte hendelser til den berørte vedkommende myndigheten nevnt i artikkel 46 i samsvar med nr. 4 i denne artikkelen.

Dersom en finansiell enhet er underlagt tilsyn av mer enn én nasjonal vedkommende myndighet som nevnt i artikkel 46, skal medlemsstatene utpeke én enkelt vedkommende myndighet som berørt vedkommende myndighet med ansvar for å ivareta de funksjonene og oppgavene som er fastsatt i denne artikkelen.

Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, skal rapportere alvorlige IKT-relaterte hendelser til den relevante nasjonale vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i direktiv 2013/36/EU, og som umiddelbart skal sende denne rapporten til Den europeiske sentralbank (ESB).

Med henblikk på første ledd skal finansielle enheter, etter å ha innhentet og analysert alle relevante opplysninger, utarbeide den første underretningen og de rapportene som er nevnt i nr. 4 i denne artikkelen ved bruk av malene nevnt i artikkel 20, og legge dem fram for den vedkommende myndigheten. Dersom det teknisk sett er umulig å sende inn den første underretningen ved bruk av malen, skal de finansielle enhetene meddele den vedkommende myndigheten om dette på annet vis.

Den første underretningen og rapportene nevnt i nr. 4 skal omfatte alle opplysninger som er nødvendige for at den vedkommende myndigheten skal kunne fastslå betydningen av den alvorlige IKT-relaterte hendelsen og vurdere mulige virkninger over landegrensene.

Uten at det berører den finansielle enhetens rapportering i henhold til første ledd til den berørte vedkommende myndigheten, kan medlemsstatene i tillegg bestemme at visse eller alle finansielle enheter også skal sende inn den første underretningen og hver rapport som er nevnt i nr. 4 i denne artikkelen ved bruk av malene nevnt i artikkel 20, til de vedkommende myndighetene eller enhetene for håndtering av digitale hendelser (CSIRT-enheter) som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555.

2. De finansielle enhetene kan på frivillig grunnlag underrette den berørte vedkommende myndigheten om betydelige cybertrusler når de anser trusselen som relevant for finanssystemet, tjenestebrukerne eller kundene. Den berørte vedkommende myndigheten kan gi slike opplysninger til andre relevante myndigheter som nevnt i nr. 6.

Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, kan på frivillig grunnlag underrette om betydelige cybertrusler til den relevante nasjonale vedkommende myndigheten, som er utpekt i samsvar med artikkel 4 i direktiv 2013/36/EU, og som umiddelbart skal sende meldingen til Den europeiske sentralbank (ESB).

Medlemsstatene kan bestemme at disse finansielle enhetene som på frivillig grunnlag underretter i samsvar med første ledd, også kan videresende denne underretningen til de CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.

3. Dersom en alvorlig IKT-relatert hendelse inntreffer og har innvirkning på kundenes finansielle interesser, skal finansielle enheter uten unødig opphold og så snart de får kjennskap til den, informere sine kunder om den alvorlige IKT-relaterte hendelsen og om hvilke tiltak som er truffet for å begrense skadevirkningene av en slik hendelse.

I tilfelle av en betydelig cybertrussel skal finansielle enheter, dersom det er relevant, informere de av kundene som potensielt er berørt av eventuelle egnede beskyttelsestiltak, som sistnevnte kan overveie å treffe.

4. De finansielle enhetene skal innen de tidsfristene som skal fastsettes i samsvar med artikkel 20 første ledd bokstav a) ii), legge fram følgende for den berørte vedkommende myndigheten:

a) En første underretning.

b) En foreløpig rapport etter den første underretningen nevnt i bokstav a) så snart statusen til den opprinnelige hendelsen har endret seg vesentlig, eller håndteringen av den alvorlige IKT-relaterte hendelsen har endret seg på grunnlag av nye tilgjengelige opplysninger, etterfulgt av, alt etter hva som er relevant, oppdaterte underretninger hver gang en relevant statusoppdatering er tilgjengelig, samt på særskilt anmodning fra den vedkommende myndigheten.

c) En sluttrapport, når analysen av de grunnleggende årsakene er fullført, uavhengig av om de avbøtende tiltakene allerede er gjennomført, og når tallene for de faktiske virkningene foreligger og kan erstatte estimatene.

5. De finansielle enhetene kan i samsvar med unionsretten og nasjonal sektorspesifikk lovgivning utkontraktere rapporteringsforpliktelsene i henhold til denne artikkelen til en tredjepartsleverandør av tjenester. Ved en slik utkontraktering bærer den finansielle enheten det fulle ansvaret for å oppfylle kravene til rapportering av hendelser.

6. Når den vedkommende myndigheten mottar den første underretningen og hver rapport som nevnt i nr. 4, skal den til rett tid gi opplysninger om den alvorlige IKT-relaterte hendelsen til følgende mottakere, alt etter hva som er relevant, på grunnlag av deres respektive kompetanse:

a) EBA, ESMA eller EIOPA.

b) ESB når det gjelder finansielle enheter som nevnt i artikkel 2 nr. 1 bokstav a), b) og d).

c) De vedkommende myndighetene, felles kontaktpunktene eller CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.

d) De krisehåndteringsmyndighetene som nevnt i artikkel 3 i direktiv 2014/59/EU og Det felles krisehåndteringsråd med hensyn til de enhetene som er nevnt i artikkel 7 nr. 2 i europaparlaments- og rådsforordning (EU) nr. 806/2014([37]), og med hensyn til enheter og grupper som nevnt i artikkel 7 nr. 4 bokstav b) og nr. 5 i forordning (EU) nr. 806/2014, dersom slike opplysninger gjelder hendelser som utgjør en risiko for å sikre kritiske funksjoner i henhold til artikkel 2 nr. 1 punkt 35) i direktiv 2014/59/EU.

e) Andre relevante offentlige myndigheter i henhold til nasjonal rett.

7. Etter å ha mottatt opplysningene i samsvar med nr. 6 skal EBA, ESMA eller EIOPA og ESB, i samråd med ENISA og i samarbeid med den berørte vedkommende myndigheten, vurdere om den alvorlige IKT-relaterte hendelsen er relevant for vedkommende myndigheter i andre medlemsstater. Etter denne vurderingen skal EBA, ESMA eller EIOPA så snart som mulig underrette berørte vedkommende myndigheter i andre medlemsstater om dette. ESB skal underrette medlemmene av Det europeiske system av sentralbanker om spørsmål som har betydning for betalingssystemet. På grunnlag av denne underretningen skal de vedkommende myndighetene, dersom det er relevant, treffe alle nødvendige tiltak for å ivareta finanssystemets umiddelbare stabilitet.

([37]) Europaparlaments- og rådsforordning (EU) nr. 806/2014 av 15. juli 2014 om fastsettelse av ensartede regler og en ensartet framgangsmåte for krisehåndtering av kredittinstitusjoner og visse verdipapirforetak innenfor rammen av en felles krisehåndteringsordning og et felles krisehåndteringsfond og om endring av forordning (EU) nr. 1093/2010 (EUT L 225 av 30.7.2014, s. 1).

8. Underretningen som skal utarbeides av ESMA i henhold til nr. 7 i denne artikkelen, skal ikke berøre den vedkommende myndighetens ansvar for omgående å oversende nærmere opplysninger om den alvorlige IKT-relaterte hendelsen til den berørte myndigheten i vertsstaten, dersom en verdipapirsentral har betydelig virksomhet over landegrensene i vertsstaten, den alvorlige IKT-relaterte hendelsen sannsynligvis vil få alvorlige konsekvenser for vertsstatens finansmarkeder og det finnes samarbeidsordninger mellom vedkommende myndigheter som gjelder tilsyn med finansielle enheter.

Artikkel 20

Harmonisering av rapporteringsinnhold og -maler

De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ENISA og ESB utarbeide

a) felles utkast til tekniske reguleringsstandarder for å

   i) fastsette innholdet i rapportene om alvorlige IKT-relaterte hendelser for å gjenspeile kriteriene fastsatt i artikkel 18 nr. 1 og innarbeide ytterligere elementer, som for eksempel nærmere opplysninger for å fastsette hvorvidt rapporteringen er relevant for andre medlemsstater, og hvorvidt den utgjør en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse,

   ii) fastsette fristene for den første underretningen og for hver rapport nevnt i artikkel 19 nr. 4,

   iii) fastsette innholdet i underretningen om betydelige cybertrusler.

   Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift, og særlig med henblikk på å sikre at ulike tidsfrister i henhold til dette nummeret bokstav a) ii), alt etter hva som er relevant, kan gjenspeile særtrekk ved finanssektorene, uten at det berører opprettholdelsen av en konsekvent strategi for rapportering av IKT-relaterte hendelser i henhold til denne forordningen og direktiv (EU) 2022/2555. De europeiske tilsynsmyndighetene skal, dersom det er relevant, gi en begrunnelse dersom de avviker fra de metodene som er anvendt i forbindelse med det nevnte direktivet,

b) felles utkast til tekniske gjennomføringsstandarder for å fastsette standardskjemaer, standardmaler og standard framgangsmåter som de finansielle enhetene skal benytte for å rapportere en alvorlig IKT-relatert hendelse og for å underrette om en betydelig cybertrussel.

De europeiske tilsynsmyndighetene skal legge fram de felles utkastene til tekniske reguleringsstandarder som nevnt i første ledd bokstav a) og de felles utkastene til tekniske gjennomføringsstandarder som nevnt i første ledd bokstav b) for Kommisjonen innen 17. juli 2024.

Kommisjonen gis myndighet til å utfylle denne forordningen ved å vedta de felles tekniske reguleringsstandardene som er nevnt i første ledd bokstav a) i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Kommisjonen gis myndighet til å vedta de felles tekniske gjennomføringsstandardene som er nevnt i første ledd bokstav b), i samsvar med artikkel 15 i henholdsvis forordning (EU) nr. 1093/2010, forordning (EU) nr. 1094/2010 og forordning (EU) nr. 1095/2010.

Artikkel 21

Sentralisering av rapportering av alvorlige IKT-relaterte hendelser

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ESB og ENISA utarbeide en felles rapport som vurderer muligheten for ytterligere sentralisering av rapportering av hendelser gjennom opprettelse av et felles EU-knutepunkt for finansielle enheters rapportering av alvorlige IKT-relaterte hendelser. Den felles rapporten skal inneholde en undersøkelse av ulike måter for å lette strømmen av rapportering av IKT-relaterte hendelser, redusere tilknyttede kostnader og underbygge tematiske analyser med sikte på å øke den tilsynsmessige tilnærmingen.

2. Den felles rapporten nevnt i nr. 1 skal inneholde minst følgende:

a) Forutsetninger for opprettelse av et felles EU-knutepunkt.

b) Fordeler, begrensninger og risikoer, herunder risikoer forbundet med den høye konsentrasjonen av følsomme opplysninger.

c) Den nødvendige kapasiteten til å sikre interoperabilitet med hensyn til andre relevante rapporteringsordninger.

d) Elementer av den operasjonelle styringen.

e) Vilkår for medlemskap.

f) Tekniske ordninger for at finansielle enheter og nasjonale vedkommende myndigheter skal få tilgang til det felles EU-knutepunktet.

g) En foreløpig vurdering av finansielle kostnader som påløper ved opprettelse av den operasjonelle plattformen, som støtter det felles EU-knutepunktet, herunder den nødvendige ekspertisen.

3. De europeiske tilsynsmyndighetene skal legge fram rapporten nevnt i nr. 1 for Europaparlamentet, Rådet og Kommisjonen innen 17. januar 2025.

Artikkel 22

Tilbakemelding fra tilsynsmyndighetene

1. Uten at det berører de tekniske opplysningene, rådene eller tiltakene og den påfølgende oppfølgingen som CSIRT-enhetene, dersom det er relevant, i henhold til direktiv (EU) 2022/255 kan gi i samsvar med nasjonal rett, skal den vedkommende myndigheten, ved mottak av den første underretningen og hver rapport som nevnt i artikkel 19 nr. 4, bekrefte mottaket og, dersom det er mulig, innen rimelig tid gi relevant og forholdsmessig tilbakemelding eller veiledning på høyt nivå til den finansielle enheten, særlig ved å gjøre tilgjengelig alle relevante anonymiserte opplysninger og etterretninger om lignende trusler, og kan drøfte hvilke tiltak som har fått anvendelse på den finansielle enheten, og måter for å minimere og begrense de negative virkningene i finanssektoren. Uten at det berører tilbakemeldingen fra tilsynsmyndigheten, skal finansielle enheter fortsatt ha det fulle ansvaret for håndteringen og konsekvensene av IKT-relaterte hendelser som rapporteres i henhold til artikkel 19 nr. 1.

2. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen, i anonymisert og aggregert form, årlig rapportere om alvorlige IKT-relaterte hendelser, hvis nærmere opplysninger skal gis av vedkommende myndigheter i samsvar med artikkel 19 nr. 6, og som minst skal angi antallet av alvorlige IKT-relaterte hendelser, deres art og innvirkning på finansielle enheters eller kunders virksomhet, samt de utbedringstiltakene som er truffet, og kostnader som er påløpt.

De europeiske tilsynsmyndighetene skal utstede varsler og utarbeide statistikk på høyt nivå for å støtte vurderinger av IKT-trusler og IKT-sårbarhet.

Artikkel 23

Betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser knyttet til kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak

Kravene fastsatt i dette kapittelet får også anvendelse på betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser og på alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser når det gjelder kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak.

KAPITTEL IV

Testing av digital operasjonell motstandsdyktighet

Artikkel 24

Generelle krav til testing av digital operasjonell motstandsdyktighet

1. Med henblikk på å vurdere beredskapen til å håndtere IKT-relaterte hendelser, til å identifisere svakheter, mangler og hull i den digitale operasjonelle motstandsdyktigheten og til å gjennomføre korrigerende tiltak omgående, skal andre finansielle enheter enn svært små bedrifter, samtidig som det tas hensyn til kriteriene fastsatt i artikkel 4 nr. 2, utarbeide, opprettholde og gjennomgå et forsvarlig og omfattende program for testing av den digitale operasjonelle motstandsdyktigheten som en integrert del av rammeverket for IKT-risikostyring som nevnt i artikkel 6.

2. Programmet for testing av digital operasjonell motstandsdyktighet skal omfatte en rekke vurderinger, tester, metoder, framgangsmåter og verktøyer som skal anvendes i samsvar med artikkel 25 og 26.

3. Når andre finansielle enheter enn svært små bedrifter gjennomfører det programmet for testing av digitale operasjonell motstandsdyktighet som er nevnt i nr. 1 i denne artikkelen, skal de følge en risikobasert tilnærming som tar hensyn til kriteriene fastsatt i artikkel 4 nr. 2, samtidig som det tas behørig hensyn til IKT-risikoens utvikling, eventuelle spesifikke risikoer som den berørte finansielle enheten er eller kan bli eksponert for, informasjonsressursenes og tjenestenes kritiske verdi samt alle andre faktorer som den finansielle enheten anser som hensiktsmessige.

4. Andre finansielle enheter enn svært små bedrifter skal sikre at testene utføres av uavhengige parter, enten interne eller eksterne. Når testene utføres av en intern tester, skal finansielle enheter avsette tilstrekkelige ressurser og sikre at interessekonflikter unngås når testen utformes og gjennomføres.

5. Andre finansielle enheter enn svært små bedrifter skal fastsette framgangsmåter og retningslinjer for å prioritere, klassifisere og avhjelpe alle problemer som dukker opp under gjennomføringen av testene, og skal fastsette interne valideringsmetoder for å sikre at alle identifiserte svakheter, mangler eller hull avhjelpes fullt ut.

6. Andre finansielle enheter enn svært små bedrifter skal minst én gang i året sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner.

Artikkel 25

Testing av IKT-verktøyer og -systemer

1. Programmet for testing av digital operasjonell motstandsdyktighet nevnt i artikkel 24 skal, i samsvar med kriteriene fastsatt i artikkel 4 nr. 2, sikre gjennomføring av hensiktsmessige tester, som for eksempel sårbarhetsvurderinger og -analyser, analyser av åpen kildekode, vurderinger av nettsikkerhet, mangelanalyser, fysiske sikkerhetsvurderinger, spørreskjemaer og programvareløsninger for skanning, gjennomgåelse av kildekoder dersom det er mulig, scenariobaserte tester, kompatibilitetstesting, ytelsestesting, ende-til-ende-testing og penetrasjonstesting.

2. Verdipapirsentraler og sentrale motparter skal utføre sårbarhetsvurderinger før eventuell innføring eller gjeninnføring av nye eller eksisterende applikasjoner og infrastrukturkomponenter, og IKT-tjenester som støtter den finansielle enhetens kritiske eller viktige funksjoner.

3. Svært små bedrifter skal gjennomføre testene nevnt i nr. 1 ved å kombinere en risikobasert tilnærming med en strategisk planlegging av IKT-testing, samtidig som det tas behørig hensyn til behovet for å opprettholde en balansert tilnærming på den ene side mellom omfanget av ressursene og tiden som skal avsettes til IKT-testing som fastsatt i denne artikkelen, og på den annen side hastesituasjonen, risikotype og den kritiske verdien til informasjonsressursene og de leverte tjenestene, samt alle andre relevante faktorer, herunder den finansielle enhetens evne til å ta kalkulerte risikoer.

Artikkel 26

Avansert testing av IKT-verktøyer, -systemer og -prosesser basert på TLPT

1. Andre finansielle enheter enn enhetene som nevnt i artikkel 16 nr. 1 første ledd og svært små bedrifter, som er identifisert i samsvar med nr. 8 tredje ledd i denne artikkelen, skal minst hvert tredje år gjennomføre avansert testing ved hjelp av TLPT. På grunnlag av den finansielle enhetens risikoprofil og samtidig som det tas hensyn til de operasjonelle omstendighetene, kan den vedkommende myndigheten ved behov anmode den finansielle enheten om å redusere eller øke denne hyppigheten.

2. Hver trusselbasert penetrasjonstest skal omfatte flere eller alle kritiske eller viktige funksjoner hos en finansiell enhet, og skal utføres på produksjonssystemer som er i drift, og som støtter slike funksjoner.

De finansielle enhetene skal identifisere alle relevante underliggende IKT-systemer, -prosesser og -teknologier som støtter kritiske eller viktige funksjoner og IKT-tjenester, herunder dem som støtter kritiske eller viktige funksjoner som er blitt utkontraktert eller kontrahert til tredjepartsleverandører av IKT-tjenester.

De finansielle enhetene skal vurdere hvilke kritiske eller viktige funksjoner som må omfattes av TLPT. Resultatet av denne vurderingen skal bestemme det nøyaktige omfanget av TLPT og skal valideres av de vedkommende myndighetene.

3. Dersom tredjepartsleverandører av IKT-tjenester omfattes av TLPT, skal den finansielle enheten treffe nødvendige tiltak og sikkerhetstiltak for å sikre at slike tredjepartsleverandører av IKT-tjenester deltar i TLPT, og den skal til enhver tid ha det fulle ansvaret for å sikre at denne forordningen overholdes.

4. Med forbehold for nr. 2 første og andre ledd kan den finansielle enheten og en tredjepartsleverandør av IKT-tjenester, dersom tredjepartsleverandørens deltakelse i TLPT som nevnt i nr. 3 kan forventes å ha en negativ innvirkning på kvaliteten eller sikkerheten til de tjenestene som tredjepartsleverandøren av IKT-tjenester leverer til kunder som er enheter som ikke er omfattet av denne forordningen, eller på fortroligheten til dataene som er knyttet til slike tjenester, skriftlig avtale at tredjepartsleverandøren av IKT-tjenester inngår kontraktsregulerte ordninger direkte med en ekstern tester med henblikk på å gjennomføre, under ledelse av én utpekt finansiell enhet, en samlet TLPT som omfatter flere finansielle enheter (felles testing), som tredjepartsleverandøren av IKT-tjenester leverer IKT-tjenester til.

Den felles testingen skal omfatte det relevante spekteret av IKT-tjenester som støtter kritiske eller viktige funksjoner, som de finansielle enhetene har kontrahert til den aktuelle tredjepartsleverandøren av IKT-tjenester. Den felles testingen skal betraktes som en TLPT utført av de finansielle enhetene som deltar i den felles testingen.

Antallet av finansielle enheter som deltar i den felles testingen, skal være behørig avpasset, samtidig som det tas hensyn til de aktuelle tjenestenes kompleksitet og type.

5. De finansielle enhetene skal, i samarbeid med tredjepartsleverandører av IKT-tjenester og andre involverte parter, herunder testere, men med unntak av de vedkommende myndighetene, anvende effektive risikostyringskontroller for å redusere risikoen for potensiell innvirkning på data, skade på eiendeler og forstyrrelser av kritiske eller viktige funksjoner, tjenester eller transaksjoner hos den finansielle enheten selv, hos dens motparter eller i finanssektoren.

6. Når testingen er avsluttet, og etter at rapporter og utbedringsplaner er godkjent, skal den finansielle enheten og, dersom det er relevant, de eksterne testerne gi den myndigheten som er utpekt i samsvar med nr. 9 eller 10, et sammendrag av de relevante resultatene, utbedringsplanene og dokumentasjonen som viser at TLPT er blitt utført i samsvar med kravene.

7. Myndighetene skal gi de finansielle enhetene en erklæring som bekrefter at testen ble utført i samsvar med de kravene som framgår av dokumentasjonen, for å gi mulighet for gjensidig anerkjennelse av trusselbaserte penetrasjonstester mellom de vedkommende myndighetene. Den finansielle enheten skal underrette den berørte vedkommende myndigheten om erklæringen, sammendraget av de relevante resultatene og utbedringsplanene.

Uten at det berører en slik erklæring, skal de finansielle enhetene alltid ha det fulle ansvaret for virkningen av de testene som er nevnt i nr. 4.

8. De finansielle enhetene skal inngå en kontrakt med testere med henblikk på å utføre en TLPT i samsvar med artikkel 27. Dersom de finansielle enhetene bruker interne testere for å utføre en TLPT, skal de inngå kontrakt med eksterne testere ved hver tredje test.

Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, skal bare bruke eksterne testere i samsvar med artikkel 27 nr. 1 bokstav a)–e).

De vedkommende myndighetene skal identifisere de finansielle enhetene som er pålagt å utføre en TLPT, samtidig som det tas hensyn til kriteriene i artikkel 4 nr. 2, på grunnlag av en vurdering av følgende:

a) Påvirkningsfaktorer, særlig i hvilket omfang de tjenestene som ytes, og de aktivitetene som utføres av den finansielle enheten, påvirker finanssektoren.

b) Eventuelle problemer med den finansielle stabiliteten, herunder den finansielle enhetens systemiske karakter på unionsplan eller nasjonalt plan, alt etter hva som er relevant.

c) Den finansielle enhetens spesifikke IKT-risikoprofil, grad av IKT-modenhet eller tekniske funksjoner.

9. Medlemsstatene kan utpeke en felles offentlig myndighet i finanssektoren som ansvarlig for TLPT-relaterte spørsmål i finanssektoren på nasjonalt plan og overdra all myndighet og alle oppgaver med henblikk på dette.

10. Dersom det ikke er utpekt noen myndighet i samsvar med nr. 9 i denne artikkelen, og uten at det berører myndigheten til å identifisere de finansielle enhetene som er pålagt å utføre en TLPT, kan en vedkommende myndighet delegere utøvelsen av visse eller alle de oppgavene som er nevnt i denne artikkelen og i artikkel 27, til en annen nasjonal myndighet i finanssektoren.

11. De europeiske tilsynsmyndighetene skal, etter avtale med ESB, utarbeide felles utkast til tekniske reguleringsstandarder i samsvar med TIBER-EU-rammeverket for å spesifisere nærmere

a) de kriteriene som brukes ved anvendelse av nr. 8 andre ledd,

b) kravene og standardene for anvendelse av interne testere,

c) kravene i forbindelse med

   i) omfanget av den TLPT-en som nevnt i nr. 2,

   ii) den testmetoden og den tilnærmingen som skal følges i hver enkelt fase av testingen,

   iii) resultatene av testingen og avslutnings- og utbedringsfaser,

d) den typen av tilsynssamarbeid og annet relevant samarbeid som er nødvendig for gjennomføring av TLPT, og for å lette gjensidig anerkjennelse av en slik testing når det gjelder finansielle enheter som driver virksomhet i mer enn én medlemsstat, slik at det sikres et passende nivå av tilsynsmessig deltakelse og en fleksibel gjennomføring for å ta hensyn til særtrekk ved finansielle delsektorer eller lokale finansmarkeder.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta behørig hensyn til eventuelle særtrekk som oppstår som følge av den særskilte arten av aktiviteter i ulike sektorer for finansielle tjenester.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 27

Krav til testere ved utførelse av TLPT

1. De finansielle enhetene skal bare bruke testere for å utføre en TLPT som

a) er de mest egnede, og som har det beste omdømmet,

b) har teknisk og organisatorisk kapasitet samt spesifikk ekspertise med hensyn til trusseletterretning, penetrasjonstesting og red team-testing,

c) er sertifisert av et akkrediteringsorgan i en medlemsstat eller overholder formelle atferdsnormer eller etiske rammer,

d) avgir en uavhengig forsikring eller en revisjonsberetning i forbindelse med forsvarlig risikostyring i forbindelse med utførelse av TLPT, herunder behørig beskyttelse av den finansielle enhetens fortrolige opplysninger og erstatning for den finansielle enhetens operasjonelle risikoer,

e) er behørig og fullt ut dekket av relevante yrkesansvarsforsikringer, herunder mot risiko for forsømmelse og uaktsomhet.

2. Når de finansielle enhetene bruker interne testere, skal de i tillegg til kravene i nr. 1, sikre at følgende vilkår er oppfylt:

a) En slik bruk er godkjent av den berørte vedkommende myndigheten eller av den felles offentlige myndigheten som er utpekt i samsvar med artikkel 26 nr. 9 og 10.

b) Den berørte vedkommende myndigheten har verifisert at den finansielle enheten har avsatt tilstrekkelig med ressurser og sikret at interessekonflikter unngås når testen utformes og gjennomføres.

c) Formidleren av trusseletterretninger er ikke en del av den finansielle enheten.

3. De finansielle enhetene skal sikre at kontrakter inngått med eksterne testere krever en forsvarlig forvaltning av resultatene av TLPT, og at enhver databehandling av disse, herunder enhver form for generering, lagring, aggregering, utkast, rapport, kommunikasjon eller destruksjon, ikke medfører risiko for den finansielle enheten.

KAPITTEL V

Styring av IKT-tredjepartsrisiko

Avsnitt I

Sentrale prinsipper for en forsvarlig styring av IKT-tredjepartsrisiko

Artikkel 28

Generelle prinsipper

1. De finansielle enhetene skal styre IKT-tredjepartsrisiko som en integrert del av IKT-risiko innenfor sitt rammeverk for IKT-risikostyring som nevnt i artikkel 6 nr. 1, og i samsvar med følgende prinsipper:

a) De finansielle enhetene som har inngått kontraktsregulerte ordninger om bruk av IKT-tjenester for å drive sin virksomhet, skal til enhver tid ha det fulle ansvaret for å overholde og oppfylle alle forpliktelser i henhold til denne forordningen og gjeldende regelverk for finansielle tjenester.

b) De finansielle enhetenes styring av IKT-tredjepartsrisiko skal gjennomføres med hensyn til forholdsmessighetsprinsippet, samtidig som det tas hensyn til

i) karakteren, omfanget, kompleksiteten og betydningen av IKT-relatert avhengighet,

ii) de risikoene som oppstår som følge av kontraktsregulerte ordninger om bruk av IKT-tjenester som er inngått med tredjepartsleverandører av IKT-tjenester, samtidig som det tas hensyn til den kritiske verdien eller betydningen av den aktuelle tjenesten, prosessen eller funksjonen, og den potensielle innvirkningen på kontinuiteten og tilgjengeligheten til finansielle tjenester og aktiviteter, på individuelt nivå og på konsernnivå.

2. Som en del av sitt rammeverk for IKT-risikostyring skal andre finansielle enheter enn de enhetene som er nevnt i artikkel 16 nr. 1 første ledd, og svært små bedrifter, vedta og regelmessig gjennomgå en strategi for IKT-tredjepartsrisiko, samtidig som det tas hensyn til strategien med flere ulike leverandører som nevnt i artikkel 6 nr. 9, dersom det er relevant. Strategien for IKT-tredjepartsrisiko skal omfatte retningslinjer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner levert av tredjepartsleverandører av IKT-tjenester, og skal gjelde på individuelt grunnlag og, dersom det er relevant, på delkonsolidert og konsolidert grunnlag. Ledelsesorganet skal, på grunnlag av en vurdering av den finansielle enhetens generelle risikoprofil og omfanget og kompleksiteten av forretningstjenestene, regelmessig gjennomgå de risikoene som er identifisert med hensyn til kontraktsregulerte ordninger om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner.

3. Som en del av sitt rammeverk for IKT-risikostyring skal de finansielle enhetene opprettholde og oppdatere et register over opplysninger på enhetsnivå, delkonsolidert nivå og konsolidert nivå om alle kontraktsregulerte ordninger om bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester.

De kontraktsregulerte ordningene nevnt i første ledd skal være behørig dokumentert, og det skal skjelnes mellom dem som omfatter IKT-tjenester som støtter kritiske eller viktige funksjoner, og dem som ikke gjør det.

De finansielle enhetene skal minst én gang i året rapportere til de vedkommende myndighetene om antall nye ordninger om bruk av IKT-tjenester, kategoriene av tredjepartsleverandører av IKT-tjenester, typen av kontraktsregulerte ordninger og de IKT-tjenestene og -funksjonene som leveres.

De finansielle enhetene skal på anmodning gi den vedkommende myndigheten tilgang til det fullstendige registeret over opplysninger eller angitte deler av det, sammen med alle opplysninger som anses som nødvendige for et effektivt tilsyn med den finansielle enheten.

De finansielle enhetene skal i god tid underrette den vedkommende myndigheten om enhver planlagt kontraktsregulert ordning om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, samt når en funksjon er blitt kritisk eller viktig.

4. Før de finansielle enhetene inngår en kontraktsregulert ordning om bruk av IKT-tjenester, skal de

a) vurdere om den kontraktsregulerte ordningen omfatter bruken av IKT-tjenester som støtter en kritisk eller viktig funksjon,

b) vurdere om tilsynsvilkårene for utkontraktering er oppfylt,

c) identifisere og vurdere alle relevante risikoer i forbindelse med den kontraktsregulerte ordningen, herunder muligheten for at en slik kontraktsregulert ordning kan bidra til å styrke IKT-konsentrasjonsrisikoen som nevnt i artikkel 29,

d) foreta en aktsomhetsvurdering av potensielle tredjepartsleverandører av IKT-tjenester og under alle utvelgelses- og vurderingsprosessene sikre at tredjepartsleverandøren av IKT-tjenester er egnet,

e) identifisere og vurdere interessekonflikter som den kontraktsregulerte ordningen kan forårsake.

5. De finansielle enhetene kan bare inngå kontraktsregulerte ordninger med tredjepartsleverandører av IKT-tjenester som overholder egnede standarder om informasjonssikkerhet. Når slike kontraktsregulerte ordninger gjelder kritiske eller viktige funksjoner, skal finansielle enheter, før de inngår ordningene, ta behørig hensyn til hvorvidt tredjepartsleverandører av IKT-tjenester bruker de nyeste standardene om informasjonssikkerhet av høyeste kvalitet.

6. Når finansielle enheter utøver retten til tilgang, inspeksjon og revisjon overfor tredjepartsleverandøren av IKT-tjenester, skal de på grunnlag av en risikobasert tilnærming på forhånd fastsette hyppigheten av revisjoner og inspeksjoner samt de områdene som skal revideres, gjennom å følge allment anerkjente revisjonsstandarder i tråd med eventuelle tilsynsinstrukser om bruk og innarbeiding av slike revisjonsstandarder.

Dersom kontraktsregulerte ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester medfører høy teknisk kompleksitet, skal den finansielle enheten kontrollere at revisorer, enten interne eller eksterne, eller et utvalg av revisorer, besitter de nødvendige ferdighetene og den nødvendige kunnskapen for å kunne utføre de relevante revisjonene og vurderingene på en effektiv måte.

7. De finansielle enhetene skal sikre at kontraktsregulerte ordninger om bruk av IKT-tjenester kan sies opp i alle følgende situasjoner:

a) tredjepartsleverandøren av IKT-tjenester begår en vesentlig overtredelse av gjeldende lover, forskrifter eller kontraktsvilkår.

b) Forhold som er avdekket under overvåkingen av IKT-tredjepartsrisiko, og som anses for å kunne endre ytelsen til de funksjonene som tilbys gjennom den kontraktsregulerte ordningen, herunder vesentlige endringer som påvirker ordningen eller situasjonen for tredjepartsleverandøren av IKT-tjenester.

c) tredjepartsleverandøren av IKT-tjenester har vist svakheter når det gjelder sin samlede IKT-risikostyring, og særlig hvordan den sikrer tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, enten det dreier seg om personopplysninger eller på annen måte sensitive opplysninger eller andre opplysninger enn personopplysninger.

d) Dersom den vedkommende myndigheten ikke lenger kan føre effektivt tilsyn med den finansielle enheten som følge av vilkårene i eller omstendighetene knyttet til respektive kontraktsregulerte ordninger.

8. For IKT-tjenester som støtter kritiske eller viktige funksjoner, skal finansielle enheter innføre exit-strategier. Exit-strategiene skal ta hensyn til risikoer som kan oppstå hos tredjepartsleverandører av IKT-tjenester, særlig en mulig svikt fra deres side, en forringelse av kvaliteten på de IKT-tjenestene som leveres, eventuelle driftsforstyrrelser på grunn av upassende eller mislykket levering av IKT-tjenester eller eventuelle vesentlige risikoer som oppstår i forbindelse med en hensiktsmessig og kontinuerlig anvendelse av den aktuelle IKT-tjenesten, eller oppsigelse av kontraktsregulerte ordninger med tredjepartsleverandører av IKT-tjenester i en av de situasjonene som er nevnt i nr. 7.

De finansielle enhetene skal sikre at de kan si opp kontraktsregulerte ordninger uten

a) at deres forretningsvirksomhet avbrytes,

b) at overholdelsen av de forskriftsmessige kravene begrenses,

c) at kontinuiteten og kvaliteten på de tjenestene som leveres til kunder, lider skade.

Exit-planene skal være omfattende og dokumenterte, og de skal, i samsvar med kriteriene fastsatt i artikkel 4 nr. 2, være tilstrekkelig testet samt være gjennomgått regelmessig.

De finansielle enhetene skal identifisere alternative løsninger og utarbeide overgangsplaner slik at de kan frata tredjepartsleverandøren av IKT-tjenester de kontraherte IKT-tjenestene og de relevante dataene, og på en sikker og fullstendig måte overføre dem til alternative leverandører eller reintegrere dem internt.

De finansielle enhetene skal innføre egnede beredskapstiltak for å opprettholde kontinuitet i virksomheten dersom omstendighetene nevnt i første ledd inntreffer.

9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske gjennomføringsstandarder for å fastsette standardmaler for det registeret over opplysninger som er nevnt i nr. 3, herunder opplysninger som er felles for alle kontraktsregulerte ordninger om bruk av IKT-tjenester. De europeiske tilsynsmyndighetene skal framlegge disse utkastene til tekniske gjennomføringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen gis myndighet til å vedta de tekniske gjennomføringsstandardene som er nevnt i første ledd, i samsvar med artikkel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

10. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske reguleringsstandarder for nærmere å angi det detaljerte innholdet i retningslinjene nevnt i nr. 2 i forbindelse med de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner som leveres av tredjepartsleverandører av IKT-tjenester.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift. De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 29

Foreløpig vurdering av IKT-konsentrasjonsrisiko på enhetsnivå

1. Når finansielle enheter foretar identifisering og vurdering av risikoene nevnt i artikkel 28 nr. 4 bokstav c), skal de også ta hensyn til om den planlagte inngåelsen av en kontraktsregulert ordning i forbindelse med IKT-tjenester som støtter kritiske eller viktige funksjoner, vil føre til noe av følgende:

a) Kontrakt med en tredjepartsleverandør av IKT-tjenester som ikke er lett å erstatte.

b) Inngåelse av flere kontraktsregulerte ordninger for levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, med den samme tredjepartsleverandøren av IKT-tjenester eller med tredjepartsleverandører av IKT-tjenester som har tette forbindelser til denne.

De finansielle enhetene skal vurdere fordelene og kostnadene ved alternative løsninger, som for eksempel bruken av ulike tredjepartsleverandører av IKT-tjenester, samtidig som det tas hensyn til om og hvordan planlagte løsninger svarer til de forretningsmessige behovene og målene som er fastsatt i deres strategi for digital motstandsdyktighet.

2. Dersom de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, omfatter muligheten for at en tredjepartsleverandør av IKT-tjenester gir IKT-tjenester som støtter en kritisk eller viktig funksjon, i underentreprise til andre tredjepartsleverandører av IKT-tjenester, skal de finansielle enhetene vurdere fordeler og risiko som kan oppstå i forbindelse med en slik underentreprise, særlig når det gjelder en IKT-underleverandør som er etablert i et tredjeland.

Dersom kontraktsregulerte ordninger gjelder IKT-tjenester som støtter kritiske eller viktige funksjoner, skal de finansielle enhetene ta behørig hensyn til de bestemmelsene i insolvensretten som får anvendelse dersom tredjepartsleverandøren av IKT-tjenester går konkurs, samt eventuelle begrensninger som kan oppstå i forbindelse med den presserende gjenopprettingen av den finansielle enhetens data.

Dersom det inngås kontraktsregulerte ordninger om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, med en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, skal de finansielle enhetene, i tillegg til de forholdene som er nevnt i andre ledd, også vurdere overholdelsen av Unionens personvernregler og den faktiske overholdelsen av retten i dette tredjelandet

Dersom de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, omfatter underentreprise, skal de finansielle enhetene vurdere om og hvordan potensielt lange eller komplekse kjeder av underentrepriser kan påvirke deres evne til fullt ut å overvåke de kontraherte funksjonene og den vedkommende myndighetens evne til å føre effektivt tilsyn med den finansielle enheten i denne forbindelse.

Artikkel 30

Viktige kontraktsbestemmelser

1. Rettighetene og forpliktelsene for den finansielle enheten og tredjepartsleverandøren av IKT-tjenester skal være klart fordelt og fastsatt skriftlig. Den fullstendige kontrakten skal omfatte tjenestenivåavtaler og dokumenteres i ett skriftlig dokument som partene skal ha tilgang til på papir, eller i et dokument i et annet nedlastbart, varig og tilgjengelig format.

2. De kontraktsregulerte ordningene om bruk av IKT-tjenester skal inneholde minst følgende elementer:

a) En klar og fullstendig beskrivelse av alle funksjoner og IKT-tjenester som skal leveres av tredjepartsleverandøren av IKT-tjenester, med angivelse av om underentreprise av en IKT-tjeneste som støtter en kritisk eller viktig funksjon, eller vesentlige deler av denne, er tillatt, og, dersom dette er tilfellet, de vilkårene som gjelder for en slik underentreprise.

b) De stedene, nærmere bestemt regioner eller land, der de funksjonene eller IKT-tjenestene som er kontrahert eller gitt i underentreprise, skal leveres, og der dataene skal behandles, herunder lagringsstedet, og kravet til tredjepartsleverandøren av IKT-tjenester om å underrette den finansielle enheten på forhånd dersom den planlegger å endre disse stedene.

c) Bestemmelser om tilgjengelighet, autentisitet, integritet og fortrolighet i forbindelse med vern av data, herunder personopplysninger.

d) Bestemmelser om å sikre tilgang, gjenoppretting og tilbakeføring i et lett tilgjengelig format av personopplysninger og andre opplysninger enn personopplysninger, som behandles av den finansielle enheten ved insolvens, krisehåndtering eller opphør av virksomheten til tredjepartsleverandøren av IKT-tjenester, eller ved oppsigelse av kontraktsregulerte ordninger.

e) En beskrivelse av tjenestenivåer, herunder oppdateringer og revideringer av disse.

f) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å yte bistand til den finansielle enheten uten ekstra kostnad, eller til en kostnad som fastsettes på forhånd, dersom det oppstår en IKT-hendelse som er knyttet til den IKT-tjenesten som leveres til den finansielle enheten.

g) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å samarbeide fullt ut med den finansielle enhetens vedkommende myndigheter og krisehåndteringsmyndigheter, herunder personer som de har utpekt.

h) Oppsigelsesrett og tilhørende minste oppsigelsesfrist for oppsigelse av de kontraktsregulerte ordningene i samsvar med forventningene til vedkommende myndigheter og krisehåndteringsmyndigheter.

i) Vilkårene for deltakelse av tredjepartsleverandører av IKT-tjenester i de finansielle enhetenes bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet i samsvar med artikkel 13 nr. 6.

3. De kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, skal i tillegg til elementene nevnt i nr. 2 minst omfatte følgende:

a) En fullstendig beskrivelse av tjenestenivåer, herunder oppdateringer og revideringer av disse med nøyaktige kvantitative og kvalitative ytelsesmål innenfor de avtalte tjenestenivåene, slik at den finansielle enheten kan overvåke IKT-tjenester på en effektiv måte og gjøre det mulig å iverksette egnede korrigerende tiltak uten unødig forsinkelse når de avtalte tjenestenivåene ikke oppnås.

b) Oppsigelsesfrister og rapporteringsforpliktelser for tredjepartsleverandøren av IKT-tjenester overfor den finansielle enheten, herunder underretning om enhver utvikling som kan ha en vesentlig innvirkning på hvorvidt tredjepartsleverandøren av IKT-tjenester har evnen til å levere IKT-tjenester som støtter kritiske eller viktige funksjoner, på en effektiv måte og i tråd med avtalte tjenestenivåer.

c) Krav til tredjepartsleverandøren av IKT-tjenester om å gjennomføre og teste beredskapsplaner for virksomheten og innføre IKT-sikkerhetstiltak, IKT-verktøyer og IKT-retningslinjer som gir et hensiktsmessig sikkerhetsnivå for den finansielle enhetens levering av tjenester i tråd med dens regelverk.

d) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å delta i og fullt ut samarbeide om den finansielle enhetens TLPT som nevnt i artikkel 26 og 27.

e) Retten til fortløpende å overvåke det ytelsesnivået som tredjepartsleverandøren av IKT-tjenester leverer, hvilket innebærer følgende:

i) Ubegrenset rett til tilgang, inspeksjon og revisjon for den finansielle enheten, eller en utpekt tredjepart, og for den vedkommende myndigheten, og retten til å ta kopier av relevant dokumentasjon på stedet dersom de er av avgjørende betydning for virksomheten hos tredjepartsleverandøren av IKT-tjenester, hvis faktiske utøvelse ikke hindres eller begrenses av andre kontraktsregulerte ordninger eller gjennomføringsstrategier.

ii) Retten til å komme til enighet om alternative sikkerhetsnivåer dersom andre kunders rettigheter påvirkes.

iii) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å samarbeide fullt ut under de stedlige inspeksjonene og revisjonene som utføres av de vedkommende myndighetene, hovedovervåkeren, den finansielle enheten eller en utpekt tredjepart.

iv) Forpliktelsen om å gi nærmere opplysninger om omfanget, de framgangsmåtene som skal følges, og hyppigheten av slike inspeksjoner og revisjoner.

f) Exit-strategier, særlig innføring av en obligatorisk passende overgangsperiode,

i) under hvilken tredjepartsleverandøren av IKT-tjenester kommer til å fortsette å levere de respektive funksjonene eller IKT-tjenestene med sikte på å redusere risikoen for forstyrrelser hos den finansielle enheten eller for å sikre en effektiv krisehåndtering og omstrukturering av denne,

ii) slik at den finansielle enheten kan bytte til en annen tredjepartsleverandør av IKT-tjenester eller bytte til interne løsninger som er forenlige med den leverte tjenestens kompleksitet.

Som unntak fra bokstav e) kan tredjepartsleverandøren av IKT-tjenester og den finansielle enheten som er en svært liten bedrift, bli enige om at den finansielle enhetens rett til tilgang, inspeksjon og revisjon kan delegeres til en uavhengig tredjepart som utpekes av tredjepartsleverandøren av IKT-tjenester, og at den finansielle enheten når som helst kan anmode tredjeparten om opplysninger og garantier i forbindelse med de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår.

4. Når finansielle enheter og tredjepartsleverandører av IKT-tjenester forhandler om kontraktsregulerte ordninger, skal de vurdere å bruke standardavtalevilkår utarbeidet av offentlige myndigheter for bestemte tjenester.

5. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske reguleringsstandarder for å spesifisere nærmere de elementene som er nevnt i nr. 2 bokstav a), og som en finansiell enhet må fastsette og vurdere når den gir IKT-tjenester som støtter kritiske eller viktige funksjoner, i underentreprise.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Avsnitt II

Tilsynsramme for kritiske tredjepartsleverandører av IKT-tjenester

Artikkel 31

Utpeking av kritiske tredjepartsleverandører av IKT-tjenester

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og på anmodning fra overvåkingsforumet nedsatt i henhold til artikkel 32 nr. 1

a) utpeke tredjepartsleverandører av IKT-tjenester som er kritiske for finansielle enheter, etter en vurdering som tar hensyn til kriteriene angitt i nr. 2,

b) oppnevne som hovedovervåker for hver kritisk tredjepartsleverandør av IKT-tjenester den europeiske tilsynsmyndigheten som er ansvarlig i samsvar med forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 eller (EU) nr. 1095/2010, for de finansielle enhetene som til sammen har den største andelen av de samlede eiendelene av verdien av de samlede eiendelene for alle de finansielle enhetene som benytter seg av tjenestene fra den relevante kritiske tredjepartsleverandøren av IKT-tjenester, slik det framgår av summen av de individuelle balansene for disse finansielle enhetene.

2. Den utpekingen som er nevnt i nr. 1 bokstav a), skal i forbindelse med IKT-tjenester levert av tredjepartsleverandøren av IKT-tjenester baseres på alle følgende kriterier:

a) Den systemiske virkningen på stabiliteten, kontinuiteten eller kvaliteten på leveringen av finansielle tjenester dersom den berørte tredjepartsleverandøren av IKT-tjenester skulle rammes av omfattende driftsforstyrrelser, slik at denne ikke kan levere sine tjenester, samtidig som det tas hensyn til antallet av finansielle enheter og den samlede verdien av eiendeler hos de finansielle enhetene som den berørte tredjepartsleverandøren av IKT-tjenester leverer tjenester til.

b) Den systemiske karakteren eller betydningen av de finansielle enhetene som er avhengige av den berørte tredjepartsleverandøren av IKT-tjenester, vurdert i samsvar med følgende parametrer:

   i) Antallet av globalt systemviktige institusjoner eller andre systemviktige institusjoner som er avhengige av den aktuelle tredjepartsleverandøren av IKT-tjenester.

   ii) Den gjensidige avhengigheten mellom de globalt systemviktige institusjonene eller de andre systemviktige institusjonene nevnt i punkt i) og andre finansielle enheter, herunder situasjoner der de globalt systemviktige institusjonene eller de andre systemviktige institusjonene leverer finansielle infrastrukturtjenester til andre finansielle enheter.

c) Finansielle enheters avhengighet av tjenestene som leveres av den berørte tredjepartsleverandøren av IKT-tjenester i forbindelse med kritiske eller viktige funksjoner hos finansielle enheter som i siste instans involverer den samme tredjepartsleverandøren av IKT-tjenester, uavhengig av om finansielle enheter er avhengige av disse tjenestene direkte eller indirekte, gjennom underleverandøravtaler.

d) Graden av erstattbarhet hos tredjepartsleverandøren av IKT-tjenester, samtidig som det tas hensyn til følgende parametrer:

   i) Mangelen på reelle alternativer, også delvis, på grunn av det begrensede antallet av tredjepartsleverandører av IKT-tjenester som er aktive på et bestemt marked, eller markedsandelen for den berørte tredjepartsleverandøren av IKT-tjenester, eller den tekniske kompleksiteten eller den avanserte karakteren, herunder i forbindelse med eventuell proprietær teknologi, eller særtrekkene ved organisasjonen eller virksomheten til tredjepartsleverandøren av IKT-tjenester.

   ii) Vanskeligheter i forbindelse med delvis eller fullstendig overføring av relevante data og arbeidsbelastninger fra den berørte tredjepartsleverandøren av IKT-tjenester til en annen tredjepartsleverandør av IKT-tjenester, enten på grunn av betydelige finansielle kostnader, tid eller andre ressurser som overføringsprosessen kan medføre, eller på grunn av økt IKT-risiko eller andre operasjonelle risikoer som den finansielle enheten kan bli eksponert for gjennom en slik overføring.

3. Dersom tredjepartsleverandøren av IKT-tjenester inngår i et konsern, skal kriteriene nevnt i nr. 2 vurderes med hensyn til de IKT-tjenestene som leveres av konsernet som helhet.

4. Kritiske tredjepartsleverandører av IKT-tjenester som er en del av et konsern, skal utpeke en juridisk person som koordineringspunkt for å sikre tilstrekkelig representasjon og kommunikasjon med hovedovervåkeren.

5. Hovedovervåkeren skal underrette tredjepartsleverandøren av IKT-tjenester om resultatet av vurderingen som fører til utpekingen nevnt i nr. 1 bokstav a). Innen 6 uker fra datoen for underretningen kan tredjepartsleverandøren av IKT-tjenester sende en begrunnet uttalelse til hovedovervåkeren med alle relevante opplysninger med henblikk på vurderingen. Hovedovervåkeren skal vurdere den begrunnede uttalelsen og kan be om ytterligere opplysninger som skal legges fram innen 30 kalenderdager etter mottak av en slik uttalelse.

Etter å ha utpekt en tredjepartsleverandør av IKT-tjenester som kritisk skal de europeiske tilsynsmyndighetene gjennom Felleskomiteen underrette tredjepartsleverandøren av IKT-tjenester om en slik utpeking og om startdatoen for når den faktisk vil være omfattet av tilsynsvirksomhet. Denne startdatoen skal ikke være senere enn én måned etter underretningen. tredjepartsleverandøren av IKT-tjenester skal underrette de finansielle enhetene som den leverer tjenester til, om at den er utpekt som kritisk.

6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 57 for å utfylle denne forordningen ved å spesifisere nærmere kriteriene i nr. 2 i denne artikkelen innen 17. juni 2024.

7. Den utpekingen som er nevnt i nr. 1 bokstav a), får ikke anvendelse før Kommisjonen har vedtatt en delegert rettsakt i samsvar med nr. 6.

8. Utpekingen nevnt i nr. 1 bokstav a) får ikke anvendelse på følgende:

i) Finansielle enheter som leverer IKT-tjenester til andre finansielle enheter.

ii) tredjepartsleverandører av IKT-tjenester som er underlagt tilsynsrammer etablert for å støtte oppgavene nevnt i artikkel 127 nr. 2 i traktaten om Den europeiske unions virkemåte.

iii) Konserninterne leverandører av IKT-tjenester.

iv) tredjepartsleverandører av IKT-tjenester som utelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheter som bare er aktive i den aktuelle medlemsstaten.

9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen opprette, offentliggjøre og oppdatere årlig listen over kritiske tredjepartsleverandører av IKT-tjenester på unionsplan.

10. Ved anvendelse av nr. 1 bokstav a) skal vedkommende myndigheter årlig og i aggregert form oversende de rapportene som er nevnt i artikkel 28 nr. 3 tredje ledd, til det overvåkingsforumet som er opprettet i henhold til artikkel 32. Overvåkingsforumet skal vurdere finansielle enheters avhengighet av tredjepartsleverandører av IKT-tjenester på grunnlag av opplysninger som det mottar fra de vedkommende myndighetene.

11. Tredjepartsleverandører av IKT-tjenester som ikke er oppført på listen nevnt i nr. 9, kan anmode om å bli utpekt som kritiske i samsvar med nr. 1 bokstav a).

Med henblikk på første ledd skal tredjepartsleverandøren av IKT-tjenester inngi en begrunnet søknad til EBA, ESMA eller EIOPA, som gjennom Felleskomiteen skal beslutte om denne tredjepartsleverandøren av IKT-tjenester skal utpekes som kritisk i samsvar med nr. 1 bokstav a).

Beslutningen nevnt i andre ledd skal vedtas og meddeles tredjepartsleverandøren av IKT-tjenester innen seks måneder etter mottak av søknaden.

12. Finansielle enheter skal bare benytte seg av tjenestene til en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med nr. 1 bokstav a), dersom sistnevnte har etablert et datterforetak i Unionen innen tolv måneder etter utpekingen.

13. Den kritiske tredjepartsleverandøren av IKT-tjenester nevnt i nr. 12 skal underrette hovedovervåkeren om eventuelle endringer i ledelsesstrukturen i det datterforetaket som er etablert i Unionen.

Artikkel 32

Overvåkingsrammeverkets struktur

1. Felleskomiteen skal i samsvar med artikkel 57 nr. 1 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 opprette overvåkingsforumet som en underkomité med henblikk på å støtte arbeidet som utføres i Felleskomiteen og av hovedovervåkeren nevnt i artikkel 31 nr. 1 bokstav b), på området for IKT-tredjepartsrisiko i alle finanssektorer. Overvåkingsforumet skal utarbeide utkast til felles holdninger og utkast til felles rettsakter for Felleskomiteen på dette området.

Overvåkingsforumet skal regelmessig drøfte relevante utviklingstrekk med hensyn til IKT-risiko og -sårbarheter og fremme en konsekvent strategi for overvåking av IKT-tredjepartsrisiko på unionsplan.

2. Overvåkingsforumet skal hvert år foreta en samlet vurdering av resultatene og konklusjonene av den overvåkingsvirksomheten som utføres for alle kritiske tredjepartsleverandører av IKT-tjenester, og fremme koordineringstiltak for å øke finansielle enheters digitale operasjonelle motstandsdyktighet, fremme beste praksis for å håndtere IKT-konsentrasjonsrisiko og undersøke risikoreduserende tiltak for sektorovergripende risikooverføring.

3. Overvåkingsforumet skal legge fram omfattende referanseverdier for kritiske tredjepartsleverandører av IKT-tjenester som Felleskomiteen skal vedta som de europeiske tilsynsmyndighetenes felles holdninger i samsvar med artikkel 56 nr. 1 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. Overvåkingsforumet skal bestå av følgende:

a) Lederne for de europeiske tilsynsmyndighetene.

b) Én representant på høyt nivå for det nåværende personalet i den berørte vedkommende myndigheten som nevnt i artikkel 46 fra hver medlemsstat.

c) De administrerende direktørene for hver europeisk tilsynsmyndighet og én representant fra Kommisjonen, ESRB, ESB og ENISA som observatører.

d) Dersom det er relevant, én ytterligere representant for en vedkommende myndighet som nevnt i artikkel 46 fra hver medlemsstat som observatør.

e) Dersom det er relevant, én representant for de vedkommende myndighetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, og som er ansvarlig for tilsynet med en vesentlig eller viktig enhet som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester, som observatør.

Overvåkingsforumet kan, dersom det er relevant, rådføre seg med uavhengige eksperter som er utpekt i samsvar med nr. 6.

5. Hver medlemsstat skal utpeke den berørte vedkommende myndigheten hvis ansatte skal være den representanten på høyt nivå som er nevnt i nr. 4 første ledd bokstav b), og skal underrette hovedovervåkeren om dette.

De europeiske tilsynsmyndighetene skal offentliggjøre på sitt nettsted listen over representanter på høyt nivå fra det nåværende personalet i den berørte vedkommende myndigheten som er utpekt av medlemsstatene.

6. De uavhengige ekspertene nevnt i nr. 4 andre ledd skal utpekes av overvåkingsforumet fra en gruppe av eksperter som velges ut etter en offentlig og gjennomsiktig søknadsprosess.

De uavhengige ekspertene skal utpekes på grunnlag av sin ekspertise om finansiell stabilitet, digital operasjonell motstandsdyktighet og IKT-sikkerhet. De skal opptre uavhengig og upartisk og utelukkende i hele Unionens interesse, og skal ikke be om eller motta instrukser fra Unionens institusjoner eller organer, medlemsstaters regjeringer eller annet offentlig eller privat organ.

7. I samsvar med artikkel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 skal de europeiske tilsynsmyndighetene innen 17. juli 2024 med henblikk på dette avsnittet utstede retningslinjer for samarbeidet mellom de europeiske tilsynsmyndighetene og de vedkommende myndighetene om de nærmere framgangsmåtene og vilkårene for tildeling og utførelse av oppgaver mellom de vedkommende myndighetene og de europeiske tilsynsmyndighetene, og de nærmere opplysningene om den utvekslingen av opplysninger som er nødvendig for at de vedkommende myndighetene skal kunne sikre oppfølgingen av de anbefalingene som er rettet til kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 35 nr. 1 bokstav d).

8. De kravene som er fastsatt i dette avsnittet berører ikke anvendelsen av direktiv (EU) 2022/2555 og andre unionsregler om tilsyn som gjelder for leverandører av skytjenester.

9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og på grunnlag av overvåkingsforumets forberedende arbeid årlig legge fram en rapport om anvendelsen av dette avsnittet for Europaparlamentet, Rådet og Kommisjonen.

Artikkel 33

Hovedovervåkerens oppgaver

1. Hovedovervåkeren, som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b), skal overvåke de tildelte kritiske tredjepartsleverandørene av IKT-tjenester og skal i forbindelse med alle forhold knyttet til overvåkingen være det primære kontaktpunktet for disse kritiske tredjepartsleverandørene av IKT-tjenester.

2. Ved anvendelse av nr. 1 skal hovedovervåkeren vurdere om hver kritisk tredjepartsleverandør av IKT-tjenester har innført omfattende, forsvarlige og effektive regler, framgangsmåter, mekanismer og ordninger for å styre den IKT-risikoen som den kan utsette finansielle enheter for.

Den vurderingen som er nevnt i første ledd, skal hovedsakelig fokusere på IKT-tjenester som leveres av den kritiske tredjepartsleverandøren av IKT-tjenester, og som støtter finansielle enheters kritiske eller viktige funksjoner. Dersom det er nødvendig for å håndtere alle relevante risikoer, skal denne vurderingen omfatte IKT-tjenester som støtter andre funksjoner enn dem som er kritiske eller viktige.

3. Vurderingen nevnt i nr. 2 skal omfatte følgende:

a) IKT-krav som særlig skal sikre sikkerheten, tilgjengeligheten, kontinuiteten, skalerbarheten og kvaliteten på tjenestene som den kritiske tredjepartsleverandøren av IKT-tjenester leverer til finansielle enheter, samt evnen til alltid å opprettholde høye standarder for tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene.

b) Den fysiske sikkerheten som bidrar til å sikre IKT-sikkerheten, herunder sikkerheten i lokaler, på anlegg og i datasentre.

c) Risikostyringsprosessene, herunder retningslinjer for IKT-risikostyring, IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting.

d) Styringsordninger, herunder en organisasjonsstruktur med klare, gjennomsiktige og konsekvente regler om ansvar og ansvarlighet som muliggjør effektiv IKT-risikostyring.

e) Identifisering, overvåking og rask rapportering av vesentlige IKT-relaterte hendelser til finansielle enheter, styring og krisehåndtering av disse hendelsene, særlig cyberangrep.

f) Ordninger for dataportabilitet, applikasjonsportabilitet og interoperabilitet som sikrer at de finansielle enhetene effektivt kan utøve sin oppsigelsesrett.

g) Testing av IKT-systemer, IKT-infrastruktur og IKT-kontroller.

h) IKT-revisjoner.

i) Bruk av relevante nasjonale og internasjonale standarder som får anvendelse på levering av IKT-tjenester til de finansielle enhetene.

4. På grunnlag av vurderingen nevnt i nr. 2 og koordinert med det felles tilsynsnettverket som er nevnt i artikkel 34 nr. 1, skal hovedovervåkeren vedta en klar, detaljert og begrunnet individuell tilsynsplan som beskriver de årlige tilsynsmålene og de viktigste tilsynshandlingene som er planlagt for hver kritisk tredjepartsleverandør av IKT-tjenester. Denne planen skal hvert år meddeles den kritiske tredjepartsleverandøren av IKT-tjenester.

Før tilsynsplanen vedtas, skal hovedovervåkeren oversende utkastet til tilsynsplan til den kritiske tredjepartsleverandøren av IKT-tjenester.

Ved mottak av utkastet til tilsynsplan kan den kritiske tredjepartsleverandøren av IKT-tjenester sende inn en begrunnet uttalelse innen 15 kalenderdager som viser den forventede innvirkningen på de kundene som er enheter som faller utenfor virkeområdet for denne forordningen, og dersom det er relevant, utarbeide løsninger for å redusere risikoene.

5. Når de årlige tilsynsplanene nevnt i nr. 4 er vedtatt og meddelt de kritiske tredjepartsleverandørene av IKT-tjenester, kan vedkommende myndigheter treffe tiltak med hensyn til slike kritiske tredjepartsleverandører av IKT-tjenester bare etter avtale med hovedovervåkeren.

Artikkel 34

Operasjonell koordinering mellom hovedovervåkere

1. For å sikre en konsekvent strategi for overvåkingsvirksomhet og for å muliggjøre koordinerte generelle tilsynsstrategier og sammenhengende operasjonelle tilnærminger og arbeidsmetoder skal de tre ledende tilsynsmyndighetene som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b), opprette et felles overvåkingsnettverk for seg imellom å koordinere de forberedende fasene og gjennomføringen av overvåkingsvirksomheten for de respektive kritiske tredjepartsleverandørene av IKT-tjenester som de overvåker, samt i forbindelse med eventuelle tiltak som måtte være nødvendige i henhold til artikkel 42.

2. Ved anvendelse av nr. 1 skal hovedovervåkerne utarbeide en felles overvåkingsprotokoll som angir de nærmere framgangsmåtene som skal følges for å gjennomføre den daglige koordineringen, og for å sikre raske utvekslinger og reaksjoner. Protokollen skal revideres regelmessig for å gjenspeile operasjonelle behov, særlig utviklingen av praktiske overvåkingsordninger.

3. Hovedovervåkerne kan fra gang til gang anmode ESB og ENISA om å yte teknisk rådgivning, dele praktisk erfaring eller delta i spesifikke koordineringsmøter i det felles overvåkingsnettverket.

Artikkel 35

Hovedovervåkerens myndighet

1. For å utføre de oppgavene som er fastsatt i dette avsnittet, har hovedovervåkeren følgende myndighet med hensyn til de kritiske tredjepartsleverandørene av IKT-tjenester:

a) Å anmode om alle relevante opplysninger og dokumentasjon i samsvar med artikkel 37.

b) Å gjennomføre generelle undersøkelser og inspeksjoner i samsvar med henholdsvis artikkel 38 og 39.

c) Å anmode om, etter at overvåkingsvirksomheten er avsluttet, rapporter som angir hvilke tiltak som er truffet, eller hvilke avhjelpende tiltak som er iverksatt av de kritiske tredjepartsleverandørene av IKT-tjenester, i forbindelse med de anbefalingene som er nevnt i bokstav d) i dette nummeret.

d) Å utstede anbefalinger på de områdene som er nevnt i artikkel 33 nr. 3, særlig

   i) om anvendelse av spesifikke IKT-relaterte sikkerhets- og kvalitetskrav eller -prosesser, særlig i forbindelse med utrulling av programvareutbedringer, oppdateringer, kryptering og andre sikkerhetstiltak som hovedovervåkeren anser som relevante for å sikre IKT-sikkerheten til tjenester som leveres til finansielle enheter,

   ii) om anvendelse av vilkår og betingelser, herunder den tekniske gjennomføringen av dem, i henhold til hvilke kritiske tredjepartsleverandører av IKT-tjenester leverer IKT-tjenester til finansielle enheter, som hovedovervåkeren anser som relevante for å forhindre generering av svake punkter («single points of failure»), eller at disse forsterkes, eller for å minimere eventuelle systemiske virkninger i Unionens finanssektor i tilfelle av IKT-konsentrasjonsrisiko,

   iii) om eventuelle planlagte underentrepriser, der hovedovervåkeren anser at ytterligere underentreprise, herunder underleverandøravtaler som de kritiske tredjepartsleverandørene av IKT-tjenester planlegger å inngå med tredjepartsleverandører av IKT-tjenester eller med IKT-underleverandører som er etablert i et tredjeland, kan utløse risikoer for den finansielle enhetens levering av tjenester, eller risiko for den finansielle stabiliteten, på grunnlag av undersøkelsen av de opplysningene som er samlet inn i samsvar med artikkel 37 og 38,

   iv) om å avstå fra å inngå en ytterligere underleverandøravtale, der følgende kumulative vilkår er oppfylt:

      — den påtenkte underleverandøren er en tredjepartsleverandør av IKT-tjenester eller en underleverandør av IKT-tjenester som er etablert i et tredjeland,

      — underentreprisen gjelder den finansielle enhetens kritiske eller viktige funksjoner, og

— hovedovervåkeren anser at bruken av slik underentreprise utgjør en klar og alvorlig risiko for den finansielle stabiliteten i Unionen eller for finansielle enheter, herunder for finansielle enheters evne til å overholde tilsynskravene.

Ved anvendelse av punkt iv) i denne bokstaven skal tredjepartsleverandører av IKT-tjenester ved bruk av den malen som er nevnt i artikkel 41 nr. 1 bokstav b), overføre opplysninger om underentreprise til hovedovervåkeren.

2. Når hovedovervåkeren utøver den myndigheten som er nevnt i denne artikkelen, skal den

a) sikre regelmessig koordinering innenfor det felles overvåkingsnettverket og særlig tilstrebe konsekvente strategier, dersom det er relevant, med hensyn til overvåkingen av kritiske tredjepartsleverandører av IKT-tjenester,

b) ta behørig hensyn til det rammeverket som er fastsatt i henhold til direktiv (EU) 2022/2555, og, dersom det er nødvendig, høre de berørte vedkommende myndighetene som er utpekt eller opprettet i samsvar med det nevnte direktivet, for å unngå overlapping av tekniske og organisatoriske tiltak som kan få anvendelse på kritiske tredjepartsleverandører av IKT-tjenester i henhold til det nevnte direktivet,

c) i den grad det er mulig, tilstrebe å minimere risikoen for forstyrrelser i tjenester som leveres av kritiske tredjepartsleverandører av IKT-tjenester til kunder som er enheter som faller utenfor virkeområdet for denne forordningen.

3. Hovedovervåkeren skal høre overvåkingsforumet før den utøver den myndigheten som er nevnt i nr. 1.

Før hovedovervåkeren utsteder anbefalinger i samsvar med nr. 1 bokstav d), skal den gi tredjepartsleverandøren av IKT-tjenester mulighet til å legge fram, innen 30 kalenderdager, relevante opplysninger som dokumenterer den forventede innvirkningen på kunder som er enheter som faller utenfor virkeområdet for denne forordningen, og, dersom det er relevant, utarbeide løsninger for å redusere risikoene.

4. Hovedovervåkeren skal underrette det felles overvåkingsnettverket om resultatet av myndighetsutøvelsen nevnt i nr. 1 bokstav a) og b). Hovedovervåkeren skal uten unødig opphold oversende rapportene nevnt i nr. 1 bokstav c) til det felles overvåkingsnettverket og til de vedkommende myndighetene for de finansielle enhetene som bruker IKT-tjenester levert av den kritiske tredjepartsleverandøren av IKT-tjenester.

5. Kritiske tredjepartsleverandører av IKT-tjenester skal lojalt samarbeide med hovedovervåkeren og bistå denne i utførelsen av sine oppgaver.

6. Ved hel eller delvis manglende overholdelse av de tiltakene som kreves i henhold til myndighetsutøvelsen i nr. 1 bokstav a), b) og c), og etter utløpet av en periode på minst 30 kalenderdager fra den datoen da den kritiske tredjepartsleverandøren av IKT-tjenester ble underrettet om de respektive tiltakene, skal hovedovervåkeren treffe en beslutning om å ilegge et overtredelsesgebyr for å tvinge den kritiske tredjepartsleverandøren av IKT-tjenester til å overholde disse tiltakene.

7. Overtredelsesgebyret nevnt i nr. 6 skal ilegges daglig fram til overholdelse er oppnådd, og i høyst seks måneder etter underretningen om beslutningen om å ilegge den kritiske tredjepartsleverandøren av IKT-tjenester et overtredelsesgebyr.

8. Størrelsen på overtredelsesgebyret, beregnet fra den datoen som er fastsatt i beslutningen om å ilegge overtredelsesgebyret, skal utgjøre opp til 1 % av den gjennomsnittlige globale omsetningen per dag for den kritiske tredjepartsleverandøren av IKT-tjenester i foregående regnskapsår. Ved fastsettelse av størrelsen på overtredelsesgebyret skal hovedovervåkeren ta hensyn til følgende kriterier for manglende overholdelse av tiltakene nevnt i nr. 6:

a) Den manglende overholdelsens grovhet og varighet.

b) Hvorvidt den manglende overholdelsen er begått forsettlig eller uaktsomt.

c) Viljen hos tredjepartsleverandøren av IKT-tjenester til å samarbeide med hovedovervåkeren.

Ved anvendelse av første ledd skal hovedovervåkeren delta i samråd innenfor det felles overvåkingsnettverket for å sikre en konsekvent strategi.

9. Overtredelsesgebyr skal være av administrativ art og skal kunne tvangsfullbyrdes. Tvangsfullbyrdelsen skal følge de gjeldende sivile rettergangsreglene i den medlemsstaten på hvis territorium inspeksjoner og adgang skal finne sted. Domstolene i den berørte medlemsstaten skal ha domsmyndighet til å treffe beslutninger om klager knyttet til uregelmessigheter i forbindelse med tvangsfullbyrdelsen. Beløpene for overtredelsesgebyr skal overføres til Den europeiske unions alminnelige budsjett.

10. Hovedovervåkeren skal offentliggjøre alle overtredelsesgebyr som er ilagt, med mindre en slik offentliggjøring skulle kunne skape alvorlig uro på finansmarkedene eller påføre berørte parter uforholdsmessig stor skade.

11. Før hovedovervåkeren ilegger overtredelsesgebyr i henhold til nr. 6, skal den gi representantene for den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, mulighet til å bli hørt om de omstendighetene som overvåkingsmyndigheten har påtalt, og den skal basere sine beslutninger bare på omstendigheter som den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, har hatt mulighet til å uttale seg om.

Retten til forsvar for de personene saken gjelder, skal sikres fullt ut under saksbehandlingen. Den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, skal ha rett til innsyn i saksmappen, med forbehold for andre personers rettmessige interesse av å bevare sine forretningshemmeligheter. Retten til innsyn i saksmappen skal ikke omfatte fortrolige opplysninger eller hovedovervåkerens interne forberedende dokumenter.

Artikkel 36

Hovedovervåkerens myndighetsutøvelse utenfor unionen

1. Dersom overvåkingsmålene ikke kan oppnås ved samhandling med datterforetaket som er opprettet i henhold til artikkel 31 nr. 12, eller ved å utøve overvåkingsvirksomhet i lokaler i Unionen, kan hovedovervåkeren utøve den myndigheten som er nevnt i følgende bestemmelser, i alle lokaler i et tredjeland og som eies eller på en eller annen måte brukes av en kritisk tredjepartsleverandør av IKT-tjenester for å levere tjenester til finansielle enheter i Unionen i forbindelse med sin forretningsvirksomhet, sine funksjoner eller tjenester, herunder alle administrative kontorer, foretakslokaler eller driftssteder, anlegg, arealer, bygninger eller andre eiendommer:

a) I artikkel 35 nr. 1 bokstav a).

b) I artikkel 35 nr. 1 bokstav b), i samsvar med artikkel 38 nr. 2 bokstav a), b) og d), og i artikkel 39 nr. 1 og 2 bokstav a).

Myndigheten omhandlet i første ledd kan utøves dersom alle følgende vilkår er oppfylt:

i) Hovedovervåkeren anser det som nødvendig å gjennomføre en inspeksjon i et tredjeland for at denne fullt ut og på en effektiv måte skal kunne utføre sine oppgaver i henhold til denne forordningen.

ii) Inspeksjonen i et tredjeland har direkte tilknytning til levering av IKT-tjenester til finansielle enheter i Unionen.

iii) Den berørte kritiske tredjepartsleverandøren av IKT-tjenester samtykker i at det gjennomføres en inspeksjon i et tredjeland.

iv) Den berørte myndigheten i det berørte tredjelandet er blitt offisielt underrettet av hovedovervåkeren og har ikke gjort innsigelse mot dette.

2. Uten at det berører Unionens institusjoner og medlemsstatenes respektive myndighet, skal EBA, ESMA eller EIOPA ved anvendelse av nr. 1 inngå ordninger om administrativt samarbeid med den berørte myndigheten i det berørte tredjelandet for å gjøre det mulig for hovedovervåkeren og den gruppen som den har utpekt til oppgaven i det aktuelle tredjelandet, å gjennomføre inspeksjoner på en smidig måte i det berørte tredjelandet. Disse samarbeidsordningene skal ikke medføre juridiske forpliktelser for Unionen og dens medlemsstater og skal heller ikke hindre medlemsstatene og deres vedkommende myndigheter i å inngå bilaterale eller multilaterale avtaler med disse tredjelandene og deres berørte myndigheter.

Disse samarbeidsordningene skal minst angi følgende opplysninger:

a) Framgangsmåtene for koordinering av den overvåkingsvirksomheten som utøves i henhold til denne forordningen, og enhver tilsvarende overvåking av IKT-tredjepartsrisiko i finanssektoren som utøves av den berørte myndigheten i det berørte tredjelandet, herunder nærmere opplysninger om oversending av sistnevntes samtykke til at hovedovervåkeren og dens utpekte gruppe kan gjennomføre generelle undersøkelser og stedlige inspeksjoner i henhold til nr. 1 første ledd, på det territoriet som er omfattet av dens jurisdiksjon.

b) Ordningen for overføring av alle relevante opplysninger mellom EBA, ESMA eller EIOPA og den berørte myndigheten i det berørte tredjelandet, særlig i forbindelse med opplysninger som hovedovervåkeren kan anmode om i henhold til artikkel 37.

c) Ordningene for rask underretning fra den berørte myndigheten i det berørte tredjelandet til EBA, ESMA eller EIOPA om tilfeller der en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med artikkel 31 nr. 1 bokstav a), anses å ha overtrådt de kravene den er forpliktet til å oppfylle i henhold til gjeldende rett i det berørte tredjelandet, når den leverer tjenester til finansinstitusjoner i dette tredjelandet, samt de avhjelpende tiltakene og sanksjonene som er anvendt.

d) Regelmessig overføring av oppdateringer om utviklingen på regulerings- og tilsynsområdet når det gjelder overvåkingen av IKT-tredjepartsrisiko for finansinstitusjoner i det berørte tredjelandet.

e) Nærmere opplysninger som ved behov gjør det mulig for én representant for den relevante myndigheten i det berørte tredjelandet å delta i de inspeksjonene som hovedovervåkeren og den utpekte gruppen gjennomfører.

3. Når hovedovervåkeren ikke er i stand til å gjennomføre overvåkingsvirksomhet utenfor Unionen som nevnt i nr. 1 og 2, skal hovedovervåkeren

a) utøve sin myndighet i henhold til artikkel 35 på grunnlag av alle de forholdene som den kjenner til, og dokumentene som den har tilgang til,

b) dokumentere og redegjøre for eventuelle konsekvenser av at den ikke er i stand til å gjennomføre den planlagte overvåkingsvirksomheten som nevnt i denne artikkelen.

De potensielle konsekvensene omhandlet i bokstav b) i dette nummeret skal tas i betraktning i hovedovervåkerens anbefalinger utstedt i henhold til artikkel 35 nr. 1 bokstav d).

Artikkel 37

Anmodning om opplysninger

1. Hovedovervåkeren kan ved enkel anmodning eller ved beslutning kreve at kritiske tredjepartsleverandører av IKT-tjenester legger fram alle de opplysningene som er nødvendige for at hovedovervåkeren skal kunne utføre sine oppgaver i henhold til denne forordningen, herunder alle relevante forretningsdokumenter eller operasjonelle dokumenter, kontrakter, retningslinjer, dokumentasjon, rapporter fra revisjon av IKT-sikkerhet, IKT-relaterte hendelsesrapporter, samt alle opplysninger om parter som den kritiske tredjepartsleverandøren av IKT-tjenester har utkontraktert driftsfunksjoner eller aktiviteter til.

2. Når hovedovervåkeren sender en enkel anmodning om opplysninger i henhold til nr. 1, skal den

a) vise til denne artikkelen som rettslig grunnlag for sin anmodning,

b) angi formålet med anmodningen,

c) angi nærmere hvilke opplysninger som kreves,

d) fastsette en frist for når opplysningene skal legges fram,

e) underrette representanten for den tredjepartsleverandøren av IKT-tjenester som anmodes om opplysninger, om at vedkommende ikke er forpliktet til å legge fram opplysningene, men at de opplysningene som legges fram frivillig som svar på anmodningen, ikke må være uriktige eller villedende.

3. Når hovedovervåkeren ved en beslutning anmoder om opplysninger i henhold til nr. 1, skal den

a) vise til denne artikkelen som rettslig grunnlag for sin anmodning,

b) angi formålet med anmodningen,

c) angi nærmere hvilke opplysninger som kreves,

d) fastsette en frist for når opplysningene skal legges fram,

e) angi de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, dersom de ønskede opplysningene er ufullstendige, eller dersom de ikke er lagt fram innen den tidsfristen som er nevnt i bokstav d) i dette nummeret,

f) opplyse om retten til å anke beslutningen inn for de europeiske tilsynsmyndighetenes klageinstans og til å bringe beslutningen inn for Den europeiske unions domstol («Domstolen») i samsvar med artikkel 60 og 61 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. Representantene for de kritiske tredjepartsleverandørene av IKT-tjenester skal legge fram de opplysningene som det anmodes om. Advokater med behørig fullmakt kan legge fram opplysningene på vegne av sine klienter. Den kritiske tredjepartsleverandøren av IKT-tjenester har det fulle ansvaret dersom opplysningene som legges fram, er ufullstendige, uriktige eller villedende.

5. Hovedovervåkeren skal umiddelbart oversende en kopi av beslutningen om å utlevere opplysninger til de vedkommende myndighetene for de finansielle enhetene som benytter seg av de tjenestene som de berørte tredjepartsleverandørene av IKT-tjenester leverer, og til det felles overvåkingsnettverket.

Artikkel 38

Generelle undersøkelser

1. For å utføre sine oppgaver i henhold til denne forordningen kan hovedovervåkeren, med bistand fra den felles granskningsgruppen omhandlet i artikkel 40 nr. 1, om nødvendig gjennomføre undersøkelser av kritiske tredjepartsleverandører av IKT-tjenester.

2. Hovedovervåkeren skal ha myndighet til å

a) undersøke registre, data, framgangsmåter og alt annet materiale som har betydning for utførelsen av dens oppgaver, uansett hvilket medium de er lagret på,

b) ta eller skaffe bekreftede kopier av eller utdrag fra slike registre, opplysninger, dokumenterte framgangsmåter og alt annet materiale,

c) innkalle representanter for den kritiske tredjepartsleverandøren av IKT-tjenester og be om muntlige eller skriftlige redegjørelser for forhold eller dokumenter som berører gjenstanden for og formålet med undersøkelsen, samt registrere svarene,

d) høre enhver fysisk eller juridisk person som samtykker i å bli hørt, for å samle inn opplysninger om gjenstanden for undersøkelsen,

e) anmode om opplysninger om tele- og datatrafikk.

3. De tjenestemennene og andre personer som har fullmakt fra hovedovervåkeren til å gjennomføre undersøkelsen nevnt i nr. 1, skal utøve sin myndighet mot framvisning av en skriftlig tillatelse med nærmere opplysninger om gjenstanden for og formålet med undersøkelsen.

Denne tillatelsen skal også inneholde opplysninger om de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, dersom dokumentasjonen, opplysningene, de dokumenterte framgangsmåtene eller alt annet materiale som kreves, eller svarene på spørsmål som er stilt til representanter for tredjepartsleverandøren av IKT-tjenester, ikke legges fram eller er ufullstendige.

4. Representantene for de kritiske tredjepartsleverandørene av IKT-tjenester er pålagt å underkaste seg undersøkelsene på grunnlag av en beslutning fra hovedovervåkeren. Beslutningen skal angi undersøkelsens gjenstand og formål, de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, klageadgangen i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 samt retten til å bringe beslutningen inn for Domstolen.

5. Hovedovervåkeren skal i god tid før undersøkelsen starter, underrette vedkommende myndigheter om de finansielle enhetene som benytter seg av IKT-tjenestene til den kritiske tredjepartsleverandøren av IKT-tjenester, om den planlagte undersøkelsen og om identiteten til de bemyndigede personene.

Hovedovervåkeren skal underrette det felles overvåkingsnettverket om alle opplysninger som oversendes i henhold til første ledd.

Artikkel 39

Inspeksjoner

1. For å utføre sine oppgaver i henhold til denne forordningen kan hovedovervåkeren, med bistand fra de felles granskningsgruppene som er nevnt i artikkel 40 nr. 1, innlede og gjennomføre alle nødvendige stedlige inspeksjoner i alle forretningslokaler, på arealer eller i eiendommer som tilhører tredjepartsleverandørene av IKT-tjenester, som for eksempel hovedkontorer, operasjonssentraler og sekundære lokaler, samt gjennomføre eksterne inspeksjoner.

Ved utøvelse av den myndigheten som er nevnt i første ledd, skal hovedovervåkeren rådføre seg med det felles overvåkingsnettverket.

2. De tjenestemennene og andre personer som har fullmakt fra hovedovervåkeren til å gjennomføre en stedlig inspeksjon, skal ha myndighet til å

a) få adgang til forretningslokaler, arealer eller eiendommer og å

b) forsegle slike forretningslokaler, regnskap eller forretningsdokumenter i det tidsrommet og i det omfanget som kreves for inspeksjonen.

Tjenestemenn og andre personer som har fullmakt fra hovedovervåkeren, skal utøve sin myndighet mot framvisning av en skriftlig tillatelse med nærmere opplysninger om gjenstanden for og formålet med inspeksjonen og om overtredelsesgebyr omhandlet i artikkel 35 nr. 6 som får anvendelse dersom representantene for de berørte kritiske tredjepartsleverandørene av IKT-tjenester ikke underkaster seg inspeksjonen.

3. Hovedovervåkeren skal i god tid før inspeksjonen starter, underrette de vedkommende myndighetene for de finansielle enhetene som bruker denne tredjepartsleverandøren av IKT-tjenester.

4. Inspeksjonene skal omfatte alle relevante IKT-systemer, nettverk, utstyr, opplysninger og data som entes brukes til eller bidrar til leveringen av IKT-tjenester til finansielle enheter.

5. Før en planlagt stedlig inspeksjon skal hovedovervåkeren i rimelig tid underrette de kritiske tredjepartsleverandørene av IKT-tjenester, med mindre en slik underretning ikke er mulig på grunn av en nøds- eller krisesituasjon, eller dersom det ville føre til en situasjon der inspeksjonen eller revisjonen ikke lenger ville være effektiv.

6. Den kritiske tredjepartsleverandøren av IKT-tjenester skal underkaste seg stedlige inspeksjoner som er pålagt i henhold til en beslutning truffet av hovedovervåkeren. Beslutningen skal angi inspeksjonens gjenstand og formål, fastsette tidspunktet da inspeksjonen skal starte, og angi de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, klageadgangen i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 samt retten til å bringe beslutningen inn for Domstolen.

7. Dersom tjenestemenn og andre personer som har fullmakt fra hovedovervåkeren, konstaterer at en kritisk tredjepartsleverandør av IKT-tjenester gjør innsigelse mot en inspeksjon som er pålagt i henhold til denne artikkelen, skal hovedovervåkeren underrette den kritiske tredjepartsleverandøren av IKT-tjenester om konsekvensene av en slik innsigelse, herunder om muligheten for de relevante finansielle enhetenes vedkommende myndigheter til å kreve at de finansielle enhetene sier opp de kontraktsregulerte ordningene som er inngått med den aktuelle kritiske tredjepartsleverandøren av IKT-tjenester.

Artikkel 40

Løpende tilsyn

1. Når hovedovervåkeren utøver overvåkingsvirksomhet, særlig generelle undersøkelser eller inspeksjoner, skal den bistås av en felles granskningsgruppe som er opprettet for hver kritisk tredjepartsleverandør av IKT-tjenester.

2. Den felles granskningsgruppen nevnt i nr. 1 skal bestå av ansatte fra

a) de europeiske tilsynsmyndighetene,

b) de berørte vedkommende myndighetene som fører tilsyn med de finansielle enhetene som den kritiske tredjepartsleverandøren av IKT-tjenester leverer IKT-tjenester til,

c) den nasjonale vedkommende myndigheten nevnt i artikkel 32 nr. 4 bokstav e), på frivillig grunnlag,

d) én nasjonal vedkommende myndighet fra den medlemsstaten der den kritiske tredjepartsleverandøren av IKT-tjenester er etablert, på frivillig grunnlag.

Medlemmene av den felles granskningsgruppen skal ha kunnskap om IKT-spørsmål og operasjonell risiko. Arbeidet i den felles granskningsgruppen skal koordineres av en utpekt ansatt under hovedovervåkeren («koordinatoren for hovedovervåkeren»).

3. Innen tre måneder etter at en undersøkelse eller inspeksjon er avsluttet, skal hovedovervåkeren, etter å ha hørt overvåkingsforumet, vedta anbefalinger som skal rettes til den kritiske tredjepartsleverandøren av IKT-tjenester i henhold til den myndigheten som er nevnt i artikkel 35.

4. Anbefalingene nevnt i nr. 3 skal umiddelbart meddeles den kritiske tredjepartsleverandøren av IKT-tjenester og de vedkommende myndighetene for de finansielle enhetene som den leverer IKT-tjenester til.

For å gjennomføre overvåkingsvirksomheten kan hovedovervåkeren ta hensyn til eventuelle relevante tredjepartssertifiseringer og interne eller eksterne revisjonsrapporter fra IKT-tredjeparter som er gjort tilgjengelige av den kritiske tredjepartsleverandøren av IKT-tjenester.

Artikkel 41

Harmonisering av vilkår som muliggjør utøvelse av tilsynsvirksomhet

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide forslag til tekniske reguleringsstandarder for å presisere

a) hvilke opplysninger en tredjepartsleverandør av IKT-tjenester skal gi i sin søknad om frivillig anmodning om å bli utpekt som kritisk i henhold til artikkel 31 nr. 11,

b) innholdet, strukturen og formatet til de opplysningene som skal legges fram, offentliggjøres eller rapporteres av tredjepartsleverandører av IKT-tjenester i henhold til artikkel 35 nr. 1, herunder malen for framlegging av opplysninger om underleverandøravtaler,

c) kriteriene for å fastsette sammensetningen av den felles granskningsgruppen som sikrer en balansert deltakelse av ansatte fra de europeiske tilsynsmyndighetene og fra de berørte vedkommende myndighetene, deres utpeking, oppgaver og arbeidsordninger.

d) nærmere opplysninger om de vedkommende myndighetenes vurdering av de tiltakene som er truffet av kritiske tredjepartsleverandører av IKT-tjenester på grunnlag av anbefalingene fra hovedovervåkeren i henhold til artikkel 42 nr. 3.

2. De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i nr. 1, i samsvar med framgangsmåten fastsatt i artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 42

Vedkommende myndigheters oppfølging

1. Innen 60 kalenderdager etter mottak av anbefalingene utstedt av hovedovervåkeren i henhold til artikkel 35 nr. 1 bokstav d), skal kritiske tredjepartsleverandører av IKT-tjenester enten underrette hovedovervåkeren om at de har til hensikt å følge anbefalingene, eller gi en begrunnet forklaring på hvorfor de ikke følger slike anbefalinger. Hovedovervåkeren skal umiddelbart oversende disse opplysningene til de berørte finansielle enhetenes vedkommende myndigheter.

2. Hovedovervåkeren skal offentliggjøre tilfeller der en kritisk tredjepartsleverandør av IKT-tjenester unnlater å underrette hovedovervåkeren i samsvar med nr. 1, eller dersom den forklaringen som gis av den kritiske tredjepartsleverandøren av IKT-tjenester ikke anses å være tilstrekkelig. De offentliggjorte opplysningene skal opplyse om identiteten til den kritiske tredjepartsleverandøren av IKT-tjenester samt om typen og arten av den manglende overholdelsen. Slike opplysninger skal begrenses til hva som er relevant og forholdsmessig med henblikk på å sikre allmennhetens bevissthet, med mindre en slik offentliggjøring skulle kunne forvolde de involverte partene uforholdsmessig stor skade eller i alvorlig grad bringe finansmarkedenes velordnede funksjon og integritet eller stabiliteten i hele eller deler av Unionens finanssystem i fare.

Hovedovervåkeren skal underrette tredjepartsleverandøren av IKT-tjenester om denne offentliggjøringen.

3. De vedkommende myndighetene skal underrette de relevante finansielle enhetene om de risikoene som er identifisert i anbefalingene rettet til kritiske tredjepartsleverandører av IKT-tjenester i samsvar med artikkel 35 nr. 1 bokstav d).

Når de finansielle enhetene styrer IKT-tredjepartsrisiko skal de ta hensyn til risikoene nevnt i første ledd.

4. Dersom en vedkommende myndighet vurderer at en finansiell enhet ikke tar hensyn til, eller ikke i tilstrekkelig grad i sin styring av IKT-tredjepartsrisiko håndterer de spesifikke risikoene som er identifisert i anbefalingene, skal den underrette den finansielle enheten om muligheten for at det innen 60 kalenderdager etter mottak av en slik underretning treffes en beslutning i samsvar med nr. 6, dersom det ikke foreligger egnede kontraktsregulerte ordninger som tar sikte på å håndtere slike risikoer.

5. De vedkommende myndighetene kan etter å ha mottatt rapportene nevnt i artikkel 35 nr. 1 bokstav c) og før de treffer en beslutning som nevnt i nr. 6 i denne artikkelen, på frivillig grunnlag høre de vedkommende myndighetene som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555, og som er ansvarlige for tilsynet med en vesentlig eller viktig enhet som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester.

6. De vedkommende myndighetene kan, som en siste utvei, etter underretningen og eventuelt høringen fastsatt i nr. 4 og 5 i denne artikkelen, i samsvar med artikkel 50 treffe en beslutning som krever at finansielle enheter midlertidig, enten helt eller delvis, avbryter bruken eller innføringen av en tjeneste som leveres av den kritiske tredjepartsleverandøren av IKT-tjenester, inntil de risikoene som er identifisert i anbefalingene til kritiske tredjepartsleverandører av IKT-tjenester, er blitt håndtert. De kan om nødvendig kreve at finansielle enheter helt eller delvis sier opp de relevante kontraktsregulerte ordningene som er inngått med de kritiske tredjepartsleverandørene av IKT-tjenester.

7. Dersom en kritisk tredjepartsleverandør av IKT-tjenester nekter å godta anbefalinger, basert på en annen strategi enn den som er anbefalt av hovedovervåkeren, og en slik annen strategi kan ha en negativ innvirkning på et høyt antall finansielle enheter eller en betydelig del av finanssektoren, og individuelle advarsler fra de vedkommende myndighetene ikke har ført til konsekvente strategier som begrenser den potensielle risikoen for den finansiell stabiliteten, kan hovedovervåkeren, etter å ha hørt overvåkingsforumet, avgi ikke-bindende og ikke-offentlige uttalelser til de vedkommende myndighetene for å fremme konsekvente og konvergerende tilsynsmessige oppfølgingstiltak, alt etter hva som er relevant.

8. Etter å ha mottatt rapportene nevnt i artikkel 35 nr. 1 bokstav c) skal vedkommende myndigheter, når de treffer en beslutning som omhandlet i nr. 6 i denne artikkelen, ta hensyn til typen og omfanget av den risikoen som ikke er håndtert av den kritiske tredjepartsleverandøren av IKT-tjenester, samt alvorlighetsgraden av den manglende overholdelsen, samtidig som det tas hensyn til følgende kriterier:

a) Den manglende overholdelsens grovhet og varighet.

b) Hvorvidt manglende overholdelse har påvist alvorlige svakheter i de framgangsmåtene, de ledelsessystemene, den risikostyringen og de internkontrollene som den kritiske tredjepartsleverandøren av IKT-tjenester ivaretar.

c) Hvorvidt økonomisk kriminalitet er blitt fremmet eller forårsaket av eller på annen måte kan tilskrives den manglende overholdelsen.

d) Hvorvidt den manglende overholdelsen er forsettlig eller uaktsom.

e) Hvorvidt midlertidig oppheving eller oppsigelse av de kontraktsregulerte ordningene medfører en risiko for kontinuiteten i den finansielle enhetens forretningsvirksomhet, til tross for den finansielle enhetens innsats for å unngå avbrudd i leveringen av tjenester.

f) Dersom det er relevant, den uttalelsen som på frivillig basis er innhentet i samsvar med nr. 5 i denne artikkelen fra de vedkommende myndighetene som i samsvar med direktiv (EU) 2022/2555 er utpekt eller opprettet som ansvarlige for tilsynet med en vesentlig eller viktig enhet, som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester.

De vedkommende myndighetene skal gi de finansielle enhetene den tiden som kreves for at de skal kunne tilpasse sine kontraktsregulerte ordninger med kritiske tredjepartsleverandører av IKT-tjenester for å unngå skadelige virkninger på den digitale operasjonelle motstandsdyktigheten, og slik at de kan innføre exit-strategier og overgangsplaner som nevnt i artikkel 28.

9. Den beslutningen som er nevnt i nr. 6 i denne artikkelen, skal meddeles medlemmene av overvåkingsforumet nevnt i artikkel 32 nr. 4 bokstav a), b) og c) og det felles overvåkingsnettverket.

De kritiske tredjepartsleverandørene av IKT-tjenester som er påvirket av beslutningene fastsatt i nr. 6, skal samarbeide fullt ut med de berørte finansielle enhetene, særlig i forbindelse med prosessen med midlertidig oppheving eller oppsigelse av deres kontraktsregulerte ordninger.

10. De vedkommende myndighetene skal regelmessig underrette hovedovervåkeren om de tilnærmingene og tiltakene som de har iverksatt i forbindelse med sine tilsynsoppgaver når det gjelder finansielle enheter, samt om de kontraktsregulerte ordningene som de finansielle enhetene har inngått, når kritiske tredjepartsleverandører av IKT-tjenester ikke helt eller delvis har godkjent anbefalingene til dem fra hovedovervåkeren.

11. Hovedovervåkeren kan på anmodning gi ytterligere avklaringer når det gjelder de anbefalingene som er utstedt for å veilede de vedkommende myndighetene om oppfølgingstiltakene.

Artikkel 43

Overvåkingsavgifter

1. Hovedovervåkeren skal i samsvar med den delegerte rettsakten nevnt i nr. 2 i denne artikkelen oppkreve avgifter hos kritiske tredjepartsleverandører av IKT-tjenester som fullt ut dekker hovedovervåkerens nødvendige utgifter i forbindelse med gjennomføringen av overvåkingsoppgaver i henhold til denne forordningen, herunder godtgjøring for eventuelle kostnader som kan påløpe som følge av arbeid utført av den felles granskningsgruppen omhandlet i artikkel 40, samt kostnadene til rådgivning fra de uavhengige ekspertene omhandlet i artikkel 32 nr. 4 andre ledd, i forbindelse med forhold som hører inn under ansvarsområdet for direkte overvåkingsvirksomhet.

Det avgiftsbeløpet som oppkreves hos en kritisk tredjepartsleverandør av IKT-tjenester, skal dekke alle kostnader som følger av utførelsen av oppgavene som er fastsatt i dette avsnittet, og skal stå i et rimelig forhold til leverandørens omsetning.

2. Kommisjonen gis myndighet til å vedta en delegert rettsakt i samsvar med artikkel 57 for å utfylle denne forordningen med hensyn til hvor høye avgiftsbeløpene skal være, og hvordan de skal betales innen 17. juli 2024.

Artikkel 44

Internasjonalt samarbeid

1. Uten at det berører artikkel 36, kan EBA, ESMA og EIOPA, i samsvar med artikkel 33 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010, inngå administrative ordninger med tredjelands regulerings- og tilsynsmyndigheter for å fremme internasjonalt samarbeid om IKT-tredjepartsrisiko i ulike finanssektorer, særlig ved å utvikle beste praksis for gjennomgåelse av praksis og kontroller i forbindelse med IKT-risikostyring, avbøtende tiltak og håndtering av hendelser.

2. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen hvert femte år legge fram en felles konfidensiell rapport for Europaparlamentet, Rådet og Kommisjonen, som sammenfatter resultatene av relevante drøftinger som er gjennomført med tredjelands myndigheter nevnt i nr. 1, og som fokuserer på utviklingen av IKT-tredjepartsrisiko og konsekvensene for den finansiell stabiliteten, markedsintegriteten, investorvernet og det indre markeds virkemåte.

KAPITTEL VI

Ordninger for utveksling av opplysninger

Artikkel 45

Ordninger for utveksling av opplysninger og etterretninger om cybertrusler

1. De finansielle enhetene kan seg imellom utveksle opplysninger og etterretninger om cybertrusler, herunder indikatorer på kompromittering, taktikker, teknikker og framgangsmåter, varsling av cybersikkerhet og konfigurasjonsverktøyer, i den grad slik utveksling av opplysninger og etterretninger

a) har som mål å forbedre finansielle enheters digitale operasjonelle motstandsdyktighet, særlig ved å øke bevisstheten om cybertrusler, begrense eller hindre cybertruslenes spredningsevne, støtte forsvarskapasiteten, metoder for påvisning av trusler, skadebegrensende strategier eller respons- og gjenopprettingsfaser,

b) finner sted innenfor betrodde grupper av finansielle enheter,

c) gjennomføres gjennom ordninger for utveksling av opplysninger som beskytter den potensielt sensitive karakteren til de opplysningene som utveksles, og som er omfattet av atferdsregler med full respekt for forretningshemmeligheter, vern av personopplysninger i samsvar med forordning (EU) 2016/679 og retningslinjer for konkurransepolitikk.

2. Ved anvendelse av nr. 1 bokstav c) skal ordningene for utveksling av opplysninger inneholde fastsatte vilkår for deltakelse og, dersom det er relevant, nærmere opplysninger om offentlige myndigheters deltakelse og den kapasiteten de kan ha i forbindelse med ordningene for utveksling av opplysninger, om deltakelse av tredjepartsleverandører av IKT-tjenester og om operasjonelle elementer, herunder bruken av særskilte IT-plattformer.

3. De finansielle enhetene skal underrette de vedkommende myndighetene om sin deltakelse i de ordningene for utveksling av opplysninger som er nevnt i nr. 1, når deres medlemskap er godkjent, eller, alt etter hva som er relevant, ved opphør av medlemskapet når dette trer i kraft.

KAPITTEL VII

Vedkommende myndigheter

Artikkel 46

Vedkommende myndigheter

Med forbehold for bestemmelsene om overvåkingsrammeverket for kritiske tredjepartsleverandører av IKT-tjenester som nevnt i kapittel V avsnitt II i denne forordningen, skal overholdelse av denne forordningen sikres av følgende vedkommende myndigheter i samsvar med den myndigheten som tildeles gjennom respektive rettsakter:

a) For kredittinstitusjoner og for institusjoner som er unntatt i henhold til direktiv 2013/36/EU, den vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i det nevnte direktivet, og for kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, Den europeiske sentralbank (ESB) i samsvar med den myndigheten og de oppgavene som er gitt i henhold til den nevnte forordningen.

b) For betalingsinstitusjoner, herunder betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og ytere av kontoopplysningstjenester som omhandlet i artikkel 33 nr. 1 i direktiv (EU) 2015/2366, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i direktiv (EU) 2015/2366.

c) For verdipapirforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i europaparlaments- og rådsdirektiv (EU) 2019/2034([38]).

d) For tilbydere av kryptoeiendeler som er meddelt tillatelse i henhold til forordningen om markeder for kryptoeiendeler, og utstedere av kryptoeiendeler, den vedkommende myndigheten som er utpekt i samsvar med den relevante bestemmelsen i den nevnte forordningen.

e) For verdipapirsentraler, den vedkommende myndigheten som er utpekt i samsvar med artikkel 11 i forordning (EU) nr. 909/2014.

f) For sentrale motparter, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i forordning (EU) nr. 648/2012.

g) For handelsplasser og leverandører av datarapporteringstjenester, den vedkommende myndigheten som er utpekt i samsvar med artikkel 67 i direktiv 2014/65/EU, og den vedkommende myndigheten som er definert i artikkel 2 nr. 1 punkt 18) i forordning (EU) nr. 600/2014.

h) For transaksjonsregistre, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i forordning (EU) nr. 648/2012.

i) For forvaltere av alternative investeringsfond, den vedkommende myndigheten som er utpekt i samsvar med artikkel 44 i direktiv 2011/61/EU.

j) For forvaltningsselskaper, den vedkommende myndigheten som er utpekt i samsvar med artikkel 97 i direktiv 2009/65/EF.

k) For forsikrings- og gjenforsikringsforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 30 i direktiv 2009/138/EF.

l) For forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, den vedkommende myndigheten som er utpekt i samsvar med artikkel 12 i direktiv (EU) 2016/97.

m) For tjenestepensjonsforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 47 i direktiv (EU) 2016/2341.

n) For kredittvurderingsbyråer, den vedkommende myndigheten som er utpekt i samsvar med artikkel 21 i forordning (EF) nr. 1060/2009.

o) For administratorer av kritiske referanseverdier, den vedkommende myndigheten som er utpekt i samsvar med artikkel 40 og 41 i forordning (EU) 2016/1011.

([38]) Europaparlaments- og rådsdirektiv (EU) 2019/2034 av 27. november 2019 om tilsyn med verdipapirforetak og om endring av direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU (EUT L 314 av 5.12.2019, s. 64).

p) For tilbydere av folkefinansieringstjenester, den vedkommende myndigheten som er utpekt i samsvar med artikkel 29 i forordning (EU) 2020/1503.

q) For verdipapiriseringsregistre, den vedkommende myndigheten som er utpekt i samsvar med artikkel 10 og artikkel 14 nr. 1 i forordning (EU) 2017/2402.

Artikkel 47

Samarbeid med strukturer og myndigheter som er opprettet ved direktiv (EU) 2022/2555

1. For å fremme samarbeid og muliggjøre tilsynsmessig utveksling mellom de vedkommende myndighetene som er utpekt i henhold til denne forordningen, og den samarbeidsgruppen som er opprettet ved artikkel 14 i direktiv (EU) 2022/2555, kan de europeiske tilsynsmyndighetene og de vedkommende myndighetene delta i samarbeidsgruppens virksomhet i saker som angår deres tilsynsvirksomhet i forbindelse med finansielle enheter. De europeiske tilsynsmyndighetene og de vedkommende myndighetene kan anmode om å bli invitert til å delta i samarbeidsgruppens virksomhet i saker som gjelder vesentlige eller viktige enheter som er omfattet av direktiv (EU) 2022/2555, og som også er utpekt som kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 31 i denne forordningen.

2. De vedkommende myndighetene kan, dersom det er relevant, rådføre seg og utveksle opplysninger med de felles kontaktpunktene og CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.

3. Dersom det er relevant, kan de vedkommende myndighetene anmode om en relevant teknisk uttalelse og bistand fra de vedkommende myndighetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, og inngå samarbeidsordninger, slik at det kan opprettes effektive og raske koordineringsordninger.

4. De ordningene som er nevnt i nr. 3 i denne artikkelen, kan blant annet angi framgangsmåtene for koordinering av tilsyns- og overvåkingvirksomhet i forbindelse med vesentlige eller viktige enheter som er omfattet av direktiv (EU) 2022/2555, og som er utpekt som kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 31 i denne forordningen, herunder for gjennomføring, i samsvar med nasjonal rett, av undersøkelser og stedlige inspeksjoner, samt for ordninger for utveksling av opplysninger mellom de vedkommende myndighetene i henhold til denne forordningen og de vedkommende myndighetene som er utpekt eller opprettet i samsvar med det nevnte direktivet, og som omfatter tilgang til opplysninger som de sistnevnte myndighetene har anmodet om.

Artikkel 48

Samarbeid mellom myndigheter

1. De vedkommende myndighetene skal ha et nært samarbeid seg imellom og, dersom det er relevant, med hovedovervåkeren.

2. De vedkommende myndighetene og hovedovervåkeren skal i god tid utveksle alle relevante opplysninger om kritiske tredjepartsleverandører av IKT-tjenester som er nødvendige for at de skal kunne utføre sine respektive oppgaver i henhold til denne forordningen, særlig i forbindelse med identifiserte risikoer, tilnærminger og tiltak som er truffet som ledd i hovedovervåkerens overvåkingsoppgaver.

Artikkel 49

Øvelser, kommunikasjon og samarbeid mellom finanssektorer

1. De europeiske tilsynsmyndighetene kan gjennom Felleskomiteen og i samarbeid med de vedkommende myndighetene, krisehåndteringsmyndighetene nevnt i artikkel 3 i direktiv 2014/59/EU, ESB, Det felles krisehåndteringsråd når det gjelder opplysninger om enheter som er omfattet av virkeområdet for forordning (EU) nr. 806/2014, ESRB og ENISA, alt etter hva som er relevant, opprette ordninger som gjør det mulig å utveksle effektive framgangsmåter mellom ulike finanssektorer for å øke situasjonsbevisstheten og identifisere felles cybersårbarheter og -risikoer i ulike sektorer.

De kan utarbeide krisestyrings- og beredskapsøvelser som omfatter cyberangrepsscenarioer, med henblikk på å utvikle kommunikasjonskanaler og gradvis muliggjøre en effektiv koordinert respons på unionsplan i tilfelle av en alvorlig grenseoverskridende IKT-relatert hendelse eller relatert trussel som har en systemisk virkning på Unionens finanssektor som helhet.

Disse øvelsene kan, alt etter hva som er relevant, også omfatte testing av finanssektorens avhengighet av andre økonomiske sektorer.

2. De vedkommende myndighetene, de europeiske tilsynsmyndighetene og ESB skal samarbeide nært med hverandre og utveksle opplysninger for å kunne utføre sine oppgaver i henhold til artikkel 47–54. De skal nøye koordinere tilsynet for å påvise og avhjelpe overtredelser av denne forordningen, utarbeide og fremme beste praksis, legge til rette for samarbeid, fremme konsekvens i tolkningen og utarbeide vurderinger på tvers av jurisdiksjoner dersom det oppstår eventuelle uenigheter.

Artikkel 50

Administrative sanksjoner og avhjelpende tiltak

1. De vedkommende myndighetene skal ha den tilsyns-, undersøkelses- og sanksjonsmyndigheten som er nødvendig for å sikre at de utfører sine oppgaver i henhold til denne forordningen.

2. Den myndigheten som er nevnt i nr. 1, skal minst omfatte myndighet til å

a) få tilgang til alle dokumenter eller andre opplysninger i enhver form, som den vedkommende myndigheten anser for relevante for utførelsen av sine oppgaver, og få eller ta en kopi av dem,

b) foreta stedlige inspeksjoner eller undersøkelser, som skal omfatte, men ikke er begrenset til

   i) å innkalle representanter for de finansielle enhetene og be dem om muntlige eller skriftlige redegjørelser for forhold eller dokumenter som berører gjenstanden for og formålet med undersøkelsen, samt registrere svarene,

   ii) å høre enhver fysisk eller juridisk person som går med på å bli hørt, for å samle inn opplysninger om gjenstanden for undersøkelsen,

c) å kreve korrigerende og avhjelpende tiltak ved manglende oppfyllelse av kravene i denne forordningen.

3. Uten at det berører medlemsstatenes rett til å pålegge strafferettslige sanksjoner i samsvar med artikkel 52, skal medlemsstatene fastsette regler om egnede administrative sanksjoner og avhjelpende tiltak ved overtredelse av denne forordningen og sikre at de gjennomføres på en effektiv måte.

Disse sanksjonene og tiltakene skal være virkningsfulle, stå i rimelig forhold til overtredelsen og virke avskrekkende.

4. Medlemsstatene skal gi vedkommende myndigheter myndighet til å anvende minst følgende administrative sanksjoner eller avhjelpende tiltak ved overtredelse av denne forordningen:

a) Å utstede et pålegg der det kreves at den fysiske eller juridiske personen avslutter den atferden som utgjør en overtredelse av denne forordningen, og ikke gjentar slik atferd.

b) Å kreve midlertidig eller varig opphør av enhver praksis eller atferd som den vedkommende myndigheten anser å være i strid med bestemmelsene i denne forordningen, og forhindre at praksisen eller atferden gjentas.

c) Å treffe enhver form for tiltak, herunder av økonomisk karakter, for å sikre at finansielle enheter fortsatt oppfyller de rettslige kravene.

d) Å kreve, i den utstrekning det er tillatt i henhold til nasjonal rett, utlevering av eksisterende opplysninger om datatrafikk som oppbevares av en teleoperatør, dersom det foreligger en begrunnet mistanke om en overtredelse av denne forordningen, og dersom disse opplysningene kan være relevante for en undersøkelse av overtredelser av denne forordningen.

e) Å utstede kunngjøringer, herunder offentlige erklæringer som identifiserer den ansvarlige fysiske eller juridiske personen og overtredelsens art.

5. Dersom nr. 2 bokstav c) og nr. 4 får anvendelse på juridiske personer, skal medlemsstatene gi vedkommende myndigheter myndighet til å anvende de administrative sanksjonene og de avhjelpende tiltakene, med forbehold for de vilkårene som er fastsatt i nasjonal rett, på medlemmer av ledelsesorganet og på andre fysiske personer som i henhold til nasjonal rett er ansvarlige for overtredelsen.

6. Medlemsstatene skal sikre at enhver beslutning om påleggelse av administrative sanksjoner eller avhjelpende tiltak i henhold til nr. 2 bokstav c), er behørig begrunnet og kan påklages.

Artikkel 51

Utøvelse av myndigheten til å pålegge administrative sanksjoner og treffe avhjelpende tiltak

1. De vedkommende myndighetene skal utøve sin myndighet til å pålegge administrative sanksjoner og treffe avhjelpende tiltak som nevnt i artikkel 50 i samsvar med sine nasjonale rettslige rammer, alt etter hva som er relevant, på følgende måte:

a) Direkte.

b) I samarbeid med andre myndigheter.

c) På eget ansvar ved delegering til andre myndigheter.

d) Ved anmodning til de vedkommende rettsmyndighetene.

2. De vedkommende myndighetene skal når de bestemmer typen av og nivået på en administrativ sanksjon eller et avhjelpende tiltak som pålegges eller treffes i henhold til artikkel 50, ta hensyn til i hvilken grad overtredelsen er begått med forsett eller skyldes uaktsomhet, og til alle andre relevante omstendigheter, herunder følgende, dersom det er relevant:

a) Overtredelsens vesentlighet, grovhet og varighet.

b) Graden av ansvar hos den fysiske eller juridiske personen som er ansvarlig for overtredelsen.

c) Den ansvarlige fysiske eller juridiske personens finansielle styrke.

d) Betydningen av den fortjenesten som er oppnådd, eller det tapet som er unngått av den ansvarlige fysiske eller juridiske personen, i den grad dette kan fastslås.

e) De tapene for tredjeparter som skyldes overtredelsen, i den grad dette kan fastslås.

f) Den ansvarlige fysiske eller juridiske personens vilje til å samarbeide med den vedkommende myndigheten, uten at det berører behovet for å sikre tilbakebetaling av den fortjenesten som den fysiske eller juridiske personens har oppnådd, eller de tapene som denne har unngått.

g) Tidligere overtredelser begått av den ansvarlige fysiske eller juridiske personen.

Artikkel 52

Strafferettslige sanksjoner

1. Medlemsstatene kan beslutte ikke å innføre administrative sanksjoner eller avhjelpende tiltak for overtredelser som er omfattet av strafferettslige sanksjoner i henhold til nasjonal rett.

2. Dersom medlemsstatene har valgt å fastsette strafferettslige sanksjoner for overtredelser av denne forordningen, skal de sikre at det er truffet hensiktsmessige tiltak slik at vedkommende myndigheter har all nødvendig myndighet til å holde kontakt med rettsmyndigheter, påtalemyndigheter eller strafferettslige myndigheter innenfor sin jurisdiksjon for å få konkrete opplysninger om strafferettslige etterforskninger eller rettssaker som er innledet på grunn av overtredelser av denne forordningen, og til å gi andre vedkommende myndigheter samt EBA, ESMA eller EIOPA de samme opplysningene, slik at de kan oppfylle sine forpliktelser om å samarbeide om anvendelsen av denne forordningen.

Artikkel 53

Underretningsplikt

Medlemsstatene skal innen 17. januar 2025 underrette Kommisjonen, ESMA, EBA og EIOPA om de lovene og forskriftene, herunder eventuelle relevante strafferettslige bestemmelser, som gjennomfører dette kapittelet. Medlemsstatene skal uten unødig opphold underrette Kommisjonen, ESMA, EBA og EIOPA om eventuelle senere endringer av dem.

Artikkel 54

Offentliggjøring av administrative sanksjoner

1. De vedkommende myndighetene skal uten unødig opphold offentliggjøre på sine offisielle nettsteder enhver avgjørelse om påleggelse av en administrativ sanksjon som ikke kan påklages, etter at mottakeren av sanksjonen er blitt underrettet om avgjørelsen.

2. Offentliggjøringen nevnt i nr. 1 skal inneholde opplysninger om overtredelsens type og art, identiteten til de ansvarlige personene og sanksjonene som er pålagt.

3. Dersom den vedkommende myndigheten etter en individuell vurdering anser at offentliggjøringen av juridiske personers identitet, eller fysiske personers identitet eller personopplysninger, vil være uforholdsmessig, herunder omfatte risikoer i forbindelse med vernet av personopplysninger, vil være til skade for finansmarkedenes stabilitet eller for en pågående strafferettslig etterforskning eller, i den grad dette kan fastslås, volde den berørte personen uforholdsmessig skade, skal den vedkommende myndigheten treffe et av følgende tiltak med hensyn til avgjørelsen om å pålegge en administrativ sanksjon:

a) Utsette offentliggjøringen av avgjørelsen inntil det ikke lenger finnes noen grunn til ikke å offentliggjøre den.

b) Offentliggjøre avgjørelsen anonymt i samsvar med nasjonal rett.

c) Avstå fra å offentliggjøre avgjørelsen dersom de alternativene som angis i bokstav a) og b), ikke anses for å være tilstrekkelige for å sikre at finansmarkedenes stabilitet ikke på noen som helst måte bringes i fare, eller dersom en slik offentliggjøring ikke er forholdsmessig når det gjelder mindre strenge sanksjoner.

4. Når det gjelder en avgjørelse om å offentliggjøre en administrativ sanksjon i anonymisert form i samsvar med nr. 3 bokstav b), kan offentliggjøringen av de relevante opplysningene utsettes.

5. Dersom en vedkommende myndighet offentliggjør en avgjørelse om påleggelse av en administrativ sanksjon som kan påklages til de relevante rettsmyndighetene, skal de vedkommende myndighetene dessuten på sitt offisielle nettsted uten unødig opphold offentliggjøre disse opplysningene sammen med eventuelle senere opplysninger om utfallet av en slik klage på et senere tidspunkt. Enhver rettsavgjørelse om oppheving av en avgjørelse om påleggelse av en administrativ sanksjon skal også offentliggjøres.

6. De vedkommende myndighetene skal sikre at enhver offentliggjøring som nevnt i nr. 1–4, bare er tilgjengelig på deres offisielle nettsted i den tidsperioden som er nødvendig ved anvendelse av denne artikkelen. Denne perioden skal ikke overstige fem år etter offentliggjøringen.

Artikkel 55

Taushetsplikt

1. Alle fortrolige opplysninger som mottas, utveksles eller overføres i henhold til denne forordningen, skal være underlagt vilkårene for taushetsplikt som er fastsatt i nr. 2.

2. Taushetsplikten gjelder alle personer som arbeider eller har arbeidet for de vedkommende myndighetene i henhold til denne forordningen, eller for enhver myndighet, markedsaktør eller fysisk eller juridisk person som de vedkommende myndighetene har delegert myndighet til, herunder revisorer og eksperter som de vedkommende myndighetene har inngått kontrakt med.

3. Opplysninger som er omfattet av taushetsplikt, herunder utveksling av opplysninger mellom vedkommende myndigheter i henhold til denne forordningen og vedkommende myndigheter som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, skal ikke gis videre til noen annen person eller myndighet, unntatt når dette skjer i henhold til bestemmelser i unionsretten eller nasjonal rett.

4. Alle opplysninger som utveksles mellom de vedkommende myndighetene i henhold til denne forordningen, og som gjelder forretnings- eller driftsforhold og andre økonomiske eller personlige forhold, skal anses som fortrolige og omfattes av kravene om taushetsplikt, unntatt når den vedkommende myndigheten på det tidspunkt opplysningene meddeles, erklærer at opplysningene kan gis videre, eller når videreformidling er nødvendig i forbindelse med rettsforfølgning.

Artikkel 56

Vern av personopplysninger

1. De europeiske tilsynsmyndighetene og de vedkommende myndighetene skal bare behandle personopplysninger dersom det er nødvendig for at de skal kunne oppfylle sine respektive forpliktelser og utføre sine oppgaver i henhold til denne forordningen, særlig med hensyn til undersøkelse, inspeksjon, anmodning om opplysninger, kommunikasjon, offentliggjøring, evaluering, verifisering, vurdering og utarbeiding av tilsynsplaner. Personopplysningene skal behandles i samsvar med forordning (EU) 2016/679 eller forordning (EU) 2018/1725, alt etter hvilken som får anvendelse.

2. Med mindre annet er fastsatt i andre sektorspesifikke rettsakter, skal de personopplysningene som er nevnt i nr. 1, lagres fram til de relevante tilsynsoppgavene er utført og under alle omstendigheter i høyst 15 år, unntatt i tilfelle av pågående rettssaker som krever ytterligere lagring av slike opplysninger.

KAPITTEL VIII

Delegerte rettsakter

Artikkel 57

Utøvelse av delegert myndighet

1. Myndigheten til å vedta delegerte rettsakter gis Kommisjonen med forbehold for vilkårene fastsatt i denne artikkelen.

2. Myndigheten til å vedta delegerte rettsakter nevnt i artikkel 31 nr. 6 og artikkel 43 nr. 2 skal gis Kommisjonen for en periode på fem år fra 17. januar 2024. Kommisjonen skal utarbeide en rapport om den delegerte myndigheten senest ni måneder før utløpet av femårsperioden. Den delegerte myndigheten skal stilltiende forlenges med perioder av samme varighet, med mindre Europaparlamentet eller Rådet motsetter seg slik forlengelse senest tre måneder før utløpet av hver periode.

3. Europaparlamentet eller Rådet kan når som helst tilbakekalle den delegerte myndigheten nevnt i artikkel 31 nr. 6 og artikkel 43 nr. 2. En beslutning om tilbakekalling innebærer at den delegerte myndigheten som angis i beslutningen, opphører å gjelde. Den får virkning dagen etter at beslutningen er kunngjort i Den europeiske unions tidende, eller på et senere tidspunkt angitt i beslutningen. Den berører ikke gyldigheten av delegerte rettsakter som allerede er trådt i kraft.

4. Før Kommisjonen vedtar en delegert rettsakt, skal den høre eksperter som er utpekt av hver medlemsstat i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming.

5. Så snart Kommisjonen vedtar en delegert rettsakt, skal den underrette Europaparlamentet og Rådet samtidig om dette.

6. En delegert rettsakt vedtatt i henhold til artikkel 31 nr. 6 og artikkel 43 nr. 2 skal tre i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse mot rettsakten innen en frist på tre måneder etter at rettsakten ble meddelt Europaparlamentet eller Rådet, eller dersom Europaparlamentet og Rådet innen utløpet av denne fristen begge har underrettet Kommisjonen om at de ikke kommer til å gjøre innsigelse. På Europaparlamentets eller Rådets initiativ forlenges denne fristen med tre måneder.

KAPITTEL IX

Overgangs- og sluttbestemmelser

Avsnitt I

Artikkel 58

Revisjonsklausul

1. Etter høring av de europeiske tilsynsmyndighetene og ESRB skal Kommisjonen innen 17. januar 2028, alt etter hva som er relevant, utføre en revisjon og legge fram en rapport for Europaparlamentet og Rådet, eventuelt ledsaget av et forslag til regelverk. Revisjonen skal minst omfatte følgende:

a) Kriteriene for utpeking av kritiske tredjepartsleverandører av IKT-tjenester i samsvar med artikkel 31 nr. 2.

b) Den frivillige karakteren av underretningen om betydelige cybertrusler som er nevnt i artikkel 19.

c) Den ordningen som er nevnt i artikkel 31 nr. 12 og hovedovervåkerens myndighet fastsatt i artikkel 35 nr. 1 bokstav d) iv) første ledd, med henblikk på å vurdere effektiviteten av disse bestemmelsene med hensyn til å sikre et effektivt tilsyn med kritiske tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland, og nødvendigheten av å etablere et datterforetak i Unionen.

   Ved anvendelse av første ledd i denne bokstaven skal revisjonen inneholde en analyse av ordningen nevnt i artikkel 31 nr. 12, herunder med hensyn til tilgangen for finansielle enheter i Unionen til tjenester fra tredjeland og tilgang til slike tjenester på markedet i Unionen, og den skal ta hensyn til den fortsatte utviklingen på markedene for de tjenestene som er omfattet av denne forordningen, finansielle enheters og finansielle tilsynsmyndigheters praktiske erfaring med hensyn til henholdsvis anvendelsen av og tilsynet med den ordningen, og enhver relevant utvikling innen regulering og tilsyn som finner sted på internasjonalt plan.

d) Hensiktsmessigheten av å la de finansielle enhetene som er nevnt i artikkel 2 nr. 3 bokstav e), og som bruker automatiserte salgssystemer, være omfattet av denne forordningens virkeområde på bakgrunn av den framtidige markedsutviklingen når det gjelder bruken av slike systemer.

e) Det felles overvåkingsnettverkets funksjon og effektivitet når det gjelder å støtte konsekvens i tilsynet og effektivitet i utvekslingen av opplysninger innenfor overvåkingsrammeverket.

2. I forbindelse med revisjonen av direktiv (EU) 2015/2366 skal Kommisjonen vurdere behovet for økt motstandsdyktighet mot cyberangrep i betalingssystemer og betalingsbehandlingsaktiviteter og hensiktsmessigheten av å utvide virkeområdet for denne forordningen til å omfatte operatører av betalingssystemer og enheter som er involvert i betalingsbehandlingsaktiviteter. På bakgrunn av denne vurderingen skal Kommisjonen, som en del av revisjonen av direktiv (EU) 2015/2366, legge fram en rapport for Europaparlamentet og Rådet senest 17. juli 2023.

På grunnlag av denne revisjonsrapporten og etter høring av de europeiske tilsynsmyndighetene, ESB og ESRB, kan Kommisjonen, dersom det er relevant, og som en del av det lovforslaget som den kan vedta i henhold til artikkel 108 andre ledd i direktiv (EU) 2015/2366, legge fram et forslag for å sikre at alle operatører av betalingssystemer og enheter som er involvert i betalingsbehandlingsaktiviteter, er omfattet av et hensiktsmessig tilsyn, samtidig som det tas hensyn til sentralbankens eksisterende tilsyn.

3. Innen 17. januar 2026 skal Kommisjonen, etter høring av de europeiske tilsynsmyndighetene og Komiteen for europeiske tilsynsorganer, utføre en revisjon og oversende en rapport til Europaparlamentet og Rådet, eventuelt ledsaget av et lovforslag, om hensiktsmessigheten av strengere krav til revisorer og revisjonsselskaper med hensyn til digital operasjonell motstandsdyktighet, ved å la revisorer og revisjonsselskaper bli omfattet av denne forordningens virkeområde eller ved å endre europaparlaments- og rådsdirektiv 2006/43/EF([39]).

Avsnitt II

Endringer

Artikkel 59

Endringer av forordning (EF) nr. 1060/2009

I forordning (EF) nr. 1060/2009 gjøres følgende endringer:

1) I vedlegg I avsnitt A nr. 4 skal første ledd lyde:

«Et kredittvurderingsbyrå skal ha god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i henhold til europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) I vedlegg III skal nr. 12 lyde:

«12. Kredittvurderingsbyrået overtrer artikkel 6 nr. 2, sammenholdt med vedlegg I avsnitt A nr. 4, dersom det ikke har god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i samsvar med forordning (EU) 2022/2554, eller dersom det ikke gjennomfører og opprettholder framgangsmåter for beslutningstaking eller organisasjonsstrukturer slik det kreves i det nevnte nummeret».

Artikkel 60

Endringer av forordning (EU) nr. 648/2012

I forordning (EU) nr. 648/2012 gjøres følgende endringer:

1) I artikkel 26 gjøres følgende endringer:

a) Nr. 3 skal lyde:

«3. En sentral motpart skal opprettholde en organisasjonsstruktur som sikrer kontinuitet og regelmessighet i leveringen av tjenester og utøvelsen av virksomhet. Den skal anvende egnede og forholdsmessige systemer, ressurser og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

([39]) Europaparlaments- og rådsdirektiv 2006/43/EF av 17. mai 2006 om lovfestet revisjon av årsregnskap og konsernregnskap, om endring av rådsdirektiv 78/660/EØF og 83/349/EØF og om oppheving av rådsdirektiv 84/253/EØF (EUT L 157 av 9.6.2006, s. 87).

b) Nr. 6 utgår.

2) I artikkel 34 gjøres følgende endringer:

a) Nr. 1 skal lyde:

«1. En sentral motpart skal utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan som skal omfatte retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting, som er utarbeidet og gjennomført i samsvar med forordning (EU) 2022/2554, og som har som formål å sikre opprettholdelse av dens funksjoner, sikre rask gjenopptakelse av driften og oppfyllelse av den sentrale motpartens forpliktelser.»

b) I nr. 3 skal første ledd lyde:

«3. For å sikre en ensartet anvendelse av denne artikkelen skal ESMA etter høring av ESSB-medlemmene utarbeide utkast til tekniske reguleringsstandarder med nærmere opplysninger om hva retningslinjene for kontinuitet i virksomheten og katastrofeberedskapsplanen minst skal inneholde, unntatt retningslinjer for IKT-kontinuitet i virksomheten og katastrofeberedskapsplaner.»

3) I artikkel 56 nr. 3 skal første ledd lyde:

«3. For å sikre en ensartet anvendelse av denne artikkelen skal ESMA utarbeide utkast til tekniske reguleringsstandarder med nærmere opplysninger om den søknaden om registrering som er nevnt i nr. 1, men ikke opplysninger om krav til IKT-risikostyring».

4) I artikkel 79 skal nr. 1 og 2 lyde:

«1. Et transaksjonsregister skal kartlegge kildene til operasjonell risiko og minimere dem ved å utvikle egnede systemer, kontroller og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.

2. Et transaksjonsregister skal utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og katastrofeberedskapsplan, herunder retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting utarbeidet i samsvar med (EU) 2022/2554, som har som formål å sikre opprettholdelsen av registerets funksjoner, og sikre rask gjenopptakelse av driften og oppfyllelse av transaksjonsregisterets forpliktelser.»

5) I artikkel 80 utgår nr. 1.

6) I vedlegg I avsnitt II gjøres følgende endringer:

a) Bokstav a) og b) skal lyde:

«a) Et transaksjonsregister overtrer artikkel 79 nr. 1 dersom det ikke kartlegger kildene til operasjonell risiko og minimerer dem, ved å utvikle egnede systemer, kontroller og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.

b) Et transaksjonsregister overtrer artikkel 79 nr. 2 dersom det ikke utarbeider, gjennomfører og opprettholder egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelse av registerets funksjoner, sikre rask gjenopptakelse av driften og oppfyllelse av transaksjonsregisterets forpliktelser.»

b) Bokstav c) utgår.

7) I vedlegg III gjøres følgende endringer:

a) I avsnitt II gjøres følgende endringer:

i) Bokstav c) skal lyde:

«c) En sentral motpart i kategori 2 overtrer artikkel 26 nr. 3 dersom den ikke opprettholder en organisasjonsstruktur som sikrer kontinuitet og regelmessighet i leveringen av tjenester og utøvelsen av virksomhet, eller ikke benytter hensiktsmessige og tilpassede systemer, ressurser og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.»

ii) Bokstav f) utgår.

b) I avsnitt III skal bokstav a) lyde:

«a) En sentral motpart i kategori 2 overtrer artikkel 34 nr. 1 dersom den ikke fastsetter, gjennomfører eller opprettholder egnede retningslinjer for kontinuitet i virksomheten og en respons- og gjenopprettingsplan utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelsen av den sentrale motpartens funksjoner, sikre rask gjenopptakelse av virksomheten og oppfyllelse av den sentrale motpartens forpliktelser, og som minst gjør det mulig å gjenopprette alle transaksjoner fra det tidspunktet da de ble avbrutt, slik at den sentrale motpartens drift fortsatt er sikker, og den kan gjennomføre oppgjør på den planlagte datoen.»

Artikkel 61

Endringer av forordning (EU) nr. 909/2014

I artikkel 45 i forordning (EU) nr. 909/2014 gjøres følgende endringer:

1) Nr. 1 skal lyde:

«1. En verdipapirsentral skal identifisere både interne og eksterne kilder til operasjonell risiko og begrense deres virkning ved å anvende egnede IKT-verktøyer, -prosesser og -retningslinjer som er fastsatt og forvaltet i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*), samt ved å anvende eventuelle andre relevante verktøyer, kontroller og framgangsmåter for andre typer av operasjonell risiko, herunder for alle de verdipapiroppgjørssystemene som den driver.

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) Nr. 2 utgår.

3) Nr. 3 og 4 skal lyde:

«3. En verdipapirsentral skal for tjenester som den yter, og for hvert verdipapiroppgjørssystem som den driver, utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan, herunder retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelsen av dens tjenester, sikre rask gjenopptakelse av driften og oppfyllelse av verdipapirsentralens forpliktelser i tilfelle av hendelser som medfører betydelig risiko for driftsavbrudd.

4. Planen nevnt i nr. 3 skal gjøre det mulig å gjenopprette alle transaksjoner og deltakeres posisjoner fra det tidspunktet da de ble avbrutt, slik at verdipapirsentralens deltakere fortsatt kan utøve sin virksomhet på en sikker måte og oppgjøret kan gjennomføres på den planlagte datoen, herunder ved å sikre at kritiske IT-systemer umiddelbart kan gjenoppta driften fra det tidspunktet da de ble avbrutt, som fastsatt i artikkel 12 nr. 5 og 7 i forordning (EU) 2022/2554.»

4) Nr. 6 skal lyde:

«6. En verdipapirsentral skal identifisere, overvåke og håndtere de risikoene som de viktigste deltakerne i de verdipapiroppgjørssystemene som den driver, samt tjenesteytere, andre verdipapirsentraler eller andre markedsinfrastrukturer kan utgjøre for dens virksomhet. Den skal på anmodning gi vedkommende og berørte myndigheter opplysninger om enhver slik risiko som er identifisert. Den skal også umiddelbart underrette den vedkommende myndigheten og berørte myndigheter om eventuelle operasjonelle hendelser som følge av slike risikoer, med unntak av IKT-risiko».

5) I nr. 7 skal første ledd lyde:

«7. ESMA skal i nært samarbeid med ESSB-medlemmene utarbeide utkast til tekniske reguleringsstandarder med nærmere opplysninger om de operasjonelle risikoene nevnt i nr. 1 og 6, med unntak av IKT-risiko, og metodene for å utprøve, håndtere eller minimere disse risikoene, herunder retningslinjene for kontinuitet i virksomheten og katastrofeberedskapsplanene nevnt i nr. 3 og 4 samt metodene for å vurdere disse.»

Artikkel 62

Endringer av forordning (EU) nr. 600/2014

I forordning (EU) nr. 600/2014 gjøres følgende endringer:

1) I artikkel 27g gjøres følgende endringer:

a) Nr. 4 skal lyde:

«4. En godkjent offentliggjøringsordning skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

b) I nr. 8 skal bokstav c) lyde:

«c) de konkrete organisatoriske kravene fastsatt i nr. 3 og 5,»

2) I artikkel 27h gjøres følgende endringer:

a) Nr. 5 skal lyde:

«5. En leverandør av et konsolidert offentliggjøringssystem skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i forordning (EU) 2022/2554.»

b) I nr. 8 skal bokstav e) lyde:

«e) de konkrete organisatoriske kravene fastsatt i nr. 4.»

3) I artikkel 27i gjøres følgende endringer:

a) Nr. 3 skal lyde:

«3. En godkjent rapporteringsordning skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i forordning (EU) 2022/2554.»

b) I nr. 5 skal bokstav b) lyde:

«b) de konkrete organisatoriske kravene fastsatt i nr. 2 og 4.»

Artikkel 63

Endring av forordning (EU) 2016/1011

I artikkel 6 i forordning (EU) 2016/1011 skal nytt nummer lyde:

«6. For kritiske referanseverdier skal en administrator ha god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

Artikkel 64

Ikrafttredelse og anvendelse

Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 17. januar 2025.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Strasbourg 14. desember 2022.

For Europaparlamentet	*For Rådet*
R. METSOLA	M. BEK
President	*Formann*