Retningslinjer

EBA/GL/2019/04

28. november 2019

EBA's retningslinjer for IKT- og sikkerhedsrisikostyring

Compliance- og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle virksomheder bestræbe sig bedst muligt på at efterleve retningslinjerne.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod virksomheder.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den ([dd.mm.åååå]) underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller angive deres begrundelse for manglende efterlevelse. Meddeles dette ikke EBA inden for den angivne frist, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Meddelelser bør indsendes på formularen, der er tilgængelig på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/GL/2019/04". Meddelelser bør indsendes af personer med bemyndigelse til at indgive meddelelse om efterlevelse på vegne af de pågældende kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Meddelelser offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] 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).

Formål, anvendelsesområde og definitioner

Emne

5. Disse retningslinjer bygger på bestemmelserne i artikel 74 i direktiv 2013/36/EU (kapitalkravsdirektivet — CRD) vedrørende intern ledelse og følger af mandatet til at udstede retningslinjer i artikel 95, stk. 3, i direktiv (EU) 2015/2366 (det reviderede betalingstjenestedirektiv).

6. Disse retningslinjer fastlægger de risikostyringsforanstaltninger, som finansielle virksomheder (som defineret i punkt 9 nedenfor) skal træffe i overensstemmelse med artikel 74 i kapitalkravsdirektivet for at styre deres IKT-risici og sikkerhedsrisici for alle aktiviteter, og som betalingstjenesteudbydere (betalingstjenesteudbydere som defineret i punkt 9 nedenfor) i overensstemmelse med artikel 95, stk. 1, i det reviderede betalingstjenestedirektiv skal træffe for at styre drifts- og sikkerhedsrisici (hvorved forstås "IKT-risici og sikkerhedsrisici") i forbindelse med de betalingstjenester, som de udbyder. Retningslinjerne omfatter krav til informationssikkerhed, herunder cybersikkerhed, i det omfang oplysningerne opbevares i IKT-systemer.

Anvendelsesområde

7. Disse retningslinjer finder anvendelse på styringen af IKT-risici og sikkerhedsrisici i finansielle virksomheder (som defineret i punkt 9). I disse retningslinjer dækker udtrykket IKT-risici og sikkerhedsrisici drifts- og sikkerhedsrisiciene i henhold til artikel 95 i det reviderede betalingstjenestedirektiv vedrørende udbud af betalingstjenester.

8. For betalingstjenesteudbydere (som defineret i punkt 9) gælder disse retningslinjer for deres udbud af betalingstjenester i overensstemmelse med artikel 95 i det reviderede betalingstjenestedirektiv. For finansielle virksomheder (som defineret i punkt 9) gælder disse retningslinjer for alle de aktiviteter, som de udfører.

Målgrupper

9. Disse retningslinjer er rettet til finansielle virksomheder, der i disse retningslinjer omfatter 1) betalingstjenesteudbydere som defineret i artikel 4, stk. 11, i det reviderede betalingstjenestedirektiv og 2) institutter, dvs. kreditinstitutter og investeringsselskaber som defineret i artikel 4, stk. 1, nr. 3), i forordning (EU) nr. 575/2013. Retningslinjerne finder også anvendelse på kompetente myndigheder som defineret i artikel 4, stk. 1, nr. 40), i forordning (EU) nr. 575/2013, herunder Den Europæiske Centralbank for så vidt angår forhold, der vedrører de opgaver, denne pålægges ved forordning (EU) nr. 1024/2013, og kompetente myndigheder som omhandlet i artikel 4, stk. 2, nr. i), i forordning (EU) nr. 1093/2010.

Definitioner

10. Medmindre andet er angivet, har de udtryk, der er anvendt og defineret i direktiv 2013/36/EU (kapitalkravsdirektivet), forordning (EU) nr. 575/2013 (kapitalkravsforordningen – CRR) og direktiv 2015/2366/EU (det reviderede betalingstjenestedirektiv), den samme betydning i retningslinjerne. I disse retningslinjer gælder endvidere følgende definitioner:

IKT-risici og sikkerhedsrisiko	Tabsrisiko som følge af brud på fortroligheden, manglende integritet af systemer og data, deres utilstrækkelighed eller utilgængelighed eller manglende evne til at ændre informationsteknologi (IT) inden for en rimelig tids- og omkostningsramme, når kravene fra omgivelserne eller de forretningsmæssige krav ændrer sig (dvs. fleksibilitet)[2]. Dette omfatter sikkerhedsrisici som følge af utilstrækkelige interne processer, interne processer, som ikke har virket efter hensigten/som er fejlet, eller eksterne hændelser, herunder cyberangreb eller utilstrækkelig fysisk sikkerhed.
Ledelsesorgan	a) For kreditinstitutter og investeringsselskaber har denne betegnelse samme betydning som definitionen i artikel 3, stk. 1, nr. 7, i direktiv 2013/36/EU. b) For betalingsinstitutter eller elektroniske pengeinstitutter refererer dette udtryk til direktører eller personer, der er ansvarlige for forvaltningen af betalingsinstitutter og elektroniske pengeinstitutter, og, hvor det er relevant, personer, der er ansvarlige for forvaltningen af betalingstjenester, der udføres af betalingsinstitutter og elektroniske pengeinstitutter. c) For de betalingstjenesteudbydere, der henvises til i artikel 1, stk. 1, litra c), e) og f), i direktiv (EU) 2015/2366, har dette udtryk den betydning, det tillægges i henhold til gældende EU-lovgivning eller national lovgivning.
Drifts- eller sikkerhedshændelse	En enkeltstående hændelse eller en række hændelser, der ikke er planlagt af den finansielle virksomhed, og som har eller sandsynligvis vil have en negativ indvirkning på tjenesternes integritet, tilgængelighed, fortrolighed og/eller ægthed.
Den daglige ledelse	a) For kreditinstitutter og investeringsselskaber har denne betegnelse samme betydning som definitionen i artikel 3, stk. 1, nr. 9, i direktiv 2013/36/EU. b) For betalingsinstitutter og elektroniske pengeinstitutter refererer dette udtryk til fysiske personer, der udøver ledende

[2] Definition fra EBA's retningslinjer for fælles procedurer og metoder for tilsynskontrol- og vurderingsprocessen af 19. december 2014 (EBA/GL/2014/13), som ændret ved EBA/GL/2018/03.

	funktioner inden for en virksomhed, og som er ansvarlige for virksomhedens daglige ledelse og refererer til ledelsesorganet. c) For betalingstjenesteudbydere, som der henvises til i artikel 1, stk. 1, litra c), e) og f), i direktiv (EU) 2015/2366, har dette udtryk den betydning, det tillægges i henhold til gældende EU-lovgivning eller national lovgivning.
Risikoappetit	Det samlede risikoniveau og de typer risici, som betalingstjenesteudbyderne og virksomhederne er villige til at påtage sig for at nå deres strategiske mål inden for rammerne af deres risikokapacitet i overensstemmelse med deres forretningsmodel.
Revisionsfunktion	a) For kreditinstitutter og investeringsselskaber er revisionsfunktionen som omtalt i afsnit 22 i EBA's retningslinjer vedrørende intern ledelse (EBA/GL/2017/11). b) For andre betalingstjenesteudbydere end kreditinstitutter skal revisionsfunktionen være uafhængig inden for eller af betalingstjenesteudbyderen og kan være en intern og/eller en ekstern revisionsfunktion.
IKT-projekter	Ethvert projekt eller en del heraf, når IKT-systemer og -tjenester ændres, erstattes, afvises eller gennemføres. IKT-projekter kan være en del af bredere IKT- eller forretningsomlægningsprogrammer.
Tredjepart	En organisation, der har indgået forretningsmæssige forbindelser eller kontrakter med en virksomhed om levering af et produkt eller en tjenesteydelse[3].
Informationsaktiv	En samling af oplysninger i enten fysisk eller elektronisk form, som er værd at beskytte.
IKT-aktiv	Et aktiv bestående af enten software eller hardware, som findes i forretningsmiljøet.
IKT-systemer[4]	IKT etableret som en del af en mekanisme eller et sammenkoblet netværk, der understøtter en finansiel virksomheds drift.
IKT-tjenester[5]	Tjenester, leveret af IKT-systemer til en eller flere interne eller eksterne brugere. Dette kan f.eks. være dataindlæsning, databehandling, dataopbevaring og indberetning, men også overvågning og forretnings- og beslutningsstøttetjenester.

[3] Definition fra G7's grundlæggende elementer til tredjeparters styring af cyberrisici i den finansielle sektor.
[4] Definition fra retningslinjerne om IKT-risikovurdering under tilsynskontrol- og vurderingsprocessen (SREP) (EBA/GL/2017/05).
[5] ibid.

Gennemførelse

Anvendelsesdato

11. Disse retningslinjer finder anvendelse fra den 30. juni 2020.

Ophævelse

12. Retningslinjerne for sikkerhedsforanstaltninger for drifts- og sikkerhedsrisici ved betalingstjenester (EBA/GL/2017/17), der blev udstedt i 2017, vil blive ophævet ved disse retningslinjer på den dato, hvor disse retningslinjer træder i kraft.

Retningslinjer for IKT- og sikkerhedsrisikostyring

1.1. Proportionalitet

1. Alle finansielle virksomheder bør overholde bestemmelserne i disse retningslinjer på en måde, der står i et rimeligt forhold til og tager hensyn til de finansielle virksomheders størrelse, deres interne organisation og arten, omfanget og kompleksiteten af samt risikoen ved de tjenesteydelser og produkter, som de finansielle virksomheder leverer eller har til hensigt at levere.

1.2. Styring og strategi

1.2.1. Styring

2. Ledelsesorganet bør sikre, at finansielle virksomheder har passende rammer for intern styring og intern kontrol af deres IKT-risici og sikkerhedsrisici. Ledelsesorganet bør fastlægge klare roller og ansvarsområder for IKT-funktioner, risikostyring i forbindelse med informationssikkerhed og driftskontinuitet, herunder for ledelsesorganet og dets udvalg.
3. Ledelsesorganet bør sikre, at de finansielle virksomheders personale er tilstrækkeligt stort og kvalificeret til løbende at understøtte deres operationelle IKT-behov og deres IKT- og risikostyringsprocesser og sikre gennemførelsen af deres IKT-strategi. Ledelsesorganet bør sikre, at det tildelte budget er tilstrækkeligt til at opfylde ovenstående. Endvidere bør de finansielle virksomheder sikre, at alle medarbejdere, herunder personer med nøglefunktioner, modtager relevant uddannelse i IKT-risici og sikkerhedsrisici, herunder informationssikkerhed, en gang årligt eller oftere, hvis det er nødvendigt (se også afsnit 1.4.7).

4. Ledelsesorganet har det overordnede ansvar for at fastlægge, godkende og føre tilsyn med gennemførelsen af de finansielle virksomheders IKT-strategi som led i deres overordnede forretningsstrategi og for at etablere effektive risikostyringsrammer for IKT- og sikkerhedsrisici.

1.2.2. Strategi

5. IKT-strategien bør være i overensstemmelse med finansielle virksomheders overordnede forretningsstrategi og fastlægge:

    a) hvordan finansielle virksomheders IKT bør udvikle sig, så det effektivt understøtter og deltager i deres forretningsstrategi, herunder udviklingen i den organisatoriske struktur, ændringer i IKT-systemer og væsentlig afhængighed af tredjeparter
    b) den planlagte strategi og udvikling af IKT-arkitekturen, herunder afhængighed af tredjeparter
    c) klare målsætninger for informationssikkerhed med fokus på IKT-systemer og IKT-tjenester, personale og processer.

6. De finansielle virksomheder bør opstille handlingsplaner, der indeholder de foranstaltninger, der skal træffes for at nå IKT-strategiens mål. Disse bør meddeles alle relevante medarbejdere (herunder konsulenter og tredjepartsleverandører, hvor det er relevant). Handlingsplanerne bør revideres regelmæssigt for at sikre, at de er relevante og hensigtsmæssige. De finansielle virksomheder bør også indføre processer til at overvåge og måle effektiviteten af implementeringen af deres IKT-strategi.

1.2.3. Brug af tredjepartsleverandører

7. Med forbehold for EBA's retningslinjer for outsourcing (EBA/GL/2019/02) og artikel 19 i det reviderede betalingstjenestedirektiv bør de finansielle virksomheder sikre effektiviteten af de risikobegrænsende foranstaltninger, der er defineret i deres risikostyringsrammer, herunder de foranstaltninger, der er fastsat i disse retningslinjer, når betalingstjenesters og/eller IKT-tjenesters og IKT-systemers operationelle funktioner outsources, herunder til koncernenheder, eller når der benyttes tredjeparter.

8. For at sikre kontinuitet i IKT-tjenesterne og IKT-systemerne bør de finansielle virksomheder sikre, at kontrakter og serviceleveranceaftaler (både under normale omstændigheder og i tilfælde af driftsforstyrrelser — se også afsnit 1.7.2) med leverandører (outsourcingleverandører, koncernenheder eller tredjepartsleverandører) omfatter følgende:

    a) passende og forholdsmæssige informationssikkerhedsmål og -foranstaltninger, herunder krav som f.eks. minimumskrav til cybersikkerhed, angivelser af den finansielle virksomheds datalivscyklus, eventuelle krav vedrørende datakryptering, netværkssikkerhed og sikkerhedsovervågningsprocesser og placeringen af datacentre
    b) procedurer for håndtering af operationelle hændelser og sikkerhedshændelser, herunder eskalering og rapportering.

9. De finansielle virksomheder bør overvåge og søge at forvisse sig om disse udbyderes grad af efterlevelse af den finansielle virksomheds sikkerhedsmål, sikkerhedsforanstaltninger og præstationsmål.

1.3. Rammer for IKT-risici og sikkerhedsrisikostyring

1.3.1. Organisation og mål

10. De finansielle virksomheder bør identificere og håndtere deres IKT- og sikkerhedsrisici. Den eller de IKT-funktioner, der er ansvarlig(e) for IKT-systemer, -processer og -sikkerhedsforanstaltninger, bør have passende processer og kontrolforanstaltninger til at sikre, at alle risici identificeres, analyseres, måles, overvåges, styres, indberettes og ligger inden for den finansielle virksomheds risikoappetit, og at de projekter og systemer, de leverer, og de aktiviteter, de udfører, er i overensstemmelse med eksterne og interne krav.

11. De finansielle virksomheder bør tildele ansvaret for forvaltningen og overvågningen af IKT-risici og sikkerhedsrisici til en kontrolfunktion i overensstemmelse med kravene i afsnit 19 i EBA's retningslinjer vedrørende intern ledelse (EBA/GL/2017/11). De finansielle virksomheder bør sikre, at denne kontrolfunktion er uafhængig og objektiv ved at sikre, at den er behørigt adskilt fra IKT-driftsprocesser. Denne kontrolfunktion bør være direkte ansvarlig over for ledelsesorganet og være ansvarlig for overvågning og kontrol af overholdelsen af rammerne for styring af IKT-risici og sikkerhedsrisici. Den bør sikre, at IKT-risici og sikkerhedsrisici identificeres, måles, vurderes, styres, overvåges og indberettes. De finansielle virksomheder bør sikre, at denne kontrolfunktion ikke er ansvarlig for nogen intern revision.

    Den interne revisionsfunktion bør på grundlag af en risikobaseret tilgang have kapacitet til uafhængigt at gennemgå alle IKT-aktiviteter og sikkerhedsrelaterede aktiviteter og enheder i en finansiel virksomhed og give rimelig sikkerhed for, at de overholder den finansielle virksomheds politikker og procedurer og eksterne krav i overensstemmelse med kravene i afsnit 22 i EBA's retningslinjer vedrørende intern ledelse (EBA/GL/2017/11).

12. De finansielle virksomheder bør definere og tildele centrale roller og ansvarsområder samt relevante indberetningskanaler for at sikre effektive rammer for styring af IKT-risici og sikkerhedsrisici. Disse rammer bør integreres fuldt ud i og tilpasses de finansielle virksomheders overordnede risikostyringsprocesser.

13. IKT- og sikkerhedsrisikostyringsrammerne bør omfatte processer til at:

    a) fastsætte risikoappetitten med hensyn til IKT-risici og sikkerhedsrisici i overensstemmelse med den finansielle virksomheds risikoappetit
    b) identificere og vurdere de IKT-risici og sikkerhedsrisici, som en finansiel virksomhed er eksponeret for
    c) fastlægge mitigerende foranstaltninger, herunder kontrolforanstaltninger, for at mitigere IKT- og sikkerhedsrisici
    d) overvåge effektiviteten af disse foranstaltninger samt antallet af indberettede hændelser, herunder — for betalingstjenesteudbydere — de hændelser, der er indberettet i overensstemmelse med artikel 96 i det reviderede betalingstjenestedirektiv, som påvirker de IKT-relaterede aktiviteter, og om nødvendigt træffe foranstaltninger til at korrigere foranstaltningerne
    e) indberette til ledelsesorganet om IKT- og sikkerhedsrisici og -kontroller

f) identificere og vurdere, om der er nogen IKT-relaterede risici og sikkerhedsmæssige risici som følge af større ændringer i IKT-systemer eller IKT-tjenester, -processer eller -procedurer, og/eller efter enhver væsentlig drifts- eller sikkerhedshændelse.

14. De finansielle virksomheder bør sikre, at rammerne for styring af IKT-risici og sikkerhedsrisici dokumenteres og forbedres løbende på grundlag af "indhøstede erfaringer" i forbindelse med dens gennemførelse og overvågning. IKT- og sikkerhedsrisikostyringsrammerne bør godkendes og gennemgås mindst én gang årligt af ledelsesorganet.

1.3.2. Identifikation af funktioner, processer og aktiver

15. De finansielle virksomheder bør kortlægge deres forretningsfunktioner, roller og understøttende processer og sikre, at kortlægningen holdes opdateret for at identificere betydningen af de enkelte elementer og deres indbyrdes afhængighed i forhold til IKT-risici og sikkerhedsrisici.

16. Endvidere bør de finansielle virksomheder kortlægge, udarbejde og ajourføre de informationsaktiver, der understøtter deres forretningsfunktioner og understøttende processer, såsom IKT-systemer, medarbejdere, konsulenter, tredjeparter og afhængigheder af andre interne og eksterne systemer og processer, for at de, som minimum, kan styre de informationsaktiver, der understøtter deres kritiske forretningsfunktioner og -processer.

1.3.3. Klassificering og risikovurdering

17. De finansielle virksomheder bør klassificere de identificerede forretningsfunktioner, understøttende processer og informationsaktiver, der er beskrevet i punkt 15 og 16, på basis af deres kritikalitet.

18. For at definere kritikaliteten af disse identificerede forretningsfunktioner, understøttende processer og informationsaktiver bør de finansielle virksomheder som minimum tage hensyn til fortroligheds-, integritets- og tilgængelighedskrav. Der bør være en klar ansvarsfordeling og et klart ansvar for informationsaktiver.

19. De finansielle virksomheder bør vurdere, om klassificeringen af informationsaktiver og den relevante dokumentation er tilstrækkelig, når der foretages risikovurdering.

20. De finansielle virksomheder bør identificere de IKT-risici og sikkerhedsrisici, der påvirker de identificerede og klassificerede forretningsfunktioner, understøttende processer og informationsaktiver i overensstemmelse med deres kritikalitet. Denne risikovurdering bør foretages og dokumenteres årligt eller med kortere mellemrum, hvis det er nødvendigt. Sådanne risikovurderinger bør også foretages i forbindelse med større ændringer i infrastruktur, processer eller procedurer, der påvirker forretningsfunktionerne, de understøttende processer eller informationsaktiverne. På den baggrund bør den eksisterende risikovurdering af de finansielle virksomheder ajourføres.

21. De finansielle virksomheder bør sikre, at de løbende overvåger trusler og sårbarheder, der er relevante for deres forretningsprocesser, støttefunktioner og informationsaktiver, og bør regelmæssigt gennemgå de risikoscenarier, der påvirker dem.

1.3.4. Mitigering af risici

22. På grundlag af risikovurderingerne bør de finansielle virksomheder afgøre, hvilke foranstaltninger der er nødvendige for at mitigere identificerede IKT-risici og sikkerhedsrisici til et acceptabelt niveau, og om det er nødvendigt at foretage ændringer i eksisterende forretningsprocesser, kontrolforanstaltninger, IKT-systemer og IKT-tjenester. En finansiel virksomhed bør overveje den tid, der er nødvendig for at gennemføre disse ændringer, og den tid, det tager at træffe passende midlertidige kompenserende foranstaltninger for at minimere IKT-risiciene og sikkerhedsrisiciene med henblik på at holde sig inden for den finansielle virksomheds risikoappetit med hensyn til IKT-risici og sikkerhedsrisici.

23. De finansielle virksomheder bør definere og implementere foranstaltninger til at mitigere de identificerede IKT- og sikkerhedsrisici og beskytte informationsaktiver i overensstemmelse med deres klassificering.

1.3.5. Indberetning

24. De finansielle virksomheder bør indberette resultaterne af risikovurderinger til ledelsesorganet klart og rettidigt. Denne indberetning berører ikke betalingstjenesteudbydernes forpligtelse til at give de kompetente myndigheder en ajourført og dækkende risikovurdering, jf. artikel 95, stk. 2, i direktiv (EU) 2015/2366.

1.3.6. Revision

25. En finansiel virksomheds ledelse, systemer og processer i relation til dens IKT-relaterede og sikkerhedsmæssige risici bør revideres regelmæssigt af revisorer med tilstrækkelig viden, faglig kompetence og ekspertise inden for IKT- og sikkerhedsrisici og inden for betalinger (for betalingstjenesteudbydere) med henblik på at give ledelsesorganet sikkerhed for deres effektivitet på en uafhængig måde. Revisorerne bør være uafhængige inden for eller af den finansielle virksomhed. Hyppigheden af og fokus på sådanne revisioner bør stå i et rimeligt forhold til de relevante IKT-risici og sikkerhedsrisici.

26. En finansiel virksomheds ledelsesorgan bør godkende revisionsplanen, herunder alle IKT-revisioner og eventuelle væsentlige ændringer heraf. Revisionsplanen og dens gennemførelse, herunder revisionshyppigheden, bør afspejle og stå i et rimeligt forhold til de iboende IKT-risici og sikkerhedsrisici i den finansielle virksomhed og ajourføres regelmæssigt.

27. Der bør fastlægges en formel opfølgningsproces, herunder bestemmelser om rettidig kontrol og afhjælpning af kritiske IKT-revisionsresultater.

1.4. Informationssikkerhed

1.4.1. Informationssikkerhedspolitik

28. De finansielle virksomheder bør udvikle og dokumentere en informationssikkerhedspolitik, der fastlægger principper og regler på højt plan for at beskytte fortroligheden, integriteten og tilgængeligheden af de finansielle virksomheders og deres kunders data og oplysninger. For

betalingstjenesteudbyderne er denne politik fastlagt i det dokument om sikkerhedspolitikken, der skal vedtages i overensstemmelse med artikel 5, stk. 1, litra j), i direktiv (EU) 2015/2366. Informationssikkerhedspolitikken bør være i overensstemmelse med den finansielle virksomheds informationssikkerhedsmål og være baseret på de relevante resultater af risikovurderingsprocessen. Politikken bør godkendes af ledelsesorganet.

29. Politikken bør omfatte en beskrivelse af de vigtigste roller og ansvarsområder i forbindelse med styring af informationssikkerhed, og den bør fastsætte krav til personale og konsulenter, processer og teknologi i forbindelse med informationssikkerhed, idet det anerkendes, at medarbejdere og konsulenter på alle niveauer har et ansvar for at sikre finansielle virksomheders informationssikkerhed. Politikken skal sikre fortroligheden, integriteten og tilgængeligheden af en finansiel virksomheds kritiske logiske og fysiske aktiver, ressourcer og følsomme data, uanset om de er i hvile, i transit eller i brug. Informationssikkerhedspolitikken bør formidles til alle den finansielle virksomheds medarbejdere og konsulenter.

30. De finansielle virksomheder bør på grundlag af informationssikkerhedspolitikken fastlægge og gennemføre sikkerhedsforanstaltninger for at mitigere de IKT-risici og sikkerhedsrisici, som de er eksponeret for. Disse foranstaltninger bør omfatte:

    a) organisation og styring i overensstemmelse med punkt 10 og 11
    b) logisk sikkerhed (afsnit 1.4.2)
    c) fysisk sikkerhed (afsnit 1.4.3)
    d) IKT-driftssikkerhed (afsnit 1.4.4)
    e) sikkerhedsovervågning (afsnit 1.4.5)
    f) gennemgang, vurdering og test af informationssikkerheden (afsnit 1.4.6)
    g) uddannelse i og oplysning om informationssikkerhed (afsnit 1.4.7).

1.4.2. Logisk sikkerhed

31. De finansielle virksomheder bør definere, dokumentere og implementere procedurer for logisk adgangskontrol (identitets- og adgangsstyring). Disse procedurer bør implementeres, håndhæves, overvåges og med jævne mellemrum revideres. Procedurerne bør også omfatte kontrolforanstaltninger, som sikrer overvågning af uregelmæssigheder. Disse procedurer bør som minimum indeholde følgende elementer, hvor udtrykket "bruger" også omfatter tekniske brugere:

    a) **"Need to know"-princippet, "least privilege"-princippet og "funktionsadskillelse":** De finansielle virksomheder bør forvalte adgangsrettigheder til informationsaktiver og deres støttesystemer efter "need to know"-princippet, herunder med hensyn til fjernadgang. Brugerne bør tildeles minimumsadgangsrettigheder, der er strengt nødvendige for udførelsen af deres opgaver ("least privilege"-princippet), dvs. for at forhindre uberettiget adgang til et stort datasæt eller for at forhindre, at en bruger tildeles kombinationer af adgangsrettigheder, som kan anvendes til at omgå kontrolforanstaltninger (princippet om "funktionsadskillelse").

b) **Brugeransvar:** De finansielle virksomheder bør så vidt muligt begrænse brugen af generiske og delte brugerkonti og sikre, at brugerne, som har udført handlinger i IKT-systemerne, kan identificeres.

c) **Privilegerede adgangsrettigheder:** De finansielle virksomheder bør gennemføre stærke kontrolforanstaltninger i forhold til privilegeret systemadgang ved strengt at begrænse og nøje føre tilsyn med konti med mere omfattende systemadgangsrettigheder (f.eks. administratorkonti). For at opnå sikker kommunikation og reducere risikoen skal fjernadgang til kritiske IKT-systemer kun tildeles efter "need to know"-princippet, og når der anvendes stærke autentificeringsløsninger.

d) **Logning af brugeraktiviteter:** Som minimum bør alle aktiviteter, der udføres af privilegerede brugere, logges og overvåges. Adgangslogs bør sikres for at forhindre uautoriseret ændring eller sletning og bør opbevares i en periode, der står i et rimeligt forhold til kritikaliteten af de identificerede forretningsfunktioner, understøttende processer og informationsaktiver i overensstemmelse med afsnit 1.3.3, uden at dette berører opbevaringskravene i EU-lovgivningen og den nationale lovgivning. En finansiel virksomhed bør bruge disse oplysninger til at lette identifikationen og undersøgelsen af uregelmæssige aktiviteter, der er blevet opdaget i leveringen af tjenester.

e) **Adgangsstyring:** Adgangsrettigheder bør gives, trækkes tilbage og ændres rettidigt i overensstemmelse med foruddefinerede arbejdsgange for godkendelse, som involverer dataejeren af de informationer, der gøres tilgængelige (ejeren af informationsaktivet). I tilfælde af ophør af ansættelse bør adgangsrettighederne omgående trækkes tilbage.

f) **Fornyet tildeling af adgangsrettigheder:** Adgangsrettighederne bør gennemgås regelmæssigt for at sikre, at brugerne ikke har for brede rettigheder, og at adgangsrettighederne trækkes tilbage, når der ikke længere er behov for dem.

g) **Autentificeringsmetoder:** De finansielle virksomheder bør håndhæve autentificeringsmetoder, der er tilstrækkeligt robuste til på passende vis og effektivt at sikre, at politikkerne og procedurerne for adgangskontrol overholdes. Autentificeringsmetoderne bør modsvare kritikaliteten af de IKT-systemer, oplysninger eller den proces, som der gives adgang til. Dette bør som minimum omfatte komplekse passwords eller stærkere autentificeringsmetoder (f.eks. tofaktorgodkendelse) baseret på den relevante risiko.

32. Elektronisk adgang gennem applikationer til data- og IKT-systemer bør begrænses til det minimum, der er nødvendigt for at levere den relevante tjeneste.

1.4.3. Fysisk sikkerhed

33. De finansielle virksomheders fysiske sikringsforanstaltninger bør defineres, dokumenteres og implementeres for at beskytte deres ejendom, datacentre og følsomme områder mod uautoriseret adgang og miljøfarer.

34. Fysisk adgang til IKT-systemer bør kun tillades for autoriserede personer. Tilladelse bør gives i overensstemmelse med den enkeltes opgaver og ansvarsområder og begrænses til personer, der er behørigt uddannet og overvåget. Fysiske adgangsrettigheder bør regelmæssigt

gennemgås for at sikre, at unødvendige adgangsrettigheder straks inddrages, når der ikke er behov for dem.

35. Foranstaltninger til beskyttelse mod miljøfarer bør stå i et rimeligt forhold til bygningernes betydning og kritikaliteten af den drift eller de IKT-systemer, der er placeret i disse bygninger.

1.4.4. IKT-driftssikkerhed

36. De finansielle virksomheder bør gennemføre procedurer for at forhindre sikkerhedsproblemer i IKT-systemer og IKT-tjenester og for at minimere sikkerhedsproblemers indvirkning på leveringen af IKT-tjenester. Disse procedurer bør omfatte følgende foranstaltninger:

    a) identifikation af potentielle sårbarheder, som bør evalueres og afhjælpes ved at sikre, at software og firmware er opdateret, herunder software, der leveres af finansielle virksomheder til deres interne og eksterne brugere, ved at installere kritiske sikkerhedspatches eller ved at implementere kompenserende kontroller
    b) implementering af sikre baselines for konfigurationer af alle netværkskomponenter
    c) implementering af netværkssegmentering, systemer til at forebygge datatab (data loss prevention systems) og kryptering af netværkstrafik (i overensstemmelse med dataklassifikationen)
    d) implementering af "endpoint protection", herunder servere, arbejdsstationer og mobile enheder. De finansielle virksomheder bør vurdere, om enhederne opfylder de sikkerhedsstandarder, som de har fastlagt, før de får adgang til virksomhedens netværk
    e) sikring af, at der er indført mekanismer til kontrol af software-, firmware- og dataintegritet
    f) kryptering af data i hvile og i transit (i overensstemmelse med dataklassifikationen).

37. Endvidere bør de finansielle virksomheder løbende fastslå, om ændringer i det eksisterende driftsmiljø påvirker sikkerhedsforanstaltningerne eller kræver, at yderligere foranstaltninger implementeres for at mitigere de hermed forbundne risici tilstrækkeligt. Disse ændringer bør indgå i finansielle virksomheders formelle ændringsstyringsproces, som skal sikre, at ændringer planlægges, testes, dokumenteres, godkendes og installeres korrekt.

1.4.5. Sikkerhedsovervågning

38. De finansielle virksomheder bør fastlægge og gennemføre politikker og procedurer for at opdage uregelmæssige aktiviteter, som kan påvirke finansielle virksomheders informationssikkerhed, og for at reagere på disse aktiviteter på passende vis. Som led i denne løbende overvågning bør de finansielle virksomheder tage passende og effektive foranstaltninger i brug for at opdage og indberette fysisk eller logisk indtrængen samt brud på fortroligheden, integriteten og tilgængeligheden af informationsaktiver. De løbende overvågnings- og opdagelsesprocesser skal omfatte:

    a) relevante interne og eksterne faktorer, herunder forretningsfunktioner og administrative IKT-funktioner
    b) transaktioner til afsløring af tredjeparters eller andre enheders misbrug af adgang samt internt misbrug af adgang

c) potentielle interne og eksterne trusler.

39. De finansielle virksomheder bør etablere og implementere processer og organisationsstrukturer for at identificere og løbende overvåge sikkerhedstrusler, som kan have væsentlig indflydelse på deres evne til at levere tjenester. De finansielle virksomheder bør aktivt overvåge den teknologiske udvikling for at sikre, at de er opmærksomme på sikkerhedsrisici. De finansielle virksomheder bør implementere opdagende kontrolforanstaltninger, f.eks. for at identificere mulige informationslækager, skadelig kode og andre sikkerhedstrusler og offentligt kendte sårbarheder i software og hardware, og kontrollere, om der findes relevante nye sikkerhedsopdateringer.

40. Sikkerhedsovervågningsprocessen bør også bidrage til, at en finansiel virksomhed forstår arten af operationelle hændelser eller sikkerhedshændelser, identificerer tendenser og støtter organisationens undersøgelser.

1.4.6. Gennemgange, vurderinger og test af informationssikkerheden

41. De finansielle virksomheder bør udføre forskellige gennemgange, vurderinger og test af informationssikkerheden for at sikre effektiv identifikation af sårbarheder i deres IKT-systemer og IKT-tjenester. F.eks. kan finansielle virksomheder foretage gabanalyser i forhold til informationssikkerhedsstandarder, gennemgange af overholdelse af regler, standarder m.v. (compliance reviews), interne og eksterne revisioner af informationssystemer eller gennemgange af fysisk sikkerhed. Endvidere bør institutionen overveje god praksis såsom gennemgange af kildekode, sårbarhedsvurderinger, penetrationstest og red team-øvelser.

42. De finansielle virksomheder bør etablere og implementere rammer for test af informationssikkerheden, der sikrer, at robustheden og effektiviteten af deres informationssikkerhedsforanstaltninger valideres. De finansielle virksomheder bør sikre, at disse rammer tager højde for trusler og sårbarheder, som er identificeret gennem trusselsovervågning og risikovurderingsprocessen.

43. Rammerne for test af informationssikkerhed skal sikre, at test:

a) udføres af uafhængige testinstanser med tilstrækkelig viden, faglig kompetence og ekspertise i test af informationssikkerhedsforanstaltninger, og som ikke er involveret i udviklingen af virksomhedens informationssikkerhedsforanstaltninger
b) omfatter sårbarhedsscanninger og penetrationstest (herunder trusselsbaseret penetrationstest, hvor det er nødvendigt og hensigtsmæssigt), som står i et rimeligt forhold til det risikoniveau, der er identificeret i forretningsprocesser og -systemer.

44. De finansielle virksomheder bør gennemføre løbende og gentagne test af sikkerhedsforanstaltningerne. For alle kritiske IKT-systemer (punkt 17) bør disse test udføres mindst én gang om året, og for betalingstjenesteudbyderne vil de indgå i den omfattende vurdering af de sikkerhedsrisici, der er forbundet med de betalingstjenester, de udbyder, i henhold til artikel 95, stk. 2, i det reviderede betalingstjenestedirektiv. Ikke-kritiske systemer bør testes regelmæssigt ud fra en risikobaseret tilgang og mindst hvert tredje år.

45. De finansielle virksomheder bør sikre, at der gennemføres test af sikkerhedsforanstaltninger i tilfælde af ændringer i infrastruktur, processer eller procedurer, og hvis der foretages ændringer på grund af større drifts- eller sikkerhedshændelser eller som følge af lancering af nye eller væsentligt ændrede kritiske applikationer, der kan tilgås fra internettet.

46. De finansielle virksomheder skal overvåge og evaluere resultaterne af de udførte sikkerhedstest og opdatere deres sikringsforanstaltninger i overensstemmelse hermed uden unødig forsinkelse, når der er tale om kritiske systemer.

47. For betalingstjenesteudbydere bør testrammerne også omfatte sikringsforanstaltninger, der er relevante for i) betalingsterminaler og enheder, der anvendes til betalingstjenester, ii) betalingsterminaler og enheder, der anvendes til at autentificere betalingstjenestebrugeren, og iii) enheder og software, som betalingstjenesteudbyderen leverer til betalingstjenestebrugeren for at generere/modtage autentificeringskoder.

48. På basis af de konstaterede sikkerhedstrusler og de foretagne ændringer skal der udføres test, af scenarier, som omfatter relevante og erkendte potentielle angreb.

1.4.7. Uddannelse i informationssikkerhed og oplysning

49. De finansielle virksomheder bør udarbejde et uddannelsesprogram, herunder tilbagevendende sikkerhedsoplysningsprogrammer for alle medarbejdere og konsulenter for at sikre, at de uddannes i at varetage deres opgaver og ansvar i overensstemmelse med de relevante sikkerhedspolitikker og -procedurer for at reducere menneskelige fejl, tyveri, svig, misbrug eller tab, og hvordan informationssikkerhedsrisici skal håndteres. De finansielle virksomheder bør sikre, at uddannelsesprogrammet tilbyder uddannelse for alle medarbejdere og konsulenter mindst én gang om året.

1.5. IKT-driftsledelse

50. De finansielle virksomheder bør forvalte deres IKT-drift på grundlag af dokumenterede og implementerede processer og procedurer (der for betalingstjenesteudbydere indeholder dokumentet om sikkerhedspolitikken i overensstemmelse med artikel 5, stk. 1, litra j), i det reviderede betalingstjenestedirektiv), som er godkendt af ledelsesorganet. Dette sæt dokumenter bør definere, hvordan finansielle virksomheder driver, overvåger og kontrollerer deres IKT-systemer og -tjenester, herunder bør det indeholde dokumentation af kritisk IKT-drift, og det bør gøre det muligt for finansielle virksomheder at vedligeholde en opdateret fortegnelse over IKT-aktiver.

51. De finansielle virksomheder bør sikre, at niveauet for deres IKT-drift er i overensstemmelse med deres forretningsmæssige krav. De finansielle virksomheder bør opretholde og, når det er muligt, forbedre effektiviteten af deres IKT-drift, herunder, men ikke begrænset til nødvendigheden af at overveje, hvordan potentielle fejl som følge af udførelsen af manuelle opgaver minimeres.

52. De finansielle virksomheder bør implementere lognings- og overvågningsprocedurer for kritisk IKT-drift for at gøre det muligt at opdage, analysere og rette fejl.

53. De finansielle virksomheder bør føre en ajourført fortegnelse over deres IKT-aktiver (herunder IKT-systemer, netværksudstyr, databaser osv.). IKT-fortegnelsen bør indeholde konfigurationen for IKT-aktiverne og forbindelserne og de indbyrdes afhængigheder mellem de forskellige IKT-aktiver for at muliggøre en korrekt konfigurations- og ændringsstyringsproces.

54. Fortegnelsen over IKT-aktiver bør være tilstrækkelig detaljeret til at sikre hurtig identifikation af et IKT-aktiv, dets placering, sikkerhedsklassifikation og ejerforhold. Gensidige afhængigheder mellem aktiver bør dokumenteres med henblik på at bidrage til håndtering af sikkerhedshændelser og operationelle hændelser, herunder cyberangreb.

55. De finansielle virksomheder bør overvåge og styre IKT-aktivernes livscyklus for at sikre, at de fortsat opfylder og understøtter forretnings- og risikostyringskrav. De finansielle virksomheder bør overvåge, om deres eksterne eller interne leverandører og udviklere yder support til deres IKT-aktiver, og hvorvidt alle relevante patches og opgraderinger installeres på grundlag af dokumenterede processer. Risici som følge af forældede eller ikkeunderstøttede IKT-aktiver bør vurderes og mitigeres.

56. De finansielle virksomheder bør implementere performance-, kapacitetsplanlægnings- og overvågningsprocesser med henblik på rettidigt at forebygge, opdage og reagere på vigtige performanceproblemer vedrørende IKT-systemer og mangel på IKT-kapacitet.

57. De finansielle virksomheder bør fastlægge og implementere procedurer for backup og gendannelse af data og IKT-systemer for at sikre, at de kan gendannes efter behov. Omfanget og hyppigheden af backup bør fastsættes i overensstemmelse med de forretningsmæssige krav til genopretning og dataenes og IKT-systemernes kritikalitet og evalueres i overensstemmelse med den udførte risikovurdering. Test af backup- og gendannelsesprocedurer bør foretages med jævne mellemrum.

58. De finansielle virksomheder bør sikre, at backup af data og IKT-systemer opbevares sikkert og ligger tilstrækkeligt langt fra den primære beliggenhed, så de ikke udsættes for de samme risici.

3.5.1 IKT-hændelses- og problemhåndtering

59. De finansielle virksomheder bør etablere og implementere en proces for hændelses- og problemhåndtering med henblik på at overvåge og logge operationelle og sikkerhedsmæssige IKT-hændelser og gøre det muligt for finansielle virksomheder at fortsætte eller genoptage kritiske forretningsfunktioner og -processer rettidigt, når der opstår driftsforstyrrelser. De finansielle virksomheder bør fastsætte passende kriterier og tærskler for at klassificere hændelser som operationelle eller sikkerhedsrelaterede hændelser som omhandlet i "definitionsafsnittet" i disse retningslinjer samt tidlige varslingsindikatorer, der bør fungere som alarmer for at muliggøre tidlig opdagelse af sådanne hændelser. Disse kriterier og tærskler for betalingstjenesteudbydere berører ikke klassificeringen af større hændelser i overensstemmelse med artikel 96 i det reviderede betalingstjenestedirektiv og retningslinjerne for indberetning af større hændelser i henhold til det reviderede betalingstjenestedirektiv (EBA/GL/2017/10).

60. For at minimere virkningen af utilsigtede hændelser og muliggøre rettidig genopretning bør de finansielle virksomheder etablere passende processer og organisatoriske strukturer for at sikre en konsekvent og integreret overvågning, håndtering og opfølgning på operationelle og sikkerhedsmæssige hændelser og sikre, at de grundlæggende årsager identificeres og fjernes for at forhindre, at hændelser gentages. Processen for hændelses- og problemhåndtering bør fastlægge:

    a) procedurer for identifikation, sporing, registrering, kategorisering og klassificering af hændelser efter en prioritetsrækkefølge, der er baseret på kritikaliteten af hændelserne for forretningen
    b) roller og ansvar for forskellige hændelsesscenarier (f.eks. fejl, reduceret funktionalitet og cyberangreb)
    c) procedurer for problemhåndtering med henblik på at identificere, analysere og løse den grundlæggende årsag til en eller flere hændelser. En finansiel virksomhed bør analysere operationelle og sikkerhedsmæssige hændelser, der kan påvirke den finansielle virksomhed, og som er blevet identificeret eller har fundet sted inden for og/eller uden for organisationen, og bør tage de vigtigste erfaringer, der er indhøstet med disse analyser, i betragtning og ajourføre sikkerhedsforanstaltningerne i overensstemmelse hermed
    d) effektive interne kommunikationsplaner, herunder underretning om hændelser og eskalationsprocedurer, der også omfatter sikkerhedsrelaterede kundeklager, for at sikre, at:
        i) hændelser med potentielt stor negativ indvirkning på kritiske IKT-systemer og IKT-tjenester indberettes til den relevante daglige ledelse og IKT-ledelse
        ii) ledelsesorganet underrettes på ad hoc-basis i tilfælde af væsentlige hændelser, og som minimum underrettes om konsekvenserne, opfølgningen og de yderligere kontrolforanstaltninger, der bliver indført som resultat af hændelserne
    e) procedurer for hændelseshåndtering med henblik på at mindske konsekvenserne som følge af hændelserne, og sikre, at tjenesten rettidigt bliver operationel og sikker
    f) konkrete eksterne kommunikationsplaner for kritiske forretningsfunktioner og -processer med henblik på at:
        i) samarbejde med relevante interessenter om effektivt at håndtere hændelsen og reetablere driften
        ii) levere rettidige oplysninger til eksterne parter (f.eks. kunder, andre markedsdeltagere, tilsynsmyndigheden), alt efter hvad der er relevant, og i overensstemmelse med gældende lovgivning.

1.6. IKT-projekt- og ændringsstyring

1.6.1. IKT-projektstyring

61. En finansiel virksomhed bør gennemføre en program- og/eller en projektstyringsproces, der definerer roller og ansvar, for effektivt at støtte implementeringen af IKT-strategien.

62. En finansiel virksomhed bør behørigt overvåge og mitigere de risici, der følger af dens portefølje af IKT-projekter (programstyring), idet der også bør tages hensyn til de risici, der kan opstå som følge af indbyrdes afhængigheder mellem forskellige projekter og af afhængigheder af flere projekter, der afvikles med de samme ressourcer og/eller den samme ekspertise.

63. En finansiel virksomhed bør udarbejde og gennemføre en IKT-projektstyringspolitik, der som minimum omfatter:

    a) projektmål
    b) roller og ansvar
    c) en projektrisikovurdering
    d) en projektplan, en tidsramme og de forskellige trin
    e) vigtigste milepæle
    f) krav til ændringsstyring

64. Politikken for IKT-projektstyring bør sikre, at informationssikkerhedskrav analyseres og godkendes af en funktion, der er uafhængig af udviklingsfunktionen.

65. En finansiel virksomhed bør sikre, at alle områder, der påvirkes af et IKT-projekt, er repræsenteret i projektteamet, og at projektteamet har den nødvendige viden til at sikre en sikker og vellykket projektgennemførelse.

66. Etableringen af og fremdriften i IKT-projekter og de dermed forbundne risici bør indberettes til ledelsesorganet, individuelt eller samlet, afhængigt af IKT-projekternes betydning og omfang, regelmæssigt og på ad hoc-basis, alt efter hvad der er passende. De finansielle virksomheder bør medtage projektrisici i deres risikostyringsrammer.

1.6.2. Anskaffelse og udvikling af IKT-systemer

67. De finansielle virksomheder bør udvikle og implementere en proces for anskaffelse, udvikling og vedligeholdelse af IKT-systemer. Denne proces bør udformes på grundlag af en risikobaseret tilgang.

68. En finansiel virksomhed bør sikre, at de funktionelle og ikkefunktionelle krav (herunder krav til informationssikkerhed) defineres klart og godkendes af den relevante forretningsledelse, inden IKT-systemer anskaffes eller udvikles.

69. En finansiel virksomhed bør sikre, at der er truffet foranstaltninger til at mitigere risikoen for utilsigtet ændring eller bevidst manipulation af IKT-systemer, der er under udvikling og implementering i produktionsmiljøet.

70. De finansielle virksomheder bør have en metode til test og godkendelse af IKT-systemer, inden de tages i brug for første gang. Denne metode bør tage højde for forretningsprocessernes og aktivernes kritikalitet. Testene bør sikre, at de nye IKT-systemer fungerer efter hensigten. Der bør også anvendes testmiljøer, der i tilstrækkelig grad afspejler produktionsmiljøet.

71. De finansielle virksomheder bør teste IKT-systemer, IKT-tjenester og informationssikkerhedsforanstaltninger med henblik på at identificere potentielle sikkerhedssvagheder, -overtrædelser og -hændelser.

72. En finansiel virksomhed bør implementere adskilte IKT-miljøer for at sikre tilstrækkelig funktionsadskillelse og mitigere konsekvenserne af ikkeverificerede ændringer på produktionssystemerne. Konkret bør en finansiel virksomhed sikre adskillelse af produktionsmiljøerne fra udviklings- og testmiljøerne og andre ikkeproduktionsmiljøer. En finansiel virksomhed bør sikre integriteten og fortroligheden af produktionsdata, der anvendes i ikkeproduktionsmiljøer. Adgang til produktionsdata er begrænset til autoriserede brugere.

73. De finansielle virksomheder bør implementere foranstaltninger til at beskytte integriteten af kildekoden til IKT-systemer, der udvikles internt. De bør også grundigt dokumentere udviklingen, implementeringen, driften og/eller konfigurationen af IKT-systemerne for at mindske enhver unødvendig afhængighed af eksperter på området. Dokumentationen for IKT-systemet bør, hvor det er relevant, som minimum omfatte brugerdokumentation, teknisk systemdokumentation og driftsprocedurer.

74. En finansiel virksomheds processer for anskaffelse og udvikling af IKT-systemer bør også gælde for IKT-systemer, der udvikles eller styres af slutbrugere i forretningsfunktioner uden for IKT-organisationen (f.eks. slutbrugerapplikationer) ud fra en risikobaseret tilgang. Den finansielle virksomhed bør føre et register over disse applikationer, der understøtter kritiske forretningsfunktioner eller -processer.

1.6.3. IKT-ændringsstyring

75. De finansielle virksomheder bør indføre og implementere en IKT-ændringsstyringsproces for at sikre, at alle ændringer af IKT-systemer registreres, testes, vurderes, godkendes, implementeres og verificeres på en kontrolleret måde. De finansielle virksomheder bør håndtere ændringer i forbindelse med nødsituationer (dvs. ændringer, der skal gennemføres så hurtigt som muligt) efter procedurer, der indeholder tilstrækkelige sikringsforanstaltninger.

76. De finansielle virksomheder bør løbende vurdere, om ændringer i det eksisterende driftsmiljø påvirker de eksisterende sikringsforanstaltninger eller kræver indførelse af yderligere foranstaltninger for at mitigere risikoen herved. Disse ændringer bør ske i overensstemmelse med de finansielle virksomheders formelle ændringsstyringsproces.

1.7. Beredskabsstyring

77. De finansielle virksomheder bør etablere en forsvarlig beredskabsstyringsproces for at maksimere deres evne til løbende at levere tjenester og begrænse tab i tilfælde af alvorlige driftsforstyrrelser i overensstemmelse med artikel 85, stk. 2, i direktiv 2013/36/EU og afsnit VI i EBA's retningslinjer vedrørende intern ledelse (EBA/GL/2017/11).

1.7.1. Analyse af konsekvenserne for forretningen

78. Som led i en forsvarlig beredskabsstyring bør de finansielle virksomheder gennemføre analyser af konsekvenserne for forretningen (Business Impact Analysis, BIA) ved at analysere deres eksponering over for alvorlige driftsforstyrrelser og vurdere deres potentielle konsekvenser (herunder for fortrolighed, integritet og tilgængelighed) kvantitativt og kvalitativt ved hjælp af

interne og/eller eksterne data (f.eks. tredjepartsudbydere af data, der er relevante for en forretningsproces, eller offentligt tilgængelige data, der kan være relevante for BIA'en) og scenarieanalyse. BIA'en bør også tage kritikaliteten af de identificerede og klassificerede forretningsfunktioner, understøttende processer, tredjeparter og informationsaktiver og deres indbyrdes afhængigheder i betragtning i overensstemmelse med afsnit 1.3.3.

79. De finansielle virksomheder bør sikre, at deres IKT-systemer og IKT-tjenester er udformet og tilpasset deres BIA, f.eks. ved at sikre redundans af visse kritiske komponenter for at undgå driftsforstyrrelser forårsaget af hændelser, der påvirker disse komponenter.

1.7.2. Forretningsnødplaner

80. De finansielle virksomheder bør på grundlag af deres analyse af konsekvenserne for driften udarbejde forretningsnødplaner for at sikre driftskontinuitet (business continuity plans, BCP'er), som bør dokumenteres og godkendes af deres ledelsesorganer. Planerne bør navnlig tage hensyn til risici, der kan have en negativ indvirkning på IKT-systemer og IKT-tjenester. Planerne skal støtte mål om at beskytte og om nødvendigt genoprette fortroligheden, integriteten og tilgængeligheden af deres forretningsfunktioner, understøttende processer og informationsaktiver. De finansielle virksomheder bør samarbejde med relevante interne og eksterne interessenter, afhængigt af hvad der er passende, under udarbejdelsen af disse planer.

81. De finansielle virksomheder bør indføre forretningsnødplaner (BCP'er) for at sikre, at de på passende vis kan reagere på potentielle nedbrudsscenarier, og at de er i stand til at genoprette deres kritiske forretningsaktiviteter efter nedbrud inden for de fastsatte mål om genopretning, nemlig Recovery Time Objective, RTO (det maksimale tidsrum, inden for hvilket et system eller en proces skal genoprettes efter en hændelse) og Recovery Point Objective, RPO (det maksimalt acceptable datatab, målt i tid). I tilfælde af alvorlige driftsnedbrud, der udløser specifikke forretningsnødplaner, bør de finansielle virksomheder prioritere forretningsnødforanstaltninger ud fra en risikobaseret tilgang, som kan baseres på de risikovurderinger, der foretages i henhold til afsnit 1.3.3. For betalingstjenesteudbydere kan dette f.eks. omfatte fremme af den videre behandling af kritiske transaktioner, samtidig med at de genoprettende foranstaltninger fortsætter.

82. En finansiel virksomhed bør overveje en række forskellige scenarier i sin forretningsnødplan (BCP), herunder ekstreme, men plausible scenarier, inklusive et cyberangrebsscenarie, som den kan blive eksponeret for, og vurdere den potentielle indvirkning, som sådanne scenarier kunne have. På grundlag af disse scenarier bør en finansiel virksomhed beskrive, hvordan kontinuiteten af IKT-systemer og -tjenester samt den finansielle virksomheds informationssikkerhed sikres.

1.7.3. Beredskabs- og genopretningsplaner

83. På grundlag af BIA'erne (punkt 78) og plausible scenarier (punkt 82) bør de finansielle virksomheder udarbejde beredskabs- og genopretningsplaner. Disse planer bør beskrive, hvilke betingelser der kan føre til aktivering af planerne, og hvilke foranstaltninger der skal træffes for

at sikre tilgængelighed, kontinuitet og genopretning af i det mindste de finansielle virksomheders kritiske IKT-systemer og IKT-tjenester. Beredskabs- og genopretningsplanerne bør sigte mod at opfylde genopretningsmålene (RTO og RPO) for de finansielle virksomheders drift.

84. Beredskabs- og genopretningsplanerne bør tage højde for både kort- og langsigtede genopretningsmodeller. Planerne skal:

    a) fokusere på at genoprette driften af kritiske forretningsfunktioner, understøttende processer, informationsaktiver og deres indbyrdes afhængigheder for at undgå negative påvirkninger på de finansielle virksomheders drift og på det finansielle system, herunder på betalingssystemer og på betalingstjenestebrugere, og for at sikre gennemførelsen af udestående betalingstransaktioner
    b) dokumenteres og stilles til rådighed for forretnings- og støtteenhederne og være let tilgængelige i nødsituationer
    c) opdateres i overensstemmelse med erfaringerne fra hændelser, test, nye identificerede risici og trusler og ændrede genopretningsmål og -prioriteter.

85. Der bør i planerne også overvejes alternative muligheder i tilfælde af, at det ikke er muligt at genoprette driften på kort sigt på grund af omkostninger, risici, logistik eller uforudsete omstændigheder.

86. Som led i beredskabs- og genopretningsplanerne bør en finansiel virksomhed overveje og implementere nødplansforanstaltninger for at mitigere svigt fra tredjepartsleverandører, som er af afgørende betydning for den fortsatte drift af en finansiel virksomheds IKT-tjenester (i overensstemmelse med EBA's retningslinjer for outsourcing (EBA/GL/2019/02) vedrørende driftskontinuitetsplaner).

1.7.4. Test af planer

87. De finansielle virksomheder bør regelmæssigt teste deres forretningsnødplaner (BCP'er). De bør navnlig sikre, at forretningsnødplanerne (BCP'er) for deres kritiske funktioner, understøttende processer, informationsaktiver og deres indbyrdes afhængigheder (herunder, hvis relevant dem, der leveres af tredjeparter) testes mindst én gang om året i overensstemmelse med punkt 89.

88. Forretningsnødplanerne bør ajourføres mindst én gang om året på grundlag af testresultaterne, det aktuelle trusselsbillede og erfaringerne fra tidligere hændelser. Eventuelle ændringer i genopretningsmålene (herunder RTO'er og RPO'er) og/eller ændringer i forretningsfunktioner, understøttende processer og informationsaktiver bør også overvejes, hvor det er relevant, som grundlag for ajourføring af forretningsnødplanerne.

89. Finansielle virksomheders test af deres forretningsnødplaner bør godtgøre, at de er i stand til at opretholde virksomhedens levedygtighed, indtil de kritiske operationer bliver genoprettet. De bør navnlig:

    a) omfatte test af et passende sæt af alvorlige, men plausible scenarier, herunder dem, der tages i betragtning i forbindelse med udviklingen af forretningsnødplanerne (samt test

af tjenester, der leveres af tredjeparter, hvor det er relevant). Dette bør omfatte skift af kritiske forretningsfunktioner, understøttende processer og informationsaktiver til katastrofeberedskabsmiljøet og påvisning af, at de kan fungere på denne måde i et tilstrækkeligt repræsentativt tidsrum, og at normal drift kan genetableres derefter

b) være udformet til at udfordre de antagelser, som forretningsnødplanerne hviler på, herunder den organisatoriske styring og krisekommunikationsplaner, og

c) omfatte procedurer til at efterprøve medarbejdernes, konsulenternes, IKT-systemernes og IKT-tjenesternes evne til at reagere hensigtsmæssigt på de scenarier, der er omhandlet i punkt 89, litra a).

90. Testresultaterne skal dokumenteres, og eventuelle identificerede mangler som følge af testene bør analyseres, afhjælpes og meddeles ledelsesorganet.

1.7.5. Krisekommunikation

91. I tilfælde af nedbrud eller nødsituationer og under gennemførelsen af forretningsnødplanerne skal finansielle virksomheder sikre, at de har effektive krisekommunikationsforanstaltninger, så alle relevante interne og eksterne interessenter, herunder de kompetente myndigheder, når det kræves i henhold til nationale bestemmelser, samt eksterne tjenesteudbydere (outsourcingleverandører, koncernenheder eller tredjepartsleverandører) underrettes rettidigt og på en hensigtsmæssig måde.

1.8. Håndtering af forholdet til betalingstjenestebrugere

92. Betalingstjenesteudbydere bør etablere og gennemføre processer for at højne betalingstjenestebrugernes bevidsthed om sikkerhedsrisici i forbindelse med betalingstjenesterne ved at yde betalingstjenestebrugere hjælp og vejledning.

93. Hjælp og vejledning, der tilbydes betalingstjenestebrugere, bør opdateres i lyset af nye trusler og sårbarheder, og ændringer skal meddeles betalingstjenestebrugeren.

94. Hvis produktfunktionaliteten tillader det, skal betalingstjenesteudbydere gøre det muligt for betalingstjenestebrugerne at deaktivere specifikke betalingsfunktioner, som er knyttet til de betalingstjenester, som betalingstjenesteudbyderen tilbyder betalingstjenestebrugeren.

95. Hvis en betalingstjenesteudbyder i overensstemmelse med artikel 68, stk. 1, i direktiv (EU) 2015/2366 har aftalt beløbsgrænser med betaleren for betalingstransaktioner, der gennemføres via specifikke betalingsinstrumenter, skal betalingstjenesteudbyderen give betaleren mulighed for at tilpasse disse grænser op til den aftalte maksimumsgrænse.

96. Betalingstjenesteudbydere bør give betalingstjenestebrugere mulighed for at modtage advarsler om initierede og/eller mislykkede forsøg på at initiere betalingstransaktioner, så de kan opdage misbrug af deres konti.

97. Betalingstjenesteudbydere bør holde betalingstjenestebrugerne underrettet om opdateringer i sikkerhedsprocedurer, der påvirker betalingstjenestebrugerne for så vidt angår leveringen af betalingstjenester.

98. Betalingstjenesteudbydere bør yde betalingstjenestebrugere bistand med alle spørgsmål, anmodninger om bistand og meddelelser om uregelmæssigheder eller spørgsmål vedrørende sikkerhedsforhold i forbindelse med betalingstjenester. Betalingstjenestebrugere bør på behørig vis informeres om, hvordan denne bistand kan opnås.