2024/1774

25.6.2024

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2024/1774

af 13. marts 2024

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer IKT-risikostyringsværktøjer, -metoder, -processer og -politikker og den forenklede ramme for IKT-risikostyring

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 ([1]), særlig artikel 15, fjerde afsnit, og artikel 16, stk. 3, fjerde afsnit, og

ud fra følgende betragtninger:

(1) Forordning (EU) 2022/2554 omfatter en bred vifte af finansielle enheder, der er forskellige med hensyn til størrelse, struktur, intern organisation og karakteren og kompleksiteten af deres aktiviteter, og som dermed har øgede eller reducerede elementer af kompleksitet eller risici. For at sikre, at der tages behørigt hensyn til denne mangfoldighed, bør alle krav vedrørende IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer og for så vidt angår en forenklet ramme for IKT-risikostyring stå i rimeligt forhold til disse finansielle enheders størrelse, struktur, interne organisation, karakter og kompleksitet og til de dertil svarende risici.

(2) Af samme årsag bør finansielle enheder, der er omfattet af forordning (EU) 2022/2554, have en vis fleksibilitet med hensyn til den måde, hvorpå de opfylder eventuelle krav vedrørende IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer og med hensyn til en eventuel forenklet ramme for IKT-risikostyring. Derfor bør finansielle enheder have mulighed for at anvende al den dokumentation, som de allerede er i besiddelse af for at opfylde eventuelle krav vedrørende dokumentation, som følger af nævnte krav. Det følger heraf, at udvikling, dokumentation og gennemførelse af specifikke IKT-sikkerhedspolitikker kun bør være påkrævet for visse væsentlige elementer, idet der bl.a. tages hensyn til førende praksis og standarder på sektorplan. For at dække specifikke tekniske gennemførelsesaspekter er det desuden nødvendigt at udvikle, dokumentere og gennemføre IKT-sikkerheds-procedurer for at dække specifikke tekniske gennemførelsesaspekter, herunder styring af kapacitet og ydeevne, sårbarheds- og korrektionsstyring, data- og systemsikkerhed og logføring.

(3) For at sikre en korrekt gennemførelse over tid af de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i denne forordnings afsnit II, kapitel I, er det vigtigt, at finansielle enheder tildeler og opretholder alle roller og ansvarsområder vedrørende IKT-sikkerhed korrekt, og at de fastsætter bestemmelser om konsekvenserne af manglende overholdelse af IKT-sikkerhedspolitikker eller -procedurer.

(4) For at begrænse risikoen for interessekonflikter bør finansielle enheder sikre adskillelse af opgaver, når de tildeler IKT-relaterede roller og ansvarsområder.

(5) For at sikre fleksibilitet og forenkle de finansielle enheders kontrolramme bør finansielle enheder ikke være forpligtet til at udarbejde specifikke bestemmelser om konsekvenserne af manglende overholdelse af de IKT-sikkerhedspolitikker, -procedurer og -protokoller, som er omhandlet i denne forordnings afsnit II, kapitel I, hvis sådanne bestemmelser allerede er fastsat som led i en anden politik eller procedure.

([1]) EUT L 333 af 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) I et dynamisk miljø, hvor IKT-risici hele tiden udvikler sig, er det vigtigt, at finansielle enheder udvikler deres sæt af IKT-sikkerhedspolitikker på grundlag af førende praksis og, hvis det er relevant, standarder som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([2]). Dette bør gøre det muligt for finansielle enheder, der er omhandlet i nærværende forordnings afsnit II, fortsat at være informerede og forberedte i et miljø, der er under forandring.

(7) For at sikre deres digitale operationelle modstandsdygtighed bør de finansielle enheder, der er omhandlet i afsnit II i denne forordning, som led i deres IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer udvikle og gennemføre en politik for forvaltning af IKT-aktiver, procedurer for styring af kapacitet og ydeevne samt politikker og procedurer for IKT-operationer. Disse politikker og procedurer er nødvendige for at sikre overvågning af IKT-aktivernes status i løbet af hele deres livscyklus, således at disse aktiver anvendes og vedligeholdes effektivt (forvaltning af IKT-aktiver). Disse politikker og procedurer bør også sikre optimering af IKT-systemernes drift, og at de resultater, der opnås med IKT-systemerne og kapaciteten, opfylder de fastlagte forretnings- og informationssikkerhedsmål (styring af kapacitet og ydeevne). Endelig bør disse politikker og procedurer sikre en effektiv og gnidningsfri daglig styring og drift af IKT-systemer (IKT-operationer) og dermed minimere risikoen for tab i forbindelse med fortroligheden, integriteten og tilgængeligheden af data. Disse politikker og procedurer er derfor nødvendige for at garantere netsikkerheden, træffe tilstrækkelige sikkerhedsforanstaltninger, der forhindrer indtrængen og datamisbrug, og for at bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

(8) For at sikre en korrekt styring af legacy-IKT-systemrisiciene bør finansielle enheder registrere og overvåge slutdatoerne for IKT-støttetjenester fra tredjeparter. På grund af den potentielle indvirkning, som tab af fortrolighed, integritet og tilgængelighed af data kan have, bør finansielle enheder fokusere på de IKT-aktiver eller -systemer, der er kritiske for forretningsdriften, når de registrerer og overvåger disse slutdatoer.

(9) Kryptografiske kontroller kan sikre tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. De finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør derfor identificere og gennemføre sådanne kontroller på grundlag af en risikobaseret tilgang. Med henblik herpå bør finansielle enheder kryptere de pågældende data, som er inaktive, under overførsel eller, hvis det er nødvendigt, i brug, på grundlag af resultaterne af en tostrenget proces, dvs. dataklassificering og en omfattende IKT-risikovurdering. I betragtning af kompleksiteten af at kryptere data, som er i brug, bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, kun kryptere data, som er i brug, hvis dette er hensigtsmæssigt i lyset af resultaterne af IKT-risikovurderingen. De finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør dog, hvis kryptering af data, som er i brug, ikke er mulig eller er for kompleks, kunne beskytte fortroligheden, integriteten og tilgængeligheden af de pågældende data ved hjælp af andre IKT-sikkerhedsforanstaltninger. I betragtning af den hurtige teknologiske udvikling inden for kryptografiske teknikker bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, holde sig ajour med den relevante udvikling inden for kryptoanalyse og tage førende praksis og standarder i betragtning. De finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør derfor følge en fleksibel tilgang, som er baseret på risikoafbødning og -overvågning, for at håndtere det dynamiske landskab af kryptografiske trusler, herunder trusler fra kvantefremskridt.

(10) Sikkerhed i forbindelse med IKT-operationer og operationelle politikker, procedurer, protokoller og værktøjer er afgørende for at sikre fortroligheden, integriteten og tilgængeligheden af data. Et centralt aspekt er den strenge adskillelse af IKT-produktionsmiljøer fra de miljøer, hvor IKT-systemer udvikles og testes, eller fra andre ikkeproduktionsmiljøer. Denne adskillelse bør fungere som en vigtig IKT-sikkerhedsforanstaltning mod utilsigtet og uautoriseret adgang til, ændringer og sletning af data i produktionsmiljøet, som kan føre til større forstyrrelser i forretningsaktiviteterne i de finansielle enheder, der er omhandlet i denne forordnings afsnit II. I betragtning af den nuværende praksis for udvikling af IKT-systemer bør finansielle enheder dog under ekstraordinære omstændigheder have mulighed for at foretage test i produktionsmiljøer, forudsat at de begrunder en sådan test og opnår den nødvendige godkendelse.

([2]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) IKT-landskabernes hastige udvikling, IKT-sårbarheder og cybertrusler nødvendiggør en proaktiv og fyldestgørende tilgang til at konstatere, evaluere og afhjælpe IKT-sårbarheder. Uden en sådan tilgang risikerer finansielle enheder, deres kunder, brugere eller modparter at blive alvorligt udsat for risici, som vil udgøre en fare for deres digitale operationelle modstandsdygtighed, deres netsikkerhed og tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, som IKT-sikkerhedspolitikker og -procedurer bør beskytte. De finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør derfor konstatere og afhjælpe sårbarheder i deres IKT-miljø, og både de finansielle enheder og deres tredjepartsudbydere af IKT-tjenester bør anvende en sammenhængende, gennemsigtig og ansvarlig ramme for sårbarhedsstyring. Af samme grund bør finansielle enheder overvåge IKT-sårbarheder ved hjælp af pålidelige ressourcer og automatiserede værktøjer og efterprøve, at tredjepartsudbydere af IKT-tjenester sikrer en øjeblikkelig indsats over for sårbarheder i de leverede IKT-tjenester.

(12) Korrektionsstyring bør være en afgørende del af de IKT-sikkerhedspolitikker og -procedurer, der gennem test og ibrugtagning i et kontrolleret miljø skal afhjælpe konstaterede sårbarheder og forhindre forstyrrelser, som skyldes installationen af korrektioner.

(13) For at sikre rettidig og gennemsigtig kommunikation om potentielle sikkerhedstrusler, der kan få indvirkning på den finansielle enhed og dens interessenter, bør finansielle enheder indføre procedurer for ansvarlig offentliggørelse af IKT-sårbarheder til kunder, modparter og offentligheden. Ved indførelsen af disse procedurer bør finansielle enheder tage hensyn til faktorer, herunder sårbarhedens omfang, den potentielle indvirkning af en sådan sårbarhed på interessenterne, og hvorvidt en udbedring eller afbødende foranstaltninger er klar til brug.

(14) For at gøre det muligt at tildele brugeradgangsrettigheder bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, indføre stærke foranstaltninger til at sikre entydig identifikation af enkeltpersoner og systemer, der vil få adgang til den finansielle enheds oplysninger. Hvis dette ikke sker, vil finansielle enheder blive udsat for potentiel uautoriseret adgang, brud på datasikkerheden og svigagtige aktiviteter, hvorved fortroligheden, integriteten og tilgængeligheden af følsomme finansielle data vil blive kompromitteret. Selv om anvendelsen af generiske eller delte konti undtagelsesvis bør tillades under omstændigheder, der beskrives nærmere af finansielle enheder, bør finansielle enheder sikre, at ansvaret for de foranstaltninger, der træffes via disse konti, opretholdes. Uden denne garanti vil potentielle ondsindede brugere være i stand til at hindre efterforskningsmæssige og korrigerende foranstaltninger, hvilket vil gøre finansielle enheder sårbare over for ikkedetekterede ondsindede aktiviteter eller sanktioner for manglende overholdelse.

(15) For at håndtere de hurtige fremskridt i IKT-miljøer bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, gennemføre robuste politikker og procedurer for IKT-projektstyring for at bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Disse politikker og procedurer for IKT-projektstyring bør identificere de elementer, der er nødvendige for en vellykket forvaltning af IKT-projekter, herunder ændringer af, anskaffelser af, vedligeholdelse af og udvikling af den finansielle enheds IKT-systemer, uanset hvilken metode til IKT-projektstyring, den finansielle enhed har valgt. I forbindelse med disse politikker og procedurer bør finansielle enheder indføre testpraksis og -metoder, der passer til deres behov, samtidig med at de følger en risikobaseret tilgang og sikrer, at der opretholdes et sikkert, pålideligt og modstandsdygtigt IKT-miljø. For at garantere en sikker gennemførelse af et IKT-projekt bør finansielle enheder sikre, at personale fra specifikke erhvervssektorer, eller som spiller specifikke roller, og som påvirkes af det pågældende IKT-projekt, kan levere de nødvendige oplysninger og den nødvendige ekspertise. For at sikre effektivt tilsyn bør rapporter om IKT-projekter, navnlig om projekter, der påvirker kritiske eller vigtige funktioner, og om de dertil knyttede risici, forelægges ledelsesorganet. Finansielle enheder bør tilpasse hyppigheden og udførligheden af de systematiske og løbende gennemgange og rapportere om betydningen og omfanget af de pågældende IKT-projekter.

(16) Det er nødvendigt at sikre, at softwarepakker, der erhverves og udvikles af finansielle enheder som omhandlet i denne forordnings afsnit II, integreres effektivt og sikkert i det eksisterende IKT-miljø i overensstemmelse med fastlagte forretnings- og informationssikkerhedsmål. Finansielle enheder bør derfor foretage en grundig evaluering af sådanne softwarepakker. Med henblik herpå og for at konstatere sårbarheder og potentielle sikkerhedsmangler i både softwarepakker og de bredere IKT-systemer bør finansielle enheder foretage IKT-sikkerhedstest. For at vurdere softwarens integritet og for at sikre, at anvendelsen af nævnte software ikke indebærer IKT-sikkerhedsrisici, bør finansielle enheder også gennemgå kildekoder for erhvervet software, herunder, når det er muligt, for proprietær software, der leveres af tredjepartsudbydere af IKT-tjenester, ved hjælp af både statiske og dynamiske testmetoder.

(17) Ændringer, uanset deres omfang, indebærer iboende risici og kan udgøre en betydelig risiko for tab af fortroligheden, integriteten og tilgængeligheden af data og kan dermed føre til alvorlige driftsforstyrrelser. For at beskytte finansielle enheder mod potentielle IKT-sårbarheder og -svagheder, der kan udsætte dem for betydelige risici, er det nødvendigt at have en streng kontrolproces for at bekræfte, at alle ændringer opfylder de nødvendige krav til IKT-sikkerhed. De finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør derfor som et væsentligt element i deres IKT-sikkerhedspolitikker og -procedurer have indført forsvarlige politikker og procedurer for styring af IKT-ændringer. For at opretholde objektiviteten og effektiviteten af processen for styring af IKT-ændringer, forebygge interessekonflikter og sikre, at IKT-ændringer vurderes objektivt, er det nødvendigt at adskille de funktioner, der sørger for godkendelse af disse ændringer, fra de funktioner, der sørger for anmodning om og gennemførelse af disse ændringer. For at opnå effektive overgange, kontrolleret gennemførelse af IKT-ændringer og minimale forstyrrelser i driften af IKT-systemerne bør finansielle enheder tildele klare roller og ansvarsområder, som sikrer, at IKT-ændringer planlægges, testes på passende vis, og at kvaliteten garanteres. For at sikre, at IKT-systemerne fortsat fungerer effektivt, og for at skabe et sikkerhedsnet for finansielle enheder bør finansielle enheder også udvikle og gennemføre nødprocedurer. Finansielle enheder bør klart angive disse nødprocedurer og tildele ansvarsområder for at sikre en hurtig og effektiv reaktion i tilfælde af fejlslagne IKT-ændringer.

(18) Med henblik på at detektere, styre og indberette IKT-relaterede hændelser bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, indføre en politik for IKT-relaterede hændelser, der omfatter komponenterne i en proces for styring af IKT-relaterede hændelser. Med henblik herpå bør finansielle enheder angive alle relevante kontakter i og uden for organisationen, som kan gøre den korrekte koordinering og gennemførelse af de forskellige faser i denne proces lettere. For at optimere detektionen af og reaktionen på IKT-relaterede hændelser og for at identificere tendenser blandt disse hændelser, som er en værdifuld informationskilde, der sætter finansielle enheder i stand til at identificere og håndtere de grundlæggende årsager og problemer på en effektiv måde, bør finansielle enheder navnlig foretage en udførlig analyse af de IKT-relaterede hændelser, som de anser for at være mest væsentlige, bl.a. på grund af deres regelmæssige gentagne forekomst.

(19) For at garantere en tidlig og effektiv detektion af anormale aktiviteter bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, indsamle, overvåge og analysere de forskellige informationskilder og fordele de dermed forbundne roller og ansvarsområder. Hvad angår interne informationskilder, er logfiler en yderst relevant kilde, men finansielle enheder bør ikke være afhængige af logfiler alene. I stedet bør finansielle enheder overveje bredere oplysninger, således at de inddrager oplysninger, der indberettes fra andre interne funktioner, da sådanne funktioner ofte er en værdifuld kilde til relevante oplysninger. Af samme grund bør finansielle enheder analysere og overvåge oplysninger, der indsamles fra eksterne kilder, herunder oplysninger fra tredjepartsudbydere af IKT-tjenester om hændelser, der påvirker deres systemer og netværk, og andre informationskilder, som finansielle enheder betragter som relevante. I det omfang sådanne oplysninger udgør personoplysninger, finder Unionens databeskyttelseslovgivning anvendelse. Personoplysningerne bør begrænses til, hvad der er nødvendigt for at detektere hændelsen.

(20) For at gøre det lettere at detektere IKT-relaterede hændelser bør finansielle enheder opbevare dokumentation for disse hændelser. For på den ene side at sikre, at en sådan dokumentation opbevares tilstrækkelig længe, og for på den anden side at undgå en uforholdsmæssig stor regelbyrde, bør finansielle enheder fastsætte opbevaringsperioden under hensyntagen til bl.a. den kritiske betydning af de data- og opbevaringskrav, der hidrører fra EU-retten.

(21) For at sikre, at IKT-relaterede hændelser detekteres i tide, bør de finansielle enheder, der er omhandlet i denne forordnings afsnit II, betragte de kriterier, der er fastlagt for at udløse detektion af og reaktion på IKT-relaterede hændelser, som ikkeudtømmende. Selvom finansielle enheder bør tage hensyn til hvert af disse kriterier, bør det ikke være et krav, at de omstændigheder, der er beskrevet i kriterierne, skal indtræffe samtidig, og der bør tages behørigt hensyn til betydningen af de berørte IKT-tjenester for at udløse detektions- og reaktionsprocesser i forbindelse med IKT-relaterede hændelser.

(22) Når de finansielle enheder, der er omhandlet i denne forordnings afsnit II, udvikler en politik for IKT-driftsstabilitet, bør de tage hensyn til de væsentlige komponenter i IKT-risikostyring, herunder styrings- og kommunikationsstrategier for styring af IKT-relaterede hændelser, processen for styring af IKT-ændringer og de risici, der er forbundet med tredjepartsudbydere af IKT-tjenester.

(23) Det er nødvendigt at fastlægge de scenarier, som de finansielle enheder, der er omhandlet i denne forordnings afsnit II, bør tage hensyn til både i forbindelse med gennemførelsen af planer for IKT-indsats- og genopretning og i forbindelse med test af planer for IKT-driftsstabilitet. Disse scenarier bør fungere som udgangspunkt for, at finansielle enheder kan analysere både relevansen og sandsynligheden af de enkelte scenarier og behovet for at udarbejde alternative scenarier. Finansielle enheder bør fokusere på de scenarier, hvor investeringer i modstandsdygtighedsforanstaltninger kan være mere effektive og virkningsfulde. Ved at teste omstillingsscenarier mellem den primære IKT-infrastruktur og enhver redundant kapacitet, sikkerhedskopier og redundante faciliteter bør de finansielle institutioner vurdere, om denne kapacitet, sikkerhedskopiering og disse faciliteter fungerer effektivt over en tilstrækkelig lang periode, og sikre, at den primære IKT-infrastrukturs normale funktion genoprettes i overensstemmelse med genopretningsmålene.

(24) Det er nødvendigt at fastsætte krav til operationelle risici og navnlig krav til IKT-projektstyring, styring af ændringer og styring af IKT-driftsstabilitet, der bygger på de krav, der allerede gælder for centrale modparter, værdipapircentraler og markedspladser i henhold til henholdsvis Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([3]), (EU) nr. 600/2014 ([4]) og (EU) nr. 909/2014 ([5]).

(25) I henhold til artikel 6, stk. 5, i forordning (EU) 2022/2554 skal finansielle enheder gennemgå deres ramme for IKT-risikostyring og forelægge deres kompetente myndighed en rapport om denne gennemgang. For at de kompetente myndigheder let kan behandle oplysningerne i disse rapporter og for at sikre tilstrækkelig overførsel af disse oplysninger, bør finansielle enheder indgive disse rapporter i et søgbart elektronisk format.

(26) Kravene til de finansielle enheder, der er omfattet af den forenklede ramme for IKT-risikostyring, jf. artikel 16 i forordning (EU) 2022/2554, bør fokusere på de væsentlige områder og elementer, der i lyset af det omfang, den risiko, størrelse og kompleksitet forbundet med disse finansielle enheder, som minimum er nødvendige for at sikre fortroligheden, integriteten, tilgængeligheden og autenticiteten af disse finansielle enheders data og tjenester. I den forbindelse bør disse finansielle enheder have indført en intern forvaltnings- og kontrolramme med klare ansvarsområder for at muliggøre en effektiv og forsvarlig ramme for risikostyring. For at mindske den administrative og operationelle byrde bør disse finansielle enheder desuden kun udvikle og dokumentere én politik, nemlig en informationssikkerhedspolitik, der præciserer de principper og regler på højt niveau, som er nødvendige for at bevare fortroligheden, integriteten, tilgængeligheden og autenticiteten af disse finansielle enheders data og tjenester.

(27) Bestemmelserne i denne forordning vedrører det område, der henhører under rammen for IKT-risikostyring, idet de præciserer specifikke elementer, der finder anvendelse på de finansielle enheder i overensstemmelse med artikel 15 i forordning (EU) 2022/2554, og idet de udformer den forenklede ramme for IKT-risikostyring for de finansielle enheder, jf. nævnte forordnings artikel 16, stk. 1. For at sikre sammenhæng mellem den almindelige og den forenklede ramme for IKT-risikostyring og i betragtning af, at disse bestemmelser bør træde i kraft samtidig, bør disse bestemmelser samles i én enkelt lovgivningsmæssig retsakt.

(28) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som Den Europæiske Banktilsynsmyndighed, Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger og Den Europæiske Værdipapir- og Markedstilsynsmyndighed (de europæiske tilsynsmyndigheder) har forelagt Kommissionen i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

([3]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Det Fælles Udvalg af Europæiske Tilsynsmyndigheder, jf. artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([6]), artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([7]) og artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([8]), har afholdt åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele ved de foreslåede standarder og anmodet om rådgivning fra interessentgruppen for banker, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1093/2010, interessentgruppen for forsikrings- og genforsikringsordninger og interessentgruppen for arbejdsmarkedspensionsordninger, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1094/2010, og interessentgruppen for værdipapirer og markeder, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1095/2010.

(30) I det omfang behandling af personoplysninger er nødvendig for at opfylde forpligtelserne i denne retsakt, bør forordning (EU) 2016/679 ([9]) og forordning (EU) 2018/1725 ([10]) af Europa-Parlamentet og Rådet finde fuld anvendelse. For eksempel bør princippet om dataminimering overholdes, når der indsamles personoplysninger, for at sikre en passende detektion af hændelser. Den Europæiske Tilsynsførende for Databeskyttelse er også blevet hørt om udkastet til denne retsakt —

VEDTAGET DENNE FORORDNING:

AFSNIT I

GENERELLE PRINCIPPER

Artikel 1

Overordnet risikoprofil og kompleksitet

Ved udviklingen og gennemførelsen af de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i afsnit II, og den forenklede ramme for IKT-risikostyring, der er omhandlet i afsnit III, skal der tages hensyn til den finansielle enheds størrelse og overordnede risikoprofil samt karakteren, omfanget og elementerne af øget eller reduceret kompleksitet af dens tjenester, aktiviteter og operationer, herunder elementer vedrørende:

a) kryptering og kryptografi

b) sikkerhed i forbindelse med IKT-operationer

c) netsikkerhed

([6]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

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

d) styring af IKT-projekter og -ændringer

e) IKT-risikoens potentielle indvirkning på fortroligheden, integriteten og tilgængeligheden af data, og den potentielle indvirkning af forstyrrelserne på driftsstabiliteten og tilgængeligheden af den finansielle enheds aktiviteter.

AFSNIT II

YDERLIGERE HARMONISERING AF IKT-RISIKOSTYRINGSVÆRKTØJER, -METODER, -PROCESSER OG -POLITIKKER I OVERENSSTEMMELSE MED ARTIKEL 15 I FORORDNING (EU) 2022/2554

KAPITEL I

IKT-SIKKERHEDSPOLITIKKER, -PROCEDURER, -PROTOKOLLER OG -VÆRKTØJER

Afdeling 1

Artikel 2

Generelle elementer i IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer

1. Finansielle enheder sikrer, at deres IKT-sikkerhedspolitikker, informationssikkerhed og dermed forbundne procedurer, protokoller og værktøjer som omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554 er integreret i deres ramme for IKT-risikostyring. Finansielle enheder indfører de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er fastsat i dette kapitel, og som:

a) garanterer netsikkerheden

b) indeholder sikkerhedsforanstaltninger, der forhindrer indtrængninger og datamisbrug

c) bevarer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, herunder ved anvendelse af kryptografiske teknikker

d) garanterer en nøjagtig og hurtig dataoverførsel uden større forstyrrelser og unødige forsinkelser.

2. Finansielle enheder sikrer, at de i stk. 1 omhandlede IKT-sikkerhedspolitikker:

a) er tilpasset den finansielle enheds informationssikkerhedsmål, der indgår i strategien for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, i forordning (EU) 2022/2554

b) angiver datoen for ledelsesorganets formelle godkendelse af IKT-sikkerhedspolitikkerne

c) indeholder indikatorer og foranstaltninger med henblik på at:

   i) overvåge gennemførelsen af IKT-sikkerhedspolitikkerne, -procedurerne, -protokollerne og -værktøjerne

   ii) registrere undtagelser fra denne gennemførelse

   iii) sikre, at den finansielle enheds digitale operationelle modstandsdygtighed bevares i tilfælde af undtagelser som omhandlet i nr. ii)

d) præciserer personalets ansvarsområder på alle niveauer for at garantere den finansielle enheds IKT-sikkerhed

e) præciserer konsekvenserne, i tilfælde af at den finansielle enheds personale ikke overholder IKT-sikkerhedspolitikkerne, såfremt bestemmelser herom ikke er fastsat i andre af den finansielle enheds politikker

f) angiver en liste over den dokumentation, der skal opbevares

g) præciserer ordningerne for opgaveadskillelse efter modellen med tre forsvarslinjer eller en anden model for intern risikostyring og -kontrol, alt efter hvad der er relevant, for at undgå interessekonflikter

h) tager hensyn til førende praksis og, når det er relevant, standarder som defineret i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012

i) angiver roller og ansvarsområder i forbindelse med udvikling, gennemførelse og vedligeholdelse af IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer

j) gennemgås i overensstemmelse med artikel 6, stk. 5, i forordning (EU) 2022/2554

k) tager hensyn til væsentlige ændringer vedrørende den finansielle enhed, herunder væsentlige ændringer af den finansielle enheds aktiviteter eller processer, cybertrusselsbilledet eller gældende retlige forpligtelser.

Afdeling 2

Artikel 3

IKT-risikostyring

Finansielle enheder udvikler, dokumenterer og gennemfører IKT-risikostyringspolitikker og -procedurer, som skal indeholde alle følgende:

a) en angivelse af godkendelsen af det risikotoleranceniveau for IKT-risiko, der er fastsat i overensstemmelse med artikel 6, stk. 8, litra b), i forordning (EU) 2022/2554

b) en procedure for og metode til gennemførelse af IKT-risikovurdering, der identificerer:

   i) sårbarheder og trusler, der påvirker eller kan påvirke de understøttede forretningsfunktioner, IKT-systemer og IKT-aktiver, der understøtter disse funktioner

   ii) de kvantitative eller kvalitative indikatorer til måling af indvirkningen af og sandsynligheden for de sårbarheder og trusler, der er omhandlet i nr. i)

c) proceduren for identifikation, gennemførelse og dokumentation af foranstaltninger til IKT-risikobehandling med henblik på de identificerede og vurderede IKT-risici, herunder fastlæggelse af de foranstaltninger til IKT-risikobehandling, der er nødvendige for, at IKT-risikoen holdes inden for det risikotoleranceniveau, der er omhandlet i litra a)

d) for de resterende IKT-risici, der stadig er til stede efter gennemførelsen af de foranstaltninger til IKT-risikobehandling, der er omhandlet i litra c):

   i) bestemmelser om identifikation af disse resterende IKT-risici

   ii) tildeling af roller og ansvarsområder vedrørende:

      1) accepten af de resterende IKT-risici, der overskrider den finansielle enheds risikotoleranceniveau, jf. litra a),

      2) den proces for gennemgang, der er omhandlet i dette litra d), nr. iv)

   iii) udarbejdelse af en fortegnelse over de accepterede resterende IKT-risici, herunder en begrundelse for accepten heraf

   iv) bestemmelser om gennemgangen af de accepterede resterende IKT-risici mindst én gang om året, herunder:

      1) identifikation af eventuelle ændringer i de resterende IKT-risici

      2) vurderingen af tilgængelige afbødende foranstaltninger

      3) vurderingen af, om begrundelserne for accept af resterende IKT-risici stadig er gyldige og gældende på datoen for gennemgangen

e) bestemmelser om overvågning af:

   i) eventuelle ændringer i IKT-risikoen og cybertrusselsbilledet

   ii) interne og eksterne sårbarheder og trusler:

   iii) den finansielle enheds IKT-risiko, der muliggør hurtig detektion af ændringer, der kan påvirke dens IKT-risikoprofil

f) bestemmelser om en proces, der skal sikre, at der tages hensyn til eventuelle ændringer af den finansielle enheds forretningsstrategi og strategi for digital operationel modstandsdygtighed.

Med henblik på stk. 1, litra c), skal den procedure, der er omhandlet i nævnte litra, sikre:

a) overvågning, om de gennemførte foranstaltninger til IKT-risikobehandling er effektive

b) vurdering af, om den finansielle enheds fastsatte risikotoleranceniveauer er nået

c) vurdering af, om den finansielle enhed har truffet foranstaltninger til at korrigere eller forbedre disse foranstaltninger, hvis det er nødvendigt.

Afdeling 3

Forvaltning af IKT-aktiver

Artikel 4

Politik for forvaltning af IKT-aktiver

1. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder en politik for forvaltning af IKT-aktiver.

2. Den i stk. 1 omhandlede politik for forvaltning af IKT-aktiver skal:

a) fastsætte overvågning og forvaltning af livscyklussen for IKT-aktiver, der er identificeret og klassificeret i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554

b) fastsætte, at den finansielle enhed skal føre fortegnelser over alle følgende:

   i) den entydige identifikator for hvert enkelt IKT-aktiv

   ii) fysiske eller logiske oplysninger om placeringen af alle IKT-aktiver

   iii) klassificeringen af alle IKT-aktiver som omhandlet i artikel 8, stk. 1, i forordning (EU) 2022/2254

   iv) identiteten af ejere af IKT-aktiver

   v) de forretningsfunktioner eller -tjenester, som IKT-aktivet understøtter

   vi) kravene til IKT-driftsstabilitet, herunder mål for genopretningstid og genopretningspunkt

   vii) hvorvidt IKT-aktivet kan være eller er eksponeret for eksterne netværk, herunder internettet

   viii) forbindelserne og den indbyrdes afhængighed mellem IKT-aktiver og de forretningsfunktioner, der anvender det enkelte IKT-aktiv

   ix) hvis det er relevant, for alle IKT-aktiver, slutdatoerne for de almindelige, udvidede og tilpassede støttetjenester fra den pågældende tredjepartsudbyder af IKT-tjenester, hvorefter disse IKT-aktiver ikke længere understøttes af deres leverandør eller af en tredjepartsudbyder af IKT-tjenester

c) for andre finansielle enheder end mikrovirksomheder, fastsætte, at disse finansielle enheder fører fortegnelser over de oplysninger, der er nødvendige med henblik på at foretage en specifik IKT-risikovurdering af alle de legacy-IKT-systemer, der er omhandlet i artikel 8, stk. 7, i forordning (EU) 2022/2554.

Artikel 5

Procedure for forvaltning af IKT-aktiver

1. Finansielle enheder udvikler, dokumenterer og gennemfører en procedure for forvaltning af IKT-aktiver.

2. Den i stk. 1 omhandlede procedure for forvaltning af IKT-aktiver skal præcisere kriterierne for at foretage vurderingen af kritisk betydning af informationsaktiver og IKT-aktiver, der understøtter forretningsfunktioner. Denne vurdering skal tage hensyn til:

a) den IKT-risiko, der er forbundet med disse forretningsfunktioner og deres afhængighed af informationsaktiverne eller IKT-aktiverne

b) hvordan tabet af fortrolighed, integritet og tilgængelighed af sådanne informationsaktiver og IKT-aktiver vil få indvirkning på de finansielle enheders forretningsprocesser og -aktiviteter.

Afdeling 4

KRYPTERING OG KRYPTOGRAFI

Artikel 6

Kryptering og kryptografiske kontroller

1. Som led i deres IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder en politik for kryptering og kryptografiske kontroller.

2. Finansielle enheder udformer den i stk. 1 omhandlede politik for kryptering og kryptografiske kontroller på grundlag af resultaterne af en godkendt dataklassificering og IKT-risikovurdering. Denne politik skal indeholde regler for alle følgende:

a) kryptering af data, som er inaktive eller under overførsel

b) kryptering af data, som er i brug, hvis det er nødvendigt

c) kryptering af interne netværkssammenkoblinger og trafik med eksterne parter

d) forvaltning af krypteringsnøgler, jf. artikel 7, der fastsætter regler for korrekt anvendelse af, beskyttelse af og livscyklus for krypteringsnøgler.

Med henblik på litra b) skal finansielle enheder, såfremt kryptering af data, som er i brug, ikke er mulig, behandle data, som er i brug, i et adskilt og beskyttet miljø eller træffe tilsvarende foranstaltninger til at sikre fortroligheden, integriteten, autenticiteten og tilgængeligheden af data.

3. Finansielle enheder inkluderer i den politik for kryptering og kryptografiske kontroller, der er omhandlet i stk. 1, kriterier for udvælgelse af kryptografiske teknikker og anvendelsespraksis, idet de tager hensyn til førende praksis og standarder som defineret i artikel 2, nr. (1), i forordning (EU) nr. 1025/2012 og den klassificering af relevante IKT-aktiver, der er fastsat i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554. Finansielle enheder, der ikke formår at overholde førende praksis eller standarder eller anvende de mest pålidelige teknikker, vedtager afbødnings- og overvågningsforanstaltninger, der sikrer modstandsdygtighed over for cybertrusler.

4. Finansielle enheder inkluderer i den politik for kryptering og kryptografiske kontroller, der er omhandlet i stk. 1, bestemmelser om opdatering eller ændring, såfremt det er nødvendigt, af kryptografisk teknologi på grundlag af udviklingen inden for kryptoanalyse. Disse opdateringer eller ændringer skal sikre, at den kryptografiske teknologi forbliver modstandsdygtig over for cybertrusler, jf. artikel 10, stk. 2, litra a). Finansielle enheder, der ikke formår at opdatere eller ændre den kryptografiske teknologi, vedtager afbødnings- og overvågningsforanstaltninger, der sikrer modstandsdygtighed over for cybertrusler.

5. Finansielle enheder inkluderer i den politik for kryptering og kryptografiske kontroller, der er omhandlet i stk. 1, et krav om at registrere vedtagelsen afbødnings- og overvågningsforanstaltninger, der er vedtaget i overensstemmelse med stk. 3 og 4, og om at give en begrundet redegørelse for vedtagelsen heraf.

Artikel 7

Forvaltning af krypteringsnøgler

1. Finansielle enheder inkluderer i den politik for forvaltning af krypteringsnøgler, der er omhandlet i artikel 6, stk. 2, litra d), krav om forvaltning af krypteringsnøgler gennem hele deres livscyklus, herunder generering, fornyelse, lagring, sikkerhedskopiering, arkivering, genfinding, overførsel, udrangering, tilbagekaldelse og destruktion af sådanne krypteringsnøgler.

2. Finansielle enheder identificerer og gennemfører kontroller til beskyttelse af krypteringsnøgler gennem hele deres livscyklus mod tab, uautoriseret adgang, videregivelse og ændring. Finansielle enheder udformer sådanne kontroller på grundlag af resultaterne af den godkendte dataklassificering og IKT-risikovurderingen.

3. Finansielle enheder udvikler og gennemfører metoder til udskiftning af krypteringsnøglerne i tilfælde af tab, eller hvis disse krypteringsnøgler kompromitteres eller skades.

4. Finansielle enheder opretter og vedligeholder et register over alle certifikater og alt udstyr til lagring af certifikater som minimum for IKT-aktiver, der understøtter kritiske eller vigtige funktioner. Finansielle enheder sørger for at ajourføre dette register.

5. Finansielle enheder sørger for øjeblikkelig fornyelse af certifikater inden de udløber.

Afdeling 5

SIKKERHED I FORBINDELSE MED IKT-OPERATIONER

Artikel 8

Politikker og procedurer for IKT-operationer

1. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder politikker og procedurer for styring af IKT-operationer. Ved disse politikker og procedurer præciseres det, hvordan finansielle enheder anvender, overvåger, kontrollerer og genopretter deres IKT-aktiver, herunder dokumentationen vedrørende IKT-operationer.

2. De i stk. 1 omhandlede politikker og procedurer for IKT-operationer skal indeholde alle følgende:

a) en beskrivelse af IKT-aktiver, herunder alle følgende:

   i) krav vedrørende sikker installering, vedligeholdelse, konfigurering og afinstallering af et IKT-system

   ii) krav vedrørende forvaltning af informationsaktiver, der anvendes af IKT-aktiver, herunder behandling og håndtering heraf, hvad enten det sker automatisk eller manuelt

   iii) krav vedrørende identifikation og kontrol af legacy-IKT-systemer,

b) kontroller og overvågning af IKT-systemer, herunder alle følgende:

   i) krav til sikkerhedskopiering og genopretning af IKT-systemer

   ii) krav til planlægning, som tager hensyn til indbyrdes afhængighed mellem IKT-systemer

   iii) protokoller vedrørende revisionsspor og oplysninger om systemlog

   iv) krav, som skal sikre, at udøvelsen af intern revision og anden test minimerer forstyrrelser i forretningsaktiviteterne

   v) krav til adskillelse af IKT-produktionsmiljøer fra udviklings- og testmiljøer og andre ikkeproduktionsmiljøer

   vi) krav om at foretage udvikling og test i miljøer, som er adskilt fra produktionsmiljøet

   vii) krav om at foretage udvikling og test i produktionsmiljøer

c) fejlbehandling i IKT-systemer, herunder alle følgende:

i) procedurer og protokoller for fejlbehandling

ii) support- og fejlafhjælpningskontakter, herunder eksterne supportkontakter i tilfælde af uforudsete operationelle og tekniske problemer

iii) genstart af IKT-systemer, annullering af opdateringer og genopretningsprocedurer, som skal anvendes i tilfælde af forstyrrelser i IKT-systemer.

Med henblik på litra b), nr. v), skal adskillelsen omfatte alle komponenterne i miljøet, herunder konti, data eller sammenkoblinger, jf. kravene i artikel 13, stk. 1, litra a).

Med henblik på litra b), nr. vii), skal det i de politikker og procedurer, der er omhandlet i stk. 1, fastsættes, at de omstændigheder, under hvilke der foretages test i et produktionsmiljø, er klart identificerede, begrundede, at de finder sted inden for et begrænset tidsrum, og at de er godkendt af den relevante funktion, jf. artikel 16, stk. 6. Finansielle enheder sikrer tilgængeligheden, fortroligheden, integriteten og autenticiteten af IKT-systemer og produktionsdata i forbindelse med udvikling og testaktiviteter i produktionsmiljøet.

Artikel 9

Styring af kapacitet og ydeevne

1. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder procedurer for styring af kapacitet og ydeevne med henblik på følgende:

a) identifikation af kapacitetskrav til deres IKT-systemer

b) anvendelse af ressourceoptimering

c) overvågningsprocedurer med henblik på vedligeholdelse og forbedring

i) tilgængeligheden af data og IKT-systemer

ii) effektiviteten af IKT-systemer

iii) forebyggelse af IKT-kapacitetsmangler.

2. De i stk. 1 omhandlede procedurer for styring af kapacitet og ydeevne skal sikre, at finansielle enheder træffer foranstaltninger, som er passende til at tage højde for IKT-systemer med lange eller komplekse udbud eller for ressourceintensive godkendelsesprocesser eller IKT-systemer.

Artikel 10

Sårbarheds- og korrektionsstyring

1. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder procedurer for sårbarhedsstyring.

2. De i stk. 1 omhandlede procedurer for sårbarhedsstyring skal:

a) identificere og opdatere relevante og pålidelige informationsressourcer med henblik på at skabe og opretholde bevidsthed om sårbarheder

b) sikre udøvelse af automatiseret sårbarhedsscanning og automatiserede vurderinger af IKT-aktiver. hvorved hyppigheden og omfanget af disse aktiviteter skal stå i rimeligt forhold til den klassificering, der er fastlagt i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og IKT-aktivets overordnede risikoprofil

c) efterprøve, om:

i) tredjepartsudbydere af IKT-tjenester håndterer sårbarheder, som er forbundet med de IKT-tjenester, der leveres til den pågældende finansielle enhed

ii) disse tjenesteudbydere aflægger rettidig rapport til den finansielle enhed som minimum om de kritiske sårbarheder, statistikker og tendenser

d) spore brugen af:

i) tredjepartsbiblioteker, herunder open source-biblioteker, der anvendes af de IKT-tjenester, der understøtter kritiske eller vigtige funktioner

ii) IKT-tjenester, som den finansielle enhed selv har udviklet, eller som en tredjepartsudbyder af IKT-tjenester har tilpasset eller udviklet specifikt til den pågældende finansielle enhed

e) indføre procedurer for ansvarlig offentliggørelse af sårbarheder til kunder, modparter og til offentligheden

f) prioritere ibrugtagning af korrektioner og andre afbødende foranstaltninger med henblik på at afhjælpe de konstaterede sårbarheder

g) overvåge og efterprøve udbedring af sårbarheder

h) kræve registrering af alle detekterede sårbarheder, der har indvirkning på IKT-systemer, og overvågning af deres afvikling.

Med henblik på litra b) foretager finansielle enheder den automatiserede sårbarhedsscanning og de automatiserede vurderinger af IKT-aktiver for de IKT-aktiver, der understøtter kritiske eller vigtige funktioner, mindst en gang om ugen.

Med henblik på litra c) anmoder finansielle enheder tredjepartsudbydere af IKT-tjenester om at undersøge de relevante sårbarheder, fastslå de grundlæggende årsager og iværksætte passende afbødende tiltag.

Med henblik på litra d) overvåger finansielle enheder, når det er relevant, i samarbejde med den pågældende tredjepart-sudbyder af IKT-tjenester, udgaven og eventuelle ajourføringer af tredjepartsbibliotekerne. I tilfælde af brugsklare IKT-aktiver eller komponenter af IKT-aktiver (standardaktiver eller -komponenter), der anskaffes og anvendes i forbindelse med driften af IKT-tjenester, der ikke understøtter kritiske eller vigtige funktioner, sporer finansielle enheder så vidt muligt brugen af tredjepartsbiblioteker, herunder open source-biblioteker.

Med henblik på litra f) tager finansielle enheder hensyn til sårbarhedens kritiske betydning, den klassificering, der er fastlagt i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og risikoprofilen for de IKT-aktiver, der er berørt af de identificerede sårbarheder.

3. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder procedurer for korrektionsstyring.

4. De i stk. 3 omhandlede procedurer for korrektionsstyring skal:

a) så vidt muligt identificere og evaluere tilgængelige software- og hardwarekorrektioner og -opdateringer ved hjælp af automatiserede værktøjer

b) identificere nødprocedurer for korrektion og opdatering af IKT-aktiver

c) teste og ibrugtage de software- og hardwarekorrektioner og -opdateringer, der er omhandlet i artikel 8, stk. 2, litra b), nr. v), vi) og vii)

d) fastsætte frister for installation af software- og hardwarekorrektioner og -opdateringer samt fejlafhjælpnings-procedurer, hvis disse frister ikke kan overholdes.

Artikel 11

Data- og systemsikkerhed

1. Som led i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører finansielle enheder en procedure for data- og systemsikkerhed.

2. Den procedure for data- og systemsikkerhed, der er omhandlet i stk. 1, skal indeholde alle følgende elementer vedrørende datasikkerhed og IKT-systemsikkerhed i overensstemmelse med den klassificering, der er fastlagt i henhold til artikel 8, stk. 1, i forordning (EU) 2022/2554:

a) de adgangsbegrænsninger, der er omhandlet i denne forordnings artikel 21, og som understøtter beskyttelseskravene for hver klassifikationsgrad

b) identifikation af en sikker konfigurationsstandard for IKT-aktiver, der minimerer disse IKT-aktivers eksponering mod cybertrusler, og foranstaltninger til regelmæssig kontrol af, at disse standarder anvendes på en effektiv måde

c) identifikation af sikkerhedsforanstaltninger til sikring af, at der kun installeres godkendt software i IKT-systemer og endpoint-enheder

d) identifikation af sikkerhedsforanstaltninger over for ondsindede koder

e) identifikation af sikkerhedsforanstaltninger til sikring af, at kun autoriserede datalagringsmedier, -systemer og endpoint-enheder anvendes til at overføre og lagre den finansielle enheds data

f) følgende krav til sikring af brugen af bærbare endpoint-enheder og private ikkebærbare endpoint-enheder:

   i) kravet om at anvende en behandlingsløsning til fjernstyring af endpoint-enheder og fjernsletning af den finansielle enheds data

   ii) kravet om at anvende sikkerhedsmekanismer, der ikke kan ændres, fjernes eller omgås af medarbejdere eller tredjepartsudbydere af IKT-tjenester på en uautoriseret måde

   iii) kravet om kun at anvende aftagelige datalagringsenheder, hvis den resterende IKT-risiko forbliver inden for den finansielle enheds risikotoleranceniveau, jf. artikel 3, litra a), første afsnit

g) proceduren for sikker sletning af data, der findes i den finansielle enheds lokaler eller lagres eksternt, og som den finansielle enhed ikke længere behøver at indsamle eller lagre

h) processen for sikker bortskaffelse eller demontering af datalagringsenheder, der findes i den finansielle enheds lokaler eller opbevares eksternt, og som indeholder fortrolige oplysninger

i) identifikation og gennemførelse af sikkerhedsforanstaltninger til forebyggelse af datatab og -lækage i systemer og endpoint-enheder

j) gennemførelse af sikkerhedsforanstaltninger til sikring af, at telearbejde og brugen af private endpoint-enheder ikke har en negativ indvirkning på den finansielle enheds IKT-sikkerhed

k) for IKT-aktiver eller -tjenester, der drives af en tredjepartsudbyder af IKT-tjenester, identifikation og gennemførelse af krav med henblik på opretholdelse af digital operationel modstandsdygtighed i overensstemmelse med resultaterne af dataklassificeringen og IKT-risikovurderingen.

Med henblik på litra b) skal den sikre konfigurationsstandard, der er omhandlet i nævnte litra, tage hensyn til førende praksis og passende teknikker, der er fastsat i de standarder, der er defineret i artikel 2, nr. (1), i forordning (EU) nr. 1025/2012.

Med henblik på litra k) tager finansielle enheder hensyn til følgende:

a) gennemførelsen af leverandørens anbefalede indstillinger for de elementer, der drives af den finansielle enhed

b) en klar fordeling af roller og ansvarsområder inden for informationssikkerhed mellem den finansielle enhed og tredjepartsudbyderen af IKT-tjenester i overensstemmelse med princippet om den finansielle enheds fulde ansvar for dennes tredjepartsudbyder af IKT-tjenester, jf. artikel 28, stk. 1, litra a), i forordning (EU) 2022/2554, og for finansielle enheder som omhandlet i nævnte forordnings artikel 28, stk. 2, og i overensstemmelse med den finansielle enheds politik for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner

c) behovet for at sikre og opretholde tilstrækkelige kompetencer i den finansielle enhed med hensyn til forvaltning af og sikkerheden i den anvendte tjeneste

d) tekniske og organisatoriske foranstaltninger til minimering af de risici, der er forbundet med den infrastruktur, som tredjepartsudbyderen af IKT-tjenester anvender til sine IKT-tjenester, idet der tages hensyn til førende praksis og standarder som defineret i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012.

Artikel 12

Logføring

1. Som led i de sikkerhedsforanstaltninger, der forhindrer indtrængen og datamisbrug, udvikler, dokumenterer og gennemfører finansielle enheder logføringsprocedurer, -protokoller og -værktøjer.

2. De logføringsprocedurer, -protokoller og -værktøjer, der er omhandlet i stk. 1, skal indeholde alle følgende:

a) identifikation af de hændelser, der skal logføres, opbevaringsperioden for logfilerne og foranstaltningerne til sikring og håndtering af logdataene, idet der tages hensyn til formålet med oprettelsen af logfilerne

b) tilpasning af logfilernes detaljeringsgrad i forhold til deres formål og anvendelse for at muliggøre effektiv detektion af anormale aktiviteter som omhandlet i artikel 24

c) kravet om at logføre hændelser i forbindelse med alle følgende:

   i) logisk og fysisk adgangskontrol, jf. artikel 21, og identitetsstyring

   ii) kapacitetsstyring

   iii) styring af ændringer

   iv) IKT-operationer, heriblandt IKT-systemaktiviteter

   v) aktiviteter forbundet med netværkstrafik, herunder IKT-nettets ydeevne

d) foranstaltninger til beskyttelse af logføringssystemer og logføring af oplysninger til forebyggelse af manipulation af, sletning af og uautoriseret adgang til data, som er inaktive, under overførsel og, når det er relevant, i brug

e) foranstaltninger til detektion af svigt i logføringssystemer

f) uden at det berører eventuelle gældende reguleringsmæssige krav i henhold til EU-retten eller national ret, synkronisering af urene i hver af den finansielle enheds IKT-systemer efter en dokumenteret pålidelig kilde til referencetid.

Med henblik på litra a) fastsætter finansielle enheder opbevaringsperioden, idet de tager hensyn til forretnings- og informationssikkerhedsmålene, årsagen til registreringen af hændelsen i logfilerne og resultaterne af IKT-risikovurderingen.

Afdeling 6

Netsikkerhed

Artikel 13

Styring af netsikkerhed

Som led i de sikkerhedsforanstaltninger, der garanterer netsikkerheden mod indtrængen og datamisbrug, udvikler, dokumenterer og gennemfører finansielle enheder politikker, procedurer, protokoller og værktøjer for styring af netsikkerhed, herunder alle følgende:

a) adskillelse og segmentering af IKT-systemer og -netværk under hensyntagen til:

   i) hvor kritisk eller vigtig den funktion, som disse IKT-systemer og -netværk understøtter, er

   ii) den klassificering, der er fastlagt i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554

   iii) den samlede risikoprofil for IKT-aktiver, der anvender disse IKT-systemer og -netværk

b) dokumentation for alle den finansielle enheds netværksforbindelser og datastrømme

c) anvendelse af et særskilt og dertil indrettet netværk til administration af IKT-aktiver

d) identifikation og gennemførelse af netadgangskontroller, som skal forebygge og detektere forbindelser til den finansielle enheds netværk ved hjælp af en uautoriseret enhed eller et uautoriseret system eller ethvert endpoint, der ikke opfylder den finansielle enheds sikkerhedskrav

e) kryptering af netværksforbindelser, der passerer gennem virksomhedsnetværk, offentlige netværk, indenlandske netværk, tredjeparters netværk og trådløse net, til de anvendte kommunikationsprotokoller, idet der tages hensyn til resultaterne af den godkendte dataklassificering, resultaterne af IKT-risikovurderingen og krypteringen af de netforbindelser, der er omhandlet i artikel 6, stk. 2

f) udformningen af netværk i overensstemmelse med de krav til IKT-sikkerhed, der er fastsat af den finansielle enhed, idet der tages hensyn til førende praksis for at sikre fortroligheden, integriteten og tilgængeligheden af netværket

g) sikring af netværkstrafikken mellem de interne netværk og internettet og andre eksterne forbindelser

h) identifikation af roller og ansvarsområder og trin i forbindelse med specifikation, gennemførelse, godkendelse, ændring og revision af firewallregler og forbindelsesfiltre

i) udførelsen af gennemgange af netarkitekturen og af udformningen af netsikkerheden en gang om året, og regelmæssigt for mikrovirksomheder, med henblik på at identificere potentielle sårbarheder

j) foranstaltninger til midlertidig isolering, hvis det er nødvendigt, af delnet og af netværkskomponenter og -udstyr

k) gennemførelse af en sikker konfigurationsstandard for alle netværkskomponenter og hærdning af netværket og netværksudstyr i overensstemmelse med eventuelle leverandørinstruktioner, hvis det er relevant, standarder som defineret i artikel 2, nr. (1), i forordning (EU) nr. 1025/2012, og førende praksis

l) procedurer, som skal begrænse, låse og afslutte system- og fjernsessioner efter en bestemt periode uden aktivitet

m) for aftaler om netværkstjenester:

   i) identifikation og specificering af foranstaltninger vedrørende IKT og informationssikkerhed, serviceniveauer og styringskrav til alle netværkstjenester

   ii) om disse tjenesteydelser leveres af en koncernintern udbyder af IKT-tjenester eller af tredjepartsudbydere af IKT-tjenester.

Med henblik på litra h) foretager finansielle enheder regelmæssigt en gennemgang af firewallregler og forbindelsesfiltre i overensstemmelse med den klassificering, der er fastlagt i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og den overordnede risikoprofil for de involverede IKT-systemer. For IKT-systemer, der understøtter kritiske eller vigtige funktioner, efterprøver finansielle enheder mindst hver sjette måned, at de eksisterende firewallregler og forbindelsesfiltre er tilstrækkelige.

Artikel 14

Sikring af oplysninger, som er under overførsel

1. Som led i de sikkerhedsforanstaltninger, der bevarer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, udvikler, dokumenterer og gennemfører finansielle enheder politikker, procedurer, protokoller og værktøjer til beskyttelse af oplysninger, som er under overførsel. Finansielle enheder sikrer navnlig følgende:

a) tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, som er under overførsel på nettet, og fastlæggelse af procedurer til vurdering af overholdelsen af disse krav

b) forebyggelse og detektion af datalækager og sikker overførsel af oplysninger mellem den finansielle enhed og eksterne parter

c) at der foretages gennemførelse, dokumentation og regelmæssig revision af krav om fortrolighed eller hemmeligholdelsesordninger, der afspejler den finansielle enheds behov for beskyttelse af oplysninger til både den finansielle enheds og tredjeparters personale.

2. Finansielle enheder udformer de i stk. 1 omhandlede politikker, procedurer, protokoller og værktøjer til beskyttelse af oplysninger, som er under overførsel, på grundlag af resultaterne af den godkendte dataklassificering og IKT-risikovurderingen.

Afdeling 7

Styring af IKT-projekter og -ændringer

Artikel 15

Styring af IKT-projekter

1. Som led i de sikkerhedsforanstaltninger, der bevarer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data udvikler, dokumenterer og gennemfører finansielle enheder en politik for IKT-projektstyring.

2. Den i stk. 1 omhandlede politik for IKT-projektstyring skal præcisere de elementer, der sikrer en effektiv styring af de IKT-projekter, som har tilknytning til anskaffelse, vedligeholdelse og, hvis det er relevant, udvikling af den finansielle enheds IKT-systemer.

3. Den i stk. 1 omhandlede politik for IKT-projektstyring skal indeholde alt følgende:

a) mål for IKT-projekter

b) styring IKT-projekter, herunder roller og ansvarsområder

c) planlægning, tidsramme og trin forbindelse med IKT-projekter

d) risikovurdering af IKT-projekter

e) relevante milepæle

f) krav til styring af ændringer

g) test af alle krav, herunder sikkerhedskrav, og den respektive godkendelsesproces, når et IKT-system tages i brug i produktionsmiljøet.

4. Den politik for IKT-projektstyring, der er omhandlet i stk. 1, skal sikre en sikker gennemførelse af IKT-projekter gennem tilvejebringelse af de nødvendige oplysninger og den nødvendige ekspertise fra det eller de erhvervsområder, som IKT-projektet har indvirkning på.

5. I overensstemmelse med den risikovurdering af IKT-projekter, der er omhandlet i stk. 3, litra d), skal den i stk. 1 omhandlede politik for IKT-projektstyring fastsættes, at oprettelse af og fremskridt med IKT-projekter, som har indvirkning på den finansielle enheds kritiske eller vigtige funktioner og de dermed forbundne risici, indberettes til ledelsesorganet som følger:

a) individuelt eller samlet, afhængigt af IKT-projekternes betydning og størrelse

b) regelmæssigt og, hvis det er nødvendigt, på et hændelsesbaseret grundlag.

Artikel 16

Anskaffelse, udvikling og vedligeholdelse af IKT-systemer

1. Som led i de sikkerhedsforanstaltninger, der bevarer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, udvikler, dokumenterer og gennemfører finansielle enheder en politik for anskaffelse, udvikling og vedligeholdelse af IKT-systemer. Denne politik skal:

a) identificere sikkerhedspraksis og -metoder i forbindelse med anskaffelse, udvikling og vedligeholdelse af IKT-systemer

b) indeholde krav om, at følgende identificeres:

   i) tekniske specifikationer og IKT-tekniske specifikationer som defineret i artikel 2, nr. 4) og 5), i forordning (EU) nr. 1025/2012

   ii) krav vedrørende anskaffelse, udvikling og vedligeholdelse af IKT-systemer med særligt fokus på krav til IKT-sikkerhed og godkendelse heraf meddelt af den relevante forretningsfunktion og ejeren af IKT-aktiverne i overensstemmelse med den finansielle enheds interne ledelsesordninger

c) præcisere foranstaltninger til at mindske risikoen for utilsigtet ændring eller forsætlig manipulation af IKT-systemer i forbindelse med udviklingen, vedligeholdelsen og ibrugtagningen af disse IKT-systemer i produktionsmiljøet.

2. Finansielle enheder udvikler, dokumenterer og gennemfører en procedure for anskaffelse, udvikling og vedligeholdelse af IKT-systemer med henblik på test og godkendelse af alle IKT-systemer forud for deres anvendelse og efter vedligeholdelse i overensstemmelse med artikel 8, stk. 2, litra b), nr. v), vi) og vii). Testniveauet skal stå i rimeligt forhold til den kritiske betydning af de pågældende forretningsprocedurer og IKT-aktiver. Testen skal udformes med henblik på at efterprøve, om nye IKT-systemer er tilstrækkelige, således at de kan fungere efter hensigten, herunder kvaliteten af den internt udviklede software.

Centrale modparter skal ud over kravene i første afsnit, og alt efter hvad der er relevant, inddrage følgende i udformningen og gennemførelsen af den test, der er omhandlet i første afsnit:

a) clearingmedlemmer og kunder

b) interoperable centrale modparter

c) andre interessenter.

Værdipapircentraler skal ud over kravene i første afsnit, og alt efter hvad der er relevant, inddrage følgende i udformningen og gennemførelsen af den test, der er omhandlet i første afsnit:

a) brugere

b) udbydere af kritiske hjælpeprogrammer og tjenesteydelser

c) andre værdipapircentraler

d) andre markedsinfrastrukturer

e) andre institutter, med hvilke værdipapircentraler har angivet indbyrdes afhængighed i deres politik for driftsstabilitet.

3. Den i stk. 2 omhandlede procedure skal omfatte resultaterne af gennemgangene af kildekoder, som omfatter både statisk og dynamisk test. Nævnte test skal omfatte sikkerhedstest af interneteksponerede systemer og applikationer i overensstemmelse med artikel 8, stk. 2, litra b), nr. v), vi) og vii). Finansielle enheder skal:

a) konstatere og analysere sårbarheder og anomalier i kildekoden

b) vedtage en handlingsplan for at afhjælpe disse sårbarheder og anomalier

c) overvåge gennemførelsen af denne handlingsplan.

4. Proceduren i stk. 2 skal omfatte sikkerhedstest af softwarepakker senest i integrationsfasen i overensstemmelse med artikel 8, stk. 2, litra b), nr. v), vi) og vii).

5. For proceduren i artikel 2 skal følgende fastsættes.

a) ikkeproduktionsmiljøer lagrer kun anonymiserede, pseudonymiserede eller tilfældige produktionsdata

b) finansielle enheder skal beskytte integriteten og fortroligheden af data i ikkeproduktionsmiljøer.

6. Uanset stk. 5 kan det for den i stk. 2 omhandlede procedure fastsættes, at produktionsdata kun lagres med henblik på specifikke test, i begrænsede perioder og efter godkendelse meddelt af den relevante funktion og rapportering af sådanne specifikke test til IKT-risikostyringsfunktionen.

7. Den i stk. 2 omhandlede procedure skal omfatte gennemførelsen af kontroller for at beskytte integriteten af den kildekode for IKT-systemer, der er udviklet internt eller af en tredjepartsudbyder af IKT-tjenester og leveret til den finansielle enhed af en tredjepartsudbyder af IKT-tjenester.

8. Den i stk. 2 omhandlede procedure skal sikre, at proprietær software og, hvis det er muligt, den kildekode, der leveres af tredjepartsudbydere af IKT-tjenester eller kommer fra open source-projekter, skal analyseres og testes i overensstemmelse med stk. 3, inden de tages i brug i produktionsmiljøet.

9. Stk. 1-8 finder også anvendelse på IKT-systemer, der udvikles eller forvaltes af brugere uden for IKT-funktionen ved anvendelse af en risikobaseret tilgang.

Artikel 17

Styring af IKT-ændringer

1. Som led i de sikkerhedsforanstaltninger, der skal bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, inkluderer finansielle enheder i de procedurer for styring af IKT-ændringer, der er omhandlet i artikel 9, stk. 4, litra e), i forordning (EU) 2022/2554, med henblik på alle ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, alle følgende elementer:

a) en efterprøvning af, om kravene til IKT-sikkerhed er opfyldt

b) mekanismer, der skal sikre, at de funktioner, der godkender ændringer, og de funktioner, der har ansvar for at anmode om og gennemføre disse ændringer, er uafhængige

c) en klar beskrivelse af roller og ansvarsområder for at sikre, at:

   i) ændringer er nærmere angivet og planlagt

   ii) der er udformet en passende overgang

   iii) ændringerne testes og færdiggøres på en kontrolleret måde

   iv) der er en effektiv kvalitetssikring

d) dokumentation og meddelelse af oplysninger om ændringer, herunder:

   i) formål med og omfang af ændringen

   ii) tidsplanen for gennemførelsen af ændringen

   iii) de forventede resultater

e) angivelse af nødprocedurer og ansvarsområder, herunder procedurer og ansvarsområder i forbindelse med afbrydelse af ændringer eller genopretning efter ændringer, hvis gennemførelse ikke var vellykket

f) procedurer, protokoller og værktøjer til håndtering af hasteændringer, der giver tilstrækkelige garantier

g) procedurer, der skal sikre dokumentation, reevaluering, vurdering og godkendelse af hasteændringer efter deres gennemførelse, herunder arbejdsgange og korrektioner

h) identifikation af en ændrings potentielle indvirkning på eksisterende IKT-sikkerhedsforanstaltninger og en vurdering af, om en sådan ændring kræver vedtagelse af yderligere IKT-sikkerhedsforanstaltninger.

2. Når centrale modparter og værdipapircentraler har foretaget væsentlige ændringer i deres IKT-systemer, skal de lade deres IKT-systemer underkaste strenge test ved at simulere stressede forhold.

Centrale modparter skal, alt efter hvad der er relevant, inddrage følgende i udformningen og gennemførelsen af den test, der er omhandlet i første afsnit:

a) clearingmedlemmer og kunder

b) interoperable centrale modparter

c) andre interessenter.

Værdipapircentraler skal, alt efter hvad der er relevant, inddrage følgende i udformningen og gennemførelsen af den test, der er omhandlet i første afsnit:

a) brugere

b) udbydere af kritiske hjælpeprogrammer og tjenesteydelser

c) andre værdipapircentraler

d) andre markedsinfrastrukturer

e) andre institutter, med hvilke værdipapircentraler har angivet indbyrdes afhængighed i deres politik for IKT-driftsstabilitet.

Afdeling 8

Artikel 18

Fysisk og miljømæssig sikkerhed

1. Som led i de sikkerhedsforanstaltninger, der skal bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data præciserer, dokumenterer og gennemfører finansielle enheder en politik for fysisk og miljømæssig sikkerhed. Finansielle enheder udformer denne politik på grundlag af cybertrusselsbilledet i overensstemmelse med den klassificering, der er fastsat i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og på grundlag af den overordnede risikoprofil for IKT-aktiver og tilgængelige informationsaktiver.

2. Den i stk. 1 omhandlede politik for fysisk og miljømæssig sikkerhed skal indeholde alt følgende:

a) en henvisning til den del af politikken for kontrol med rettigheder vedrørende adgangsforvaltning, der er omhandlet i artikel 21, litra g), første afsnit

b) foranstaltninger til beskyttelse mod angreb, ulykker og miljøtrusler og -farer, den finansielle enheds lokaler, datacentre og sensitive udpegede områder, som er angivet af den finansielle enhed, og hvor der ligger IKT-aktiver og informationsaktiver

c) foranstaltninger til sikring af IKT-aktiver, både i og uden for den finansielle enheds lokaler, idet der tages hensyn til resultaterne af IKT-risikovurderingen af de relevante IKT-aktiver

d) foranstaltninger til sikring af tilgængeligheden, autenticiteten, integriteten og fortroligheden af den finansielle enheds IKT-aktiver, informationsaktiver og fysiske enheder til adgangskontrol ved hjælp af passende vedligeholdelse

e) foranstaltninger til sikring af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, herunder:

   i) en klar skrivebordspolitik for dokumenter

   ii) en klar skærmpolitik for udstyr til informationsbehandling.

Med henblik på litra b) skal foranstaltningerne til beskyttelse mod miljøtrusler og -farer stå i rimeligt forhold til betydningen af lokalerne, datacentrene, de sensitive udpegede områder og den kritiske betydning af de operationer eller IKT-systemer, der foretages og ligger deri.

Med henblik på litra c) skal politikken for fysisk og miljømæssig sikkerhed, der er omhandlet i stk. 1, indeholde foranstaltninger, som skal sikre passende beskyttelse af ikkeovervågede IKT-aktiver.

KAPITEL II

Politik for menneskelige ressourcer og adgangskontrol

Artikel 19

Politik for menneskelige ressourcer

Finansielle enheder inkluderer i deres politik for menneskelige ressourcer eller andre relevante politikker alle følgende IKT-sikkerhedsrelaterede elementer:

a) angivelse og tildeling af eventuelle specifikke IKT-sikkerhedsopgaver

b) krav til personalet i den finansielle enhed og hos tredjepartsudbydere af IKT-tjenester, der anvender eller har adgang til den finansielle enheds IKT-aktiver, om:

i) at være bekendt med og overholde den finansielle enheds IKT-sikkerhedspolitikker, -procedurer og -protokoller

ii) at være bekendt med de indberetningskanaler, som den finansielle enhed har indført for at detektere anormal adfærd, herunder, hvis det er relevant, de indberetningskanaler, der er indført i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 ([11])

iii) ved ansættelsesforholdets ophør at tilbagelevere alle IKT-aktiver og materielle informationsaktiver, som de er i besiddelse af, og som tilhører den finansielle enhed, til den finansielle enhed.

Artikel 20

Identitetsstyring

1. Som led i deres kontrol med rettigheder vedrørende adgangsforvaltning udvikler, dokumenterer og gennemfører finansielle enheder politikker og procedurer for identitetsstyring, der sikrer entydig identificering og autentificering af fysiske personer og systemer, der har adgang til de finansielle enheders oplysninger, for at muliggøre tildeling af brugeradgangsrettigheder i overensstemmelse med artikel 21.

2. De i stk. 1 omhandlede procedurer og protokoller for identitetsstyring skal indeholde alt følgende:

a) uden at det berører artikel 21, litra c), første afsnit, tildeles hver enkelt medarbejder i den finansielle enhed eller medarbejdere hos tredjepartsudbydere af IKT-tjenester, der har adgang til den finansielle enheds informationsaktiver og IKT-aktiver, en unik identitet svarende til en unik brugerkonto

b) en proces for livscyklusstyring af identiteter og konti, som styrer oprettelse, ændring, gennemgang og opdatering, midlertidig deaktivering og afslutning af alle konti.

Med henblik på litra a) fører finansielle enheder fortegnelser over alle identitetstildelinger. Disse fortegnelser opbevares efter en omstrukturering af den finansielle enhed eller efter kontraktforholdets ophør, uden at dette berører de krav om opbevaring, der er fastsat i gældende EU-ret og national ret.

Med henblik på litra b) anvender finansielle enheder, hvis det er muligt og hensigtsmæssigt, automatiserede løsninger til processen for livscyklusidentitetsstyring.

Artikel 21

Adgangskontrol

Som led i deres kontrol med rettigheder vedrørende adgangsforvaltning udvikler, dokumenterer og gennemfører finansielle enheder en politik, der indeholder alt følgende:

a) tildeling af adgangsrettigheder til IKT-aktiver på grundlag af need to know-princippet, need to use-princippet og least privilege-princippet, herunder fjernadgang og adgang i hastetilfælde

b) adskillelse af opgaver, der er udformet med henblik på at forhindre uberettiget adgang til kritiske data eller forhindre tildeling af kombinationer af adgangsrettigheder, der kan anvendes til at omgå kontroller

c) en bestemmelse om brugeransvar, idet brugen af generiske og delte brugerkonti begrænses så vidt muligt og det sikres, at brugerne til enhver tid kan identificeres med hensyn til de handlinger, der udføres i IKT-systemerne

([11]) Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (EUT L 305 af 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) en bestemmelse om begrænsning af adgangen til IKT-aktiver, der fastsætter kontrolforanstaltninger og værktøjer, som skal forhindre uautoriseret adgang

e) procedurer for kontoforvaltning med henblik på tildeling, ændring eller tilbagekaldelse af adgangsrettigheder for brugerkonti og generiske konti, herunder generiske administratorkonti, som omfatter bestemmelser om alt følgende:

   i) tildeling af roller og ansvarsområder for tildeling, gennemgang og tilbagekaldelse af adgangsrettigheder

   ii) tildeling af privilegeret adgang, hasteadgang og administratoradgang på need to know-basis eller ad hoc-basis for alle IKT-systemer

   iii) øjeblikkelig inddragelse af adgangsretten ved ansættelsesforholdets ophør, eller når adgangen ikke længere er nødvendig

   iv) ajourføring af adgangsrettigheder, når ændringer er nødvendige, og mindst en gang om året for alle IKT-systemer, bortset fra IKT-systemer, der understøtter kritiske eller vigtige funktioner, og mindst hver sjette måned for IKT-systemer, der understøtter kritiske eller vigtige funktioner.

f) autentificeringsmetoder, herunder alle følgende:

   i) anvendelse af autentificeringsmetoder, der svarer til den klassificering, der er fastsat i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og til IKT-aktivernes overordnede risikoprofil og under hensyntagen til førende praksis

   ii) anvendelse af stærke autentificeringsmetoder i overensstemmelse med førende praksis og teknikker vedrørende fjernadgang til den finansielle enheds netværk, privilegeret adgang, adgang til IKT-aktiver, der understøtter kritiske eller vigtige funktioner, eller IKT-aktiver, der er offentligt tilgængelige

g) foranstaltninger til fysisk adgangskontrol, herunder:

   i) identificering og logføring af fysiske personer, der har tilladelse til at få adgang til lokaler, datacentre og sensitive udpegede områder, som er angivet af den finansielle enhed, og hvor der ligger IKT-aktiver og informationsaktiver

   ii) tildeling af fysiske adgangsrettigheder til kritiske IKT-aktiver udelukkende til autoriserede personer i overensstemmelse med need to know-princippet og least privilege-princippet og på ad hoc-basis

   iii) overvågning af fysisk adgang til lokaler, datacentre og sensitive udpegede områder, som er angivet af den finansielle enhed, og hvor der både ligger IKT-aktiver og informationsaktiver

   iv) gennemgang af fysiske adgangsrettigheder for at sikre, at unødvendige adgangsrettigheder straks tilbagekaldes.

Med henblik på litra e), nr. i), fastsætter finansielle enheder opbevaringsperioden, idet de tager hensyn til forretnings- og informationssikkerhedsmålene, årsagerne til registreringen af hændelsen i logfilerne og resultaterne af IKT-risikovurderingen.

Med henblik på litra e), nr. ii), anvender finansielle enheder, når det er muligt, særlige konti til varetagelse af administrative opgaver vedrørende IKT-systemer. Hvis det er muligt og hensigtsmæssigt, anvender finansielle enheder automatiserede løsninger til forvaltning af privilegeret adgang.

Med henblik på litra g), nr. i), skal identifikationen og logføringen stå i rimeligt forhold til betydningen af lokalerne, datacentrene, de sensitive udpegede områder og den kritiske betydning af de operationer eller IKT-systemer, der foretages og ligger deri.

Med henblik på litra g), nr. iii), skal overvågningen stå i rimeligt forhold til den klassificering, der er fastlagt i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2022/2554, og den kritiske betydning af det område, hvortil der opnås adgang.

KAPITEL III

Ddetektion af og reaktion på IKT-relaterede hændelser

Artikel 22

Politik for styring af IKT-relaterede hændelser

Som led i mekanismerne til detektion af anormale aktiviteter, herunder problemer med IKT-netværkets ydeevne og IKT-relaterede hændelser, udvikler, dokumenterer og gennemfører finansielle enheder en politik for IKT-relaterede hændelser, i medfør af hvilken de skal:

a) dokumentere processen for styring af IKT-relaterede hændelser som omhandlet i artikel 17, i forordning (EU) 2022/2554

b) udarbejde en liste over relevante kontakter, som har interne funktioner, og eksterne interessenter, der er direkte involveret i sikkerheden i forbindelse med IKT-operationer, herunder om:

   i) detektion og overvågning af cybertrusler

   ii) detektion af anormale aktiviteter

   iii) sårbarhedsstyring

c) indføre, gennemføre og drive tekniske, organisatoriske og operationelle mekanismer, som skal understøtte processen for styring af IKT-relaterede hændelser, herunder mekanismer, der gør det muligt straks at detektere anormale aktiviteter og anomal adfærd i overensstemmelse med denne forordnings artikel 23

d) opbevare alt bevismateriale vedrørende IKT-relaterede hændelser i en periode, der ikke må være længere end, hvad der er nødvendigt til de formål, hvortil dataene indsamles, og som står i rimeligt forhold til de berørte forretningsfunktioners kritiske betydning, understøttende processer samt IKT-aktiver og informationsaktiver i overensstemmelse med artikel 15 i Kommissionens delegerede forordning (EU) 2024/1772 ([12]) og med eventuelle gældende opbevaringskrav i henhold til EU-retten

e) indføre og gennemføre mekanismer til analyse af væsentlige eller tilbagevendende IKT-relaterede hændelser og mønstre med hensyn til antal og forekomst af IKT-relaterede hændelser.

Med henblik på litra d) opbevarer finansielle enheder den dokumentation, der er omhandlet i nævnte litra, på en sikker måde.

Artikel 23

Detektion af anormale aktiviteter og kriterier for detektion af og reaktion af IKT-relaterede hændelser

1. Finansielle enheder tildeler klare roller og ansvarsområder med henblik på effektivt at detektere og reagere på IKT-relaterede hændelser og anormale aktiviteter.

2. Mekanismen til omgående detektion af anormale aktiviteter, herunder problemer med IKT-netværkets ydeevne og IKT-relaterede hændelser, jf. artikel 10, stk. 1, i forordning (EU) 2022/2554, skal gøre det muligt for finansielle enheder at:

a) indsamle, overvåge og analysere alle følgende:

   i) interne og eksterne faktorer, herunder som minimum de logfiler, der er indsamlet i overensstemmelse med denne forordnings artikel 12, oplysninger fra forretnings- og IKT-funktioner og eventuelle problemer indberettet af den finansielle enheds brugere

   ii) potentielle interne og eksterne cybertrusler, idet der tages hensyn til scenarier, der almindeligvis anvendes af trusselsaktører og scenarier baseret på trusselsefterretningsaktiviteter

([12]) Kommissionens delegerede forordning (EU) 2024/1772 af 13. marts 2024 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer kriterierne for klassificering af IKT-relaterede hændelser og cybertrusler, fastsætter væsentlighedstærskler og præciserer de nærmere oplysninger om indberetninger af større hændelser (EUT L, 2024/1772 af 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) underretninger om IKT-relaterede hændelser fra en tredjepartsudbyder af IKT-tjenester i den finansielle enhed, som detekteres i IKT-systemerne og -netværkene hos tredjepartsudbyderen af IKT-tjenester, og som kan påvirke den finansielle enhed

b) identificere anormale aktiviteter og anormal adfærd og indføre værktøjer, der genererer advarsler om anormale aktiviteter og anormal adfærd, som minimum for IKT-aktiver og informationsaktiver, der understøtter kritiske eller vigtige funktioner

c) prioritere de i litra b) omhandlede varslinger, således at de detekterede IKT-relaterede hændelser kan håndteres inden for den forventede afviklingstid, som angivet af finansielle enheder, både i og uden for arbejdstiden

d) registrere, analysere og evaluere alle relevante oplysninger om alle anormale aktiviteter og anormal adfærd automatisk eller manuelt.

Med henblik på litra b) skal de i nævnte litra omhandlede værktøjer indeholde de værktøjer, der giver automatiske varslinger baseret på forud fastsatte regler med henblik på at konstatere anomalier, der har indvirkning på fuldstændigheden og integriteten af datakilderne eller indsamlingen af logfiler.

3. Finansielle enheder beskytter enhver registrering af de anormale aktiviteter mod ulovlige indgreb og uautoriseret adgang til data, som er inaktive, under overførsel og, når det er relevant, i brug.

4. Finansielle enheder skal logføre alle relevante oplysninger for hver detekteret anormal aktivitet, som gør det muligt at

a) identificere dato og klokkeslæt, hvor den anormale aktivitet fandt sted

b) identificere dato og klokkeslæt, hvor den anormale aktivitet blev detekteret

c) identificere typen af anormal aktivitet.

5. Finansielle enheder tager hensyn til alle følgende kriterier for at udløse de processer for detektion af og reaktion på IKT-relaterede hændelser, der er omhandlet i artikel 10, stk. 2, i forordning (EU) 2022/2554:

a) indikationer på, at ondsindede aktiviteter kan være blevet udført i et IKT-system eller -netværk, eller at et sådant IKT-system eller -netværk kan være blevet kompromitteret

b) datatab, som detekteres i forbindelse med tilgængeligheden, autenticiteten, integriteten og fortroligheden af data

c) detekteret negativ indvirkning på den finansielle enheds transaktioner og aktiviteter

d) IKT-systemer og netværk er ikke tilgængelige.

6. Med henblik på stk. 5 tager finansielle enheder også hensyn til de berørte tjenesters kritiske betydning.

KAPITEL IV

Styring af IKT-driftsstabilitet

Artikel 24

Komponenter i politikken for IKT-driftsstabilitet

1. Finansielle enheder inkluderer i deres politik for IKT-driftsstabilitet, jf. artikel 11, stk. 1, i forordning (EU) 2022/2554, alle følgende:

a) en beskrivelse af:

i) målene for politikken for IKT-driftsstabilitet, herunder samspillet mellem IKT og den overordnede driftsstabilitet, og idet der tages hensyn til resultaterne af den forretningskonsekvensanalyse (BIA), der er omhandlet i artikel 11, stk. 5, i forordning (EU) 2022/2554

ii) omfanget af ordningerne, -planerne, -procedurerne og -mekanismerne for IKT-driftsstabilitet, herunder begrænsninger og udelukkelser

iii) den tidsramme, der skal indgå i ordningerne, planerne, procedurerne og mekanismerne for IKT-driftsstabilitet

iv) kriterierne for aktivering og deaktivering af planer for IKT-driftsstabilitet, planer for IKT-indsats- og -genopretning samt krisekommunikationsplaner

b) bestemmelser om:

i) forvaltning og organisation med henblik på gennemførelse af politikken for IKT-driftsstabilitet, herunder roller, ansvarsområder og fejlafhjælpningsprocedurer, der sikrer, at der er tilstrækkelige ressourcer til rådighed

ii) samordning af planerne for IKT-driftsstabilitet og de overordnede planer for driftsstabilitet, der som minimum vedrører alle følgende:

1) potentielle svigtrelaterede scenarier, herunder de scenarier, der er omhandlet i denne forordnings artikel 26, stk. 2

2) genopretningsmål, der præciserer, at den finansielle enhed skal være i stand til at genoprette driften af sine kritiske eller vigtige funktioner efter forstyrrelser inden for et mål om genopretningstid og et genopretningspunkt

iii) udvikling af planer for IKT-driftsstabilitet i tilfælde af alvorlige driftsforstyrrelser som led i disse planer og prioritering af tiltag vedrørende IKT-driftsstabilitet ved anvendelse af en risikobaseret tilgang

iv) udvikling, test og gennemgang af planer for IKT-indsats- og -genopretning i overensstemmelse med denne forordnings artikel 25 og 26

v) gennemgang af effektiviteten af de gennemførte ordninger, planer, procedurer og mekanismer for IKT-driftsstabilitet i overensstemmelse med denne forordnings artikel 26

vi) samordning af politikken for IKT-driftsstabilitet med følgende:

1) den kommunikationspolitik, der er omhandlet i artikel 14, stk. 2, i forordning (EU) 2022/2554

2) de kommunikationstiltag og krisekommunikationstiltag, der er omhandlet i artikel 11, stk. 2, litra e), i forordning (EU) 2022/2554.

2. Foruden de i stk. 1 omhandlede krav sikrer centrale modparter, at deres politik for IKT-driftsstabilitet:

a) indeholder en maksimal genopretningstid for deres kritiske funktioner, som ikke overstiger 2 timer

b) tager hensyn til eksterne sammenkoblinger og indbyrdes afhængighed inden for de finansielle infrastrukturer, herunder markedspladser, der cleares af den centrale modpart, værdipapirafviklings- og betalingssystemer og kreditinstitutter, der anvendes af den centrale modpart eller en tilknyttet central modpart

c) indeholder krav om, at der er indført ordninger med henblik på at:

i) sikre stabiliteten af den centrale modparts kritiske eller vigtige funktioner på grundlag af katastrofescenarier

ii) vedligeholde et sekundært afviklingssted, der kan sikre stabilitet i den centrale modparts kritiske eller vigtige funktioner, og som er identisk med det primære anlæg

iii) vedligeholde eller opnå umiddelbar adgang til et sekundært forretningssted, således at personalet kan sikre tjenestens driftsstabilitet, hvis det primære forretningssted ikke er tilgængeligt

iv) tage hensyn til behovet for ekstra afviklingssteder, navnlig såfremt det primære og sekundære steds forskellige risikoprofiler ikke giver tilstrækkelig sikkerhed for, at den centrale modparts mål for driftsstabilitet vil blive opfyldt i alle scenarier.

Med henblik på litra a) afslutter centrale modparter under alle omstændigheder procedurer ved dagens afslutning og afvikler betalinger på det krævede tidspunkt og den krævede dag.

Med henblik på litra c), nr. i), skal de ordninger, der er omhandlet heri, omhandle tilgængeligheden af tilstrækkelige menneskelige ressourcer, den maksimale nedetid for kritiske funktioner og svigt samt genopretning på et sekundært afviklingssted.

Med henblik på litra c), nr. ii), skal det sekundære afviklingssted, der er omhandlet heri, have en geografisk risikoprofil, som er forskellig fra det primære afviklingssteds risikoprofil.

3. Foruden de i stk. 1 omhandlede krav sikrer værdipapircentraler, at deres politik for IKT-driftsstabilitet:

a) tager hensyn til eventuelle sammenkoblinger med og indbyrdes afhængighed mellem brugere, udbydere af kritiske hjælpeprogrammer og tjenester, andre værdipapircentraler og andre markedsinfrastrukturer

b) indeholder krav om, at deres ordninger for IKT-driftsstabilitet skal sikre, at målet om genopretningstid for deres kritiske eller vigtige funktioner ikke er længere end 2 timer.

4. Foruden de i stk. 1 omhandlede krav sørger markedspladser for, at deres politik for IKT-driftsstabilitet sikrer, at:

a) handelen kan genoptages inden for eller tæt på 2 timer efter en forstyrrende hændelse

b) den maksimale mængde data, der må gå tabt fra en hvilken som helst IT-tjeneste på markedspladsen efter en forstyrrende hændelse, er tæt på nul.

Artikel 25

Test af politikken for IKT-driftsstabilitet

1. Når finansielle enheder tester planerne for IKT-driftsstabilitet i overensstemmelse med artikel 11, stk. 6, i forordning (EU) 2022/2554, tager de hensyn til den finansielle enheds forretningskonsekvensanalyse (BIA) og den IKT-risikovurdering, der er omhandlet i nærværende forordnings artikel 3, stk. 1, litra b).

2. Finansielle enheder vurderer gennem test af deres i stk. 1 omhandlede planer for IKT-driftsstabilitet, om de er i stand til at sikre stabilitet i den finansielle enheds kritiske eller vigtige funktioner. Nævnte test skal:

a) udføres på grundlag af testscenarier, der simulerer potentielle forstyrrelser, herunder et passende sæt alvorlige, men plausible scenarier

b) omfatte test af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, hvis det er relevant

c) for finansielle enheder, som ikke er mikrovirksomheder, jf. artikel 11, stk. 6, andet afsnit, i forordning (EU) 2022/2554, indeholde omstillingsscenarier mellem primær IKT-infrastruktur til redundant kapacitet, sikkerhedskopier og redundante faciliteter

d) være udformet på en måde, der anfægter de antagelser, som planerne for driftsstabilitet er baseret på, herunder ledelsesordninger og krisekommunikationsplaner

e) indeholde procedurer til efterprøvning af, at de finansielle enheders personale, tredjepartsudbydere af IKT-systemer, IKT-systemer og IKT-tjenester er i stand til at reagere hensigtsmæssigt på de scenarier, som der i behørig grad er taget hensyn til i overensstemmelse med artikel 26, stk. 2.

Med henblik på litra a) inkluderer finansielle enheder altid de scenarier, der overvejes i forbindelse med udarbejdelsen af planerne for driftsstabilitet, i test.

Med henblik på litra b) tager finansielle enheder behørigt hensyn til scenarier, der er forbundet med insolvens eller svigt hos tredjepartsudbydere af IKT-tjenester eller med politiske risici i tredjepartsudbydernes jurisdiktioner, hvis det er relevant.

Med henblik på litra c) skal det ved test efterprøves, om som minimum kritiske eller vigtige funktioner kan drives hensigtsmæssigt over en tilstrækkelig lang periode, og om den normale funktion kan genoprettes.

3. Foruden de i stk. 2 omhandlede krav inddrager centrale modparter følgende i testen af deres planer for IKT-driftsstabilitet, jf. stk. 1:

a) clearingmedlemmer

b) eksterne leverandører

c) relevante institutter i den finansielle infrastruktur, med hvem centrale modparter har angivet indbyrdes afhængighed i deres politikker for driftsstabilitet.

4. Foruden de i stk. 2 omhandlede krav inddrager værdipapircentraler følgende i testen af deres planer for IKT-driftsstabilitet, jf. stk. 1, alt efter hvad der er relevant:

a) brugere af værdipapircentralerne

b) udbydere af kritiske hjælpeprogrammer og tjenesteydelser

c) andre værdipapircentraler

d) andre markedsinfrastrukturer

e) andre institutter, med hvilke værdipapircentraler har angivet indbyrdes afhængighed i deres politik for driftsstabilitet.

5. Finansielle enheder dokumenterer resultaterne af den i stk. 1 omhandlede test. Eventuelle konstaterede mangler som følge af denne test analyseres, afhjælpes og indberettes til ledelsesorganet.

Artikel 26

Planer for IKT-indsats- og -genopretning

1. Ved udarbejdelsen af de planer for IKT-indsats- og -genopretning, der er omhandlet i artikel 11, stk. 3, i forordning (EU) 2022/2554, tager finansielle enheder hensyn til resultaterne af den finansielle enheds forretningskonsekvensanalyse (BIA). Disse planer for IKT-indsats- og -genopretning skal:

a) præcisere de forhold, der udløste deres aktivering eller deaktivering, og eventuelle undtagelser fra en sådan aktivering eller deaktivering

b) redegøre for, hvilke foranstaltninger der skal træffes for at sikre tilgængeligheden, integriteten, stabiliteten og genopretningen af som minimum IKT-systemer og -tjenester, der understøtter kritiske eller vigtige funktioner i den finansielle enhed

c) være udformet med henblik på at opfylde genopretningsmålene for de finansielle enheders operationer

d) dokumenteres og stilles til rådighed for det personale, der er involveret i gennemførelsen af planer for IKT-indsats- og -genopretning, og være let tilgængelige i nødsituationer

e) indeholde bestemmelser om både kort- og langsigtede genopretningsmuligheder, herunder delvis genopretning af systemer

f) fastsætte målene for planerne for IKT-indsats- og -genopretning og de betingelserne, under hvilke gennemførelsen af disse planer kan erklæres for vellykket.

Med henblik på litra d) giver finansielle enheder en klar præcisering af roller og ansvarsområder.

2. De i stk. 1 omhandlede planer for IKT-indsats- og -genopretning skal angive relevante scenarier, herunder scenarier, som indebærer alvorlige forretningsforstyrrelser og øget sandsynlighed for, at der opstår forstyrrelser. Disse planer skal indeholde scenarier baseret på aktuelle oplysninger om trusler og erfaringer, der er indhøstet fra tidligere forretningsforstyrrelser. Finansielle enheder tager behørigt hensyn til alle følgende scenarier:

a) cyberangreb og omstillingsscenarier mellem den primære IKT-infrastruktur og den redundante kapacitet, sikkerhedskopier og de redundante faciliteter

b) scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller svigter, og tager behørigt hensyn til de potentielle konsekvenser af insolvens eller andresvigt hos en relevant tredjepartsudbyder af IKT-tjenester

c) helt eller delvist svigt i lokaler, heriblandt kontor- og forretningslokaler, og datacentre

d) væsentlige svigt i IKT-aktiver eller kommunikationsinfrastrukturen

e) manglende tilgængelighed af et kritisk antal ansatte eller medarbejdere med ansvar for at sikre driftsstabiliteten

f) virkningerne af klimaændringer og miljøforringelsesrelaterede hændelser, naturkatastrofer, pandemier og fysiske angreb, herunder indtrængen og terrorangreb

g) insiderangreb

h) politisk og social ustabilitet, herunder, hvis det er relevant, i tredjepartsudbyderens jurisdiktion og på det sted, hvor dataene lagres og behandles

i) udbredte strømafbrydelser.

3. Hvis de primære genopretningsforanstaltninger ikke kan gennemføres på kort sigt på grund af omkostninger, risici, logistik eller uforudsete omstændigheder, skal det i de i stk. 1 omhandlede planer for IKT-indsats- og -genopretning overvejes at anvende alternative muligheder.

4. Som led i de i stk. 1 omhandlede de planer for IKT-indsats og -genopretning overvejer og gennemfører finansielle enheder foranstaltninger til driftsstabilitet, som skal afbøde svigt hos tredjepartsudbydere af IKT-tjenester, der understøtter kritiske eller vigtige funktioner i den finansielle enhed.

KAPITEL V

Rapport om gennemgangen af rammen for IKT-risikostyring

Artikel 27

Format og indhold af rapporten om gennemgangen af rammen for IKT-risikostyring

1. Finansielle enheder indsender rapporten om gennemgangen af den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 5, i forordning (EU) 2022/2554, i et søgbart elektronisk format.

2. Finansielle enheder medtager alle følgende oplysninger i den i stk. 1 omhandlede rapport:

a) et indledende afsnit, der:

   i) klart identificerer den finansielle enhed, der er genstand for rapporten, og beskriver dens koncernstruktur, hvis det er relevant

   ii) beskriver konteksten for rapporten med hensyn til karakteren, omfanget og kompleksiteten af den finansielle enheds tjenester, aktiviteter og operationer, dens organisation, identificerede kritiske funktioner, strategi, store igangværende projekter eller aktiviteter, forbindelser og dens afhængighed af interne og kontraherede IKT-tjenester og -systemer eller de konsekvenser, som et samlet tab eller alvorlig forringelse af sådanne systemer ville have med hensyn til kritiske eller vigtige funktioner og markedseffektivitet

   iii) sammenfatter de vigtigste ændringer i rammen for IKT-risikostyring siden den foregående indsendte rapport

   iv) giver et sammendrag på ledelsesniveau af den nuværende og den kortsigtede IKT-risikoprofil, trusselsbilledet, den vurderede effektivitet af dens kontroller og den finansielle enheds sikkerhedsstatus

b) den dato, på hvilken den finansielle enheds ledelsesorgan godkendte rapporten

c) en beskrivelse af årsagen til gennemgangen af rammen for IKT-risikostyring i overensstemmelse med artikel 6, stk. 5, i forordning (EU) 2022/2554

d) gennemgangsperiodens start- og slutdato

e) en angivelse af, hvilken funktion der har ansvar for gennemgangen

f) en beskrivelse af de vigtigste ændringer og forbedringer af rammen for IKT-risikostyring siden den foregående gennemgang

g) et sammendrag af resultaterne af gennemgangen og en detaljeret analyse og vurdering af alvorligheden af svaghederne, manglerne og hullerne i rammen for IKT-risikostyring i gennemgangsperioden

h) en beskrivelse af foranstaltningerne til afhjælpning af konstaterede svagheder, mangler og huller, herunder alle følgende:

   i) et sammendrag af de foranstaltninger, der er truffet for at udbedre konstaterede svagheder, mangler og huller

   ii) en forventet dato for gennemførelse af foranstaltningerne og datoer vedrørende den interne kontrol af gennemførelsen, herunder oplysninger om status for gennemførelsen af disse foranstaltninger på datoen for udarbejdelsen af rapporten, idet der i givet fald redegøres for, om der er risiko for, at fristerne ikke overholdes

   iii) de værktøjer, der skal anvendes, og identifikation af den funktion, der har ansvar for gennemførelsen af foranstaltningerne, med angivelse af, om værktøjerne og funktionerne er interne eller eksterne

   iv) en beskrivelse af indvirkningen af de påtænkte ændringer af foranstaltningerne på den finansielle enheds budgetmæssige, menneskelige og materielle ressourcer, herunder de ressourcer, der er afsat til gennemførelsen af eventuelle korrigerende foranstaltninger

   v) oplysninger om proceduren for underretning af den kompetente myndighed, hvis det er relevant

   vi) hvis de konstaterede svagheder, mangler eller huller ikke er genstand for korrigerende foranstaltninger, en detaljeret redegørelse for de kriterier, der anvendes til at analysere virkningen af disse svagheder, mangler eller huller med henblik på at evaluere den dermed forbundne resterende IKT-risiko, og af de kriterier, der er anvendt til at acceptere den relaterede resterende risiko

i) oplysninger om den planlagte videre udvikling af rammen for IKT-risikostyring

j) konklusioner fra gennemgangen af rammen for IKT-risikostyring

k) oplysninger om tidligere gennemgange, herunder:

   i) en liste over de hidtidige gennemgange

   ii) hvis det er relevant, en status for gennemførelsen af de korrigerende foranstaltninger, der er angivet i den seneste rapport

   iii) hvis de foreslåede korrigerende foranstaltninger i tidligere gennemgange har vist sig at være ineffektive eller har medført uventede udfordringer, en beskrivelse af, hvordan disse korrigerende foranstaltninger kan forbedres, eller af disse uventede udfordringer

l) informationskilder, der er anvendt ved udarbejdelsen af rapporten, herunder alle følgende:

   i) for andre finansielle enheder end mikrovirksomheder, jf. artikel 6, stk. 6, i forordning (EU) 2022/2554, resultaterne af interne revisioner

   ii) resultaterne af overensstemmelsesvurderingerne

   iii) resultater af test af digital operationel modstandsdygtighed og, hvis det er relevant, resultaterne af avanceret test af IKT-værktøjer, -systemer og -processer baseret på trusselsbaseret penetrationstest (TLPT)

   iv) eksterne kilder.

Med henblik på litra c) skal rapporten, hvis gennemgangen blev indledt efter tilsynsmæssige instrukser eller konklusioner udledt af relevante test- eller revisionsprocesser for digital operationel modstandsdygtighed, indeholde udtrykkelige henvisninger til sådanne instrukser eller konklusioner, som gør det muligt at identificere årsagen til at indlede revisionen. Hvis gennemgangen blev indledt efter IKT-relaterede hændelser, skal rapporten indeholde en liste over alle IKT-relaterede hændelser med analyser af de grundlæggende årsager til hændelser.

Med henblik på litra f) skal beskrivelsen indeholde en analyse af ændringernes indvirkning på den finansielle enheds strategi for digital operationel modstandsdygtighed, på den finansielle enheds ramme for intern IKT-kontrol og på den finansielle enheds forvaltning af IKT-risikostyring.

AFSNIT III

DEN FORENKLEDE RAMME FOR IKT-RISIKOSTYRING FOR FINANSIELLE ENHEDER SOM OMHANDLET I ARTIKEL 16, STK. 1, I FORORDNING (EU) 2022/2554

KAPITEL I

Forenklet ramme for IKT-risikostyring

Artikel 28

Forvaltning og organisation

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, sikrer, at de har indført en intern forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af IKT-risici med henblik på at opnå et højt niveau af digital operationel modstandsdygtighed.

2. De i stk. 1 omhandlede finansielle enheder sikrer som led i deres forenklede ramme for IKT-risikostyring, at deres ledelsesorgan:

a) bærer det overordnede ansvar for at sikre, at den forenklede ramme for IKT-risikostyring gør det muligt at gennemføre den finansielle enheds forretningsstrategi i overensstemmelse med den pågældende finansielle enheds risikovillighed, og sikrer, at der i denne sammenhæng tages hensyn til IKT-risikoen

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

c) fastsætter mål for informationssikkerhed og IKT-krav

d) godkender, fører tilsyn med og foretager regelmæssig gennemgang af:

   i) klassificeringen af den finansielle enheds informationsaktiver, jf. denne forordnings artikel 30, stk. 1, listen over de vigtigste konstaterede risici og forretningskonsekvensanalysen og relaterede politikker

   ii) den finansielle enheds planer for driftsstabilitet samt de indsats- og genopretningsforanstaltninger, der er omhandlet i artikel 16, stk. 1, litra f), i forordning (EU) 2022/2554

e) tildeler og gennemgår mindst én om gang året det budget, der er nødvendigt for at opfylde den finansielle enheds behov i forbindelse med digital operationel modstandsdygtighed med hensyn til alle ressourcetyper, herunder relevante IKT-programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed og IKT-færdigheder for alt personale

f) præciserer og gennemfører de politikker og foranstaltninger, der er omfattet af dette afsnits kapitel I, II og III, med henblik på at identificere, vurdere og styre den IKT-risiko, som den finansielle enhed er eksponeret for

g) identificerer og gennemfører procedurer, IKT-protokoller og værktøjer, der er nødvendige for at beskytte alle informationsaktiver og IKT-aktiver

h) sikrer, at personalet i den finansielle enheds ledelsesorgan holdes ajour med den viden og de færdigheder, der er nødvendige for at forstå og vurdere IKT-risiko og dens indvirkning på den finansielle enheds drift, herunder ved regelmæssigt at følge særlige kurser, svarende til den IKT-risiko, der styres

i) indfører rapporteringsordninger, som bl.a. vedrører hyppigheden, formen og indholdet af rapporteringen til ledelsesorganet om informationssikkerhed og digital operationel modstandsdygtighed.

3. De i stk. 1 omhandlede finansielle enheder kan i overensstemmelse med sektorspecifik EU-ret og national ret outsource de opgaver, der er forbundet med efterprøvning af overholdelsen af kravene til IKT-risikostyring, til tredjepart-sudbydere af IKT-tjenester. I tilfælde af en sådan outsourcing har den finansielle enhed fortsat det fulde ansvar for at efterprøve overholdelsen af kravene til IKT-risikostyring.

4. De i stk. 1 omhandlede finansielle enheder sikrer en passende adskillelse af og uafhængighed blandt kontrolfunktioner og interne revisionsfunktioner.

5. De i stk. 1 omhandlede finansielle enheder sikrer, at deres forenklede ramme for IKT-risikostyring gøres til genstand for intern revision, som udføres af revisorer i overensstemmelse med de finansielle enheders revisionsplan. Revisorerne skal besidde tilstrækkelig viden, faglig kompetence og ekspertise med hensyn til IKT-risici og være uafhængige. Hyppigheden af IKT-revisioner og deres fokus skal stå i rimeligt forhold til den finansielle enheds IKT-risiko.

6. På grundlag af resultatet af den i stk. 5 omhandlede revision sikrer de finansielle enheder, der er omhandlet i stk. 1, rettidig efterprøvning og udbedring af kritiske resultater af IKT-revisioner.

Artikel 29

Informationssikkerhedspolitik og -foranstaltninger

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører en informationssikkerhedspolitik i forbindelse med den forenklede ramme for IKT-risikostyring. Denne informationssikkerhedspolitik skal præcisere de overordnede principper og regler for beskyttelse af fortroligheden, integriteten, tilgængeligheden og autenticiteten af data og af de tjenester, som disse finansielle enheder leverer.

2. På grundlag af deres informationssikkerhedspolitik, jf. stk. 1, indfører og gennemfører de i stk. 1 omhandlede finansielle enheder IKT-sikkerhedsforanstaltninger for at mindske deres eksponering for IKT-risici, herunder afbødende foranstaltninger, der gennemføres af tredjepartsudbydere af IKT-tjenester.

IKT-sikkerhedsforanstaltningerne skal omfatte alle de foranstaltninger, der er omhandlet i artikel 30-38.

Artikel 30

Klassificering af informationsaktiver og IKT-aktiver

1. Som led i den forenklede ramme for IKT-risikostyring, der er omhandlet i artikel 16, stk. 1, litra a), i forordning (EU) 2022/2554, identificerer, klassificerer og dokumenterer de finansielle enheder, der er omhandlet i nævnte artikels stk. 1, alle kritiske eller vigtige funktioner, de informationsaktiver og IKT-aktiver, der understøtter dem, og deres indbyrdes afhængighed. Finansielle enheder reviderer denne identifikation og klassificering efter behov.

2. De i stk. 1 omhandlede finansielle enheder identificerer alle kritiske eller vigtige funktioner, der understøttes af tredjepartsudbydere af IKT-tjenester.

Artikel 31

IKT-risikostyring

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, inkluderer i deres forenklede ramme for IKT-risikostyring alle følgende:

a) en fastlæggelse af risikotoleranceniveauerne for IKT-risiko i overensstemmelse med den finansielle enheds risikovillighed

b) konstatering og vurdering af de IKT-risici, som den finansielle enhed er eksponeret for

c) nærmere beskrivelse af strategier for afbødning som minimum for de IKT-risici, der ikke ligger inden for den finansielle enheds risikotoleranceniveauer

d) overvågning af effektiviteten af de strategier for afbødning, der er omhandlet i litra c)

e) konstatering og vurdering af alle IKT- og informationssikkerhedsrisici som følge af større ændringer i IKT-systemer eller -tjenester, -processer eller -procedurer, resultater af IKT-sikkerhedstest og efter alle større IKT-relaterede hændelser.

2. De i stk. 1 omhandlede finansielle enheder foretager og dokumenterer regelmæssigt IKT-risikovurderingen på den måde, der står i rimeligt forhold til de finansielle enheders IKT-risikoprofil.

3. De i stk. 1 omhandlede finansielle enheder overvåger løbende trusler og sårbarheder, der er relevante for deres kritiske eller vigtige funktioner, og informationsaktiver og IKT-aktiver og gennemgår regelmæssigt de risikoscenarier, der har indvirkning på disse kritiske eller vigtige funktioner.

4. De i stk. 1 omhandlede finansielle enheder fastlægger varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod IKT-relaterede hændelser.

Artikel 32

Fysisk og miljømæssig sikkerhed

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, identificerer og gennemfører fysiske sikkerhedsforanstaltninger, der er udformet på grundlag af trusselsbilledet og i overensstemmelse med den klassificering, der er omhandlet i nærværende forordnings artikel 30, stk. 1, IKT-aktivers overordnede risikoprofil og tilgængelige informationsaktiver.

2. De i stk. 1 omhandlede foranstaltninger skal beskytte finansielle enheders lokaler og, hvis det er relevant, datacentre i finansielle enheder, hvor der ligger IKT-aktiver og informationsaktiver, mod uautoriseret adgang, angreb og ulykker og mod miljøtrusler og -farer.

3. Beskyttelsen mod miljøtrusler og -farer skal stå i rimeligt forhold til betydningen af de pågældende lokaler og, når det er relevant, datacentrene og den kritiske betydning af de operationer eller IKT-systemer, der foretages og ligger deri.

KAPITEL II

Yderligere elementer i systemer, protokoller og værktøjer til minimering af virkningerne af IKT-risici

Artikel 33

Adgangskontrol

De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører procedurer for kontrol af logisk og fysisk adgang og håndhæver, overvåger og gennemgår regelmæssigt disse procedurer. Disse procedurer skal indeholde følgende elementer af kontrol af logisk og fysisk adgang:

a) adgangsrettigheder til informationsaktiver, IKT-aktiver og deres understøttede funktioner og til kritiske driftssteder for den finansielle enhed forvaltes på need to know-basis, need to use-basis og least privilege-basis, herunder for fjern- og hasteadgang

b) brugeransvar, som sikrer, at brugerne kan identificeres for de handlinger, der udføres i IKT-systemerne

c) procedurer for kontoforvaltning med henblik på tildeling, ændring eller tilbagekaldelse af adgangsrettigheder for brugerkonti og generiske konti, herunder generiske administratorkonti

d) autentificeringsmetoder, der svarer til den klassificering, der er omhandlet i artikel 30, stk. 1, og til IKT-aktivernes overordnede risikoprofil, og som er baseret på førende praksis

e) adgangsrettigheder gennemgås regelmæssigt og trækkes tilbage, når de ikke længere er nødvendige.

Med henblik på litra c) tildeler den finansielle enhed privilegeret adgang, haste- og administratoradgang på need to use-basis eller ad hoc-basis til alle IKT-systemer, og de logføres i overensstemmelse med artikel 34, litra f), første afsnit.

Med henblik på litra d) anvender finansielle enheder stærke autentificeringsmetoder, der er baseret på førende praksis for fjernadgang til de finansielle enheders netværk, privilegeret adgang og adgang til IKT-aktiver, der understøtter kritiske eller vigtige funktioner, som er offentligt tilgængelige.

Artikel 34

Sikkerhed i forbindelse med IKT-operationer

De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, gør følgende som en del af deres systemer, protokoller og værktøjer og for alle IKT-aktiver:

a) overvåger og forvalter livscyklussen for alle IKT-aktiver

b) overvåger, om IKT-aktiverne understøttes af tredjepartsudbydere af IKT-tjenester fra finansielle enheder, hvis det er relevant

c) identificerer kapacitetskrav til deres IKT-aktiver og foranstaltninger til at opretholde og forbedre IKT-systemernes tilgængelighed og effektivitet og forebygge mangel på IKT-kapacitet, inden de forekommer

d) foretager automatiseret sårbarhedsscanning og automatiserede vurderinger af IKT-aktiver, som står i rimeligt forhold til deres klassificering, jf. artikel 30, stk. 1, og til IKT-aktivets overordnede risikoprofil, og tager korrektioner i brug for at afhjælpe konstaterede sårbarheder

e) styrer de risici, der er forbundet med forældede, ikkeunderstøttede eller legacy-IKT-aktiver

f) logfører hændelser, som vedrører logisk og fysisk adgangskontrol, IKT-operationer, herunder system- og netværkstrafikaktiviteter, og styring af IKT-ændringer

g) identificerer og gennemfører foranstaltninger til overvågning og analyse af oplysninger om anormale aktiviteter og anormal adfærd, som vedrører kritiske eller vigtige IKT-operationer

h) gennemfører foranstaltninger til overvågning af relevante og ajourførte oplysninger om cybertrusler

i) gennemfører foranstaltninger til at konstatere mulige informationslækager, ondsindede kodetyper og andre sikkerhedstrusler og offentligt kendte sårbarheder i software og hardware og tjekker, om der findes dertil svarende nye sikkerhedsopdateringer.

Med henblik på litra f) tilpasser finansielle enheder logfilernes detaljeringsgrad i forhold til deres formål og anvendelse af det IKT-aktiv, der producerer disse logfiler.

Artikel 35

Data-, system- og netsikkerhed

De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udvikler og gennemfører som en del af deres systemer, protokoller og værktøjer sikkerhedsforanstaltninger, der garanterer netsikkerheden mod indtrængen og datamisbrug, og som bevarer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Navnlig indfører finansielle enheder under hensyntagen til den klassificering, der er omhandlet i denne forordnings artikel 30, stk. 1, alt følgende:

a) identifikation og gennemførelse af foranstaltninger til beskyttelse af data, som i brug, under overførsel og inaktive

b) identifikation og gennemførelse af sikkerhedsforanstaltninger med henblik på brugen af software, datalagringsmedier, -systemer og endpoint-enheder til at overføre og lagre den finansielle enheds data

c) identifikation og gennemførelse af foranstaltninger til forebyggelse og detektion af uautoriserede forbindelser til den finansielle enheds netværk og til sikring af nettrafikken mellem den finansielle enheds interne netværk og internettet og andre eksterne forbindelser

d) identifikation og gennemførelse af foranstaltninger, der sikrer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i forbindelse med under overførsel på nettet

e) proces for sikker sletning af data, der findes i den finansielle enheds lokaler eller lagres eksternt, som den finansielle enhed ikke længere behøver at indsamle eller lagre

f) en proces til sikker bortskaffelse eller demontering af datalagringsenheder i lokaler eller datalagringsenheder, der er lagret eksternt, og som indeholder fortrolige oplysninger

g) identifikation og gennemførelse af foranstaltninger til at sikre, at telearbejde og brugen af private endpoint-enheder ikke har en negativ indvirkning på den finansielle enheds evne til at udøve sine kritiske aktiviteter på en passende, rettidig og sikker måde.

Artikel 36

IKT-sikkerhedstest

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udarbejder og gennemfører en plan for IKT-sikkerhedstest med henblik på at validere effektiviteten af deres IKT-sikkerhedsforanstaltninger, der er udviklet i overensstemmelse med nærværende forordnings artikel 33, 34 og 35 og artikel 37 og 38. Finansielle enheder sikrer, at planen tager hensyn til trusler og sårbarheder, der er konstateret som led i den forenklede ramme for IKT-risikostyring, der er omhandlet i denne forordnings artikel 31.

2. De i stk. 1 omhandlede finansielle enheder gennemgår, vurderer og tester IKT-sikkerhedsforanstaltninger, idet de tager hensyn til den samlede risikoprofil for den finansielle enheds IKT-aktiver.

3. De i stk. 1 omhandlede finansielle enheder overvåger og evaluerer resultaterne af disse sikkerhedstest og ajourfører uden unødigt ophold deres sikkerhedsforanstaltninger i overensstemmelse hermed i tilfælde af IKT-systemer, der understøtter kritiske eller vigtige funktioner.

Artikel 37

Anskaffelse, udvikling og vedligeholdelse af IKT-systemer

De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udformer og gennemfører, hvis det er relevant, en procedure for anskaffelse, udvikling og vedligeholdelse af IKT-systemer efter en risikobaseret tilgang. Denne procedure skal:

a) inden erhvervelse eller udvikling af IKT-systemer finder sted, sikre, at de funktionelle og ikkefunktionelle krav, herunder informationssikkerhedskrav, er klart angivet og godkendt af den pågældende forretningsfunktion

b) sikre test og godkendelse af IKT-systemer forud for deres første anvendelse, og inden der indføres ændringer i produktionsmiljøet

c) angive foranstaltninger, som skal mindske risikoen for utilsigtet ændring eller forsætlig manipulation af IKT-systemer i forbindelse med udviklingen og gennemførelsen af disse IKT-systemer i produktionsmiljøet.

Artikel 38

Styring af IKT-projekter og -ændringer

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udvikler, dokumenterer og gennemfører en procedure for IKT-projektstyring og præciserer de roller og ansvarsområder, der er forbundet med gennemførelsen heraf. Denne procedure skal omfatte alle faser af IKT-projekterne fra deres start til deres afslutning.

2. De i stk. 1 omhandlede finansielle enheder udvikler, dokumenterer og gennemfører en procedure for IKT-projektstyring for at sikre, at alle ændringer af IKT-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde og med de passende sikkerhedsforanstaltninger, som skal bevare den finansielle enheds digital operationelle modstandsdygtighed.

Kapitel III

Styring af IKT-driftsstabilitet

Artikel 39

Komponenter i planen for IKT-driftsstabilitet

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, udarbejder deres planer for IKT-driftsstabilitet, idet de tager hensyn til resultaterne af analysen af deres eksponeringer mod og potentielle virkninger af alvorlige forretningsforstyrrelser og scenarier, som de af deres IKT-aktiver, der understøtter kritiske eller vigtige funktioner, kan blive eksponeret for, herunder et cyberangrebsscenarie.

2. De i stk. 1 omhandlede planer for IKT-driftsstabilitet skal:

a) være godkendt af den finansielle enheds ledelsesorgan

b) være dokumenterede og let tilgængelige i tilfælde af en nødsituation eller krise

c) afsætte tilstrækkelige ressourcer til gennemførelse af disse planer

d) fastlægge planlagte genopretningsniveauer og tidsrammer for genopretning og genoptagelse af funktioner og centrale interne og ekstern afhængighed, herunder tredjepartsudbydere af IKT-tjenester

e) identificere de betingelser, der kan føre til aktivering af planerne for IKT-driftsstabilitet, og hvilke foranstaltninger der skal træffes for at sikre tilgængeligheden, stabiliteten og genopretningen af de af de finansielle enheders IKT-aktiver, der understøtter kritiske eller vigtige funktioner

f) angive gendannelses- og genopretningsforanstaltningerne for kritiske eller vigtige forretningsfunktioner, støtteprocesser, informationsaktiver og deres indbyrdes afhængighed for at undgå negative virkninger for de finansielle enheders funktion

g) angive procedurer for og foranstaltninger til sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på den kritiske betydning af den funktion, der anvender dataene

h) overveje alternative muligheder, i tilfælde hvor genopretning måske ikke er mulig på kort sigt på grund af omkostninger, risici, logistik eller uforudsete omstændigheder

i) præcisere de interne og eksterne kommunikationsordninger, herunder fejlafhjælpningsplaner

j) ajourføres i overensstemmelse med erfaringerne fra hændelser, test, nye risici og konstaterede trusler, ændrede genopretningsmål, større ændringer af den finansielle enheds organisation og af de IKT-aktiver, der understøtter kritiske funktioner eller forretningsfunktioner.

Med henblik på litra f) skal de foranstaltninger, der er omhandlet i nævnte litra, afbøde svigt hos kritiske tredjepart-sudbydere.

Artikel 40

Test af planer for driftsstabilitet

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, tester deres planer for driftsstabilitet som omhandlet i nærværende forordnings artikel 39, herunder de scenarier, der er omhandlet i nævnte artikel, mindst én gang om året med henblik på sikkerhedskopierings- og gendannelsesprocedurer, eller efter enhver større ændring af planen for driftsstabilitet.

2. Den i stk. 1 omhandlede test af planer for driftsstabilitet skal påvise, at de finansielle enheder, der er omhandlet heri, er i stand til at opretholde deres virksomheders levedygtighed, indtil kritiske operationer er genetableret, og konstatere eventuelle mangler i disse planer.

3. De i stk. 1 omhandlede finansielle enheder dokumenterer resultaterne af testen af planerne for driftsstabilitet, og eventuelle konstaterede mangler som følge af denne test analyseres, afhjælpes og indberettes til ledelsesorganet.

KAPITEL IV

Rapport om gennemgangen af den forenklede ramme for IKT-risikostyring

Artikel 41

Format og indhold af rapporten om gennemgangen af den forenklede ramme for IKT-risikostyring

1. De finansielle enheder, der er omhandlet i artikel 16, stk. 1, i forordning (EU) 2022/2554, indsender rapporten om gennemgangen af den ramme for IKT-risikostyring, der er omhandlet i nævnte artikels stk. 2 i et søgbart elektronisk format.

2. Den i stk. 1 omhandlede rapport skal indeholde følgende oplysninger:

a) et indledende afsnit, der indeholder:

   i) en beskrivelse af konteksten for rapporten med hensyn til karakteren, omfanget og kompleksiteten af den finansielle enheds tjenester, aktiviteter og operationer, den finansielle enheds organisation, identificerede kritiske funktioner, strategi, store igangværende projekter eller aktiviteter og forbindelser samt den finansielle enheds afhængighed af interne og outsourcede IKT-tjenester og -systemer eller de konsekvenser, som et samlet tab eller alvorlig forringelse af sådanne systemer ville have for kritiske eller vigtige funktioner og markedseffektivitet

   ii) et sammendrag på ledelsesniveau af den konstaterede nuværende og kortsigtede IKT-risiko, trusselsbilledet, den vurderede effektivitet af dens kontroller og den finansielle enheds sikkerhedsstatus

   iii) oplysninger om det indberettede område

   iv) et sammendrag af de vigtigste ændringer i rammen for IKT-risikostyring siden den foregående rapport

   v) et sammendrag og en beskrivelse af indvirkningen af de vigtigste ændringer i den forenklede ramme for IKT-risikostyring siden den foregående rapport

b) hvis det er relevant, den dato, på hvilken den finansielle enheds ledelsesorgan godkendte rapporten

c) en beskrivelse af årsagerne til gennemgangen, herunder:

   i) hvis gennemgangen blev indledt efter tilsynsmæssige instrukser, dokumentation for sådanne instrukser

   ii) hvis gennemgangen blev indledt efter forekomsten af IKT-relaterede hændelser, en liste over alle disse IKT-relaterede hændelser med en analyse af relaterede grundlæggende årsager til hændelserne

d) gennemgangsperiodens start- og slutdato

e) en angivelse af den person, som har ansvar for gennemgangen

f) et sammendrag af resultaterne og en selvevaluering af alvorsgraden af de svagheder, mangler og huller, der er konstateret i rammen for IKT-risikostyring for revisionsperioden, herunder en detaljeret analyse heraf

g) identificerede afhjælpende foranstaltninger til at afbøde svagheder, mangler og huller i den forenklede ramme for IKT-risikostyring og den forventede dato for gennemførelsen af disse foranstaltninger, herunder opfølgning på svagheder, mangler og huller, der er konstateret i tidligere rapporter, hvis disse svagheder, mangler og huller endnu ikke er blevet afhjulpet

h) overordnede konklusioner om gennemgangen af den forenklede ramme for IKT-risikostyring, herunder eventuel yderligere planlagt udvikling.

AFSNIT IV

AFSLUTTENDE BESTEMMELSER

Artikel 42

Ikrafttræden

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

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

Udfærdiget i Bruxelles, den 13. marts 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand