EIOPA-BoS-20/600

Retningslinjer for IKT-sikkerhed og -ledelsesstyring

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Tyskland - Tlf.: + 49 69-951119-20;
Fax: + 49 69-951119-19; e-mail: info@eiopa.europa.eu websted: www.eiopa.europa.eu

Indhold

Baggrund **3**
Indledning **6**
Definitioner 6
Retningslinje 1 – Proportionalitet 8
Retningslinje 2 – IKT inden for ledelsesstyringssystemet 8
Retningslinje 3 - IKT-strategi 9
Retningslinje 4 – IKT og sikkerhedsrisici inden for risikostyringssystemet 9
Retningslinje 5 – Revision 10
Retningslinje 6 – Informationssikkerhedspolitik og -foranstaltninger 10
Retningslinje 7 – Informationssikkerhedsfunktion 11
Retningslinje 8 – Logisk sikkerhed 11
Retningslinje 9 – Fysisk sikkerhed 12
Retningslinje 10 – Sikkerhed for IKT-drift 13
Retningslinje 11 – Sikkerhedsovervågning 13
Retningslinje 12 – Gennemgange, vurderinger og test af informationssikkerhed 14
Retningslinje 13 – Informationssikkerhedsuddannelse og informationskurser 14
Retningslinje 14 – IKT-driftsledelse 14
Retningslinje 15 – Håndtering af IKT-hændelser og -problemer 15
Retningslinje 16 – IKT-projektstyring 16
Retningslinje 17 – Erhvervelse og udvikling af IKT-systemer 16
Retningslinje 18 - IKT-ændringshåndtering 17
Retningslinje 19 – Forvaltning af driftskontinuitet 17
Retningslinje 20 – Konsekvensanalyse 17
Retningslinje 21 – Kontinuitetsplanlægning 18
Retningslinje 22 – Beredskabs- og genopretningsplaner 18
Retningslinje 23 – Testning af planer 19
Retningslinje 24 – Krisekommunikationer 19
Retningslinje 25 – Outsourcing af IKT-tjenester og IKT-systemer 19
Bestemmelser om efterlevelse og indberetning **21**
Afsluttende bestemmelse om revision **21**

Baggrund

1. I henhold til artikel 16 i forordning (EU) nr. 1094/2010 kan EIOPA udstede retningslinjer og henstillinger til kompetente myndigheder og finansielle institutioner med henblik på at fastlægge en konsekvent og effektiv tilsynspraksis og sikre en fælles, ensartet og konsekvent anvendelse af EU-retten.

2. I henhold til artikel 16, stk. 3, i nævnte forordning skal de kompetente myndigheder og finansielle institutioner bestræbe sig mest muligt på at efterleve retningslinjer og henstillinger.

3. EIOPA afdækkede behovet for at udarbejde særlig vejledning om IKT-sikkerhed og -ledelsesstyring inden for rammerne af artikel 41 og 44 i direktiv 2009/138/EF på baggrund af den analyse, der er udført som svar på Europa-Kommissionens fintech-handlingsplan (COM(2018)0109 final), EIOPA's plan for ensartet tilsyn 2018-2019[1] og følgende interaktioner med flere andre interessenter[2].

4. Ifølge den fælles rådgivning fra de europæiske tilsynsmyndigheder til Europa-Kommissionen afspejler EIOPA's retningslinjer for ledelsessystem ikke fuldstændigt, hvor vigtigt det er at tage hånd om IKT-risikostyring (herunder cyberrisici). Der findes ingen vejledning om de vigtige elementer, der generelt anerkendes som værende en del af korrekt IKT-sikkerhed og -ledelsesstyring.

5. Analyser af den nuværende (lovmæssige) situation i EU for ovennævnte fælles rådgivning viser, at størstedelen af EU's medlemsstater har fastlagt nationale regler for IKT-sikkerhed og -ledelsesstyring. Selvom kravene ligner hinanden, er lovrammerne stadig fragmenterede. Derudover påviste en undersøgelse af gældende tilsynspraksis en bred række af praksisser – fra "intet specifikt tilsyn" til "omfattende tilsyn" (inklusive "ikkestedlige inspektioner" og "inspektioner på stedet").

6. Desuden stiger kompleksiteten af IKT samt hyppigheden af IKT-relaterede hændelser (inklusive cyberhændelser), og sådanne hændelsers negative indvirkninger på selskabernes driftsmæssige funktion stiger således også. Af denne grund er IKT- og sikkerhedsrisikostyring vigtigt for, at et selskab kan opnå sine strategiske samt erhvervs-, drifts- og omdømmemæssige mål.

7. Derudover er der inden for forsikringssektoren, herunder både traditionelle og nytænkende forretningsmodeller, en stigende brug af IKT til levering af forsikringstjenester og til selskabernes normale driftsmæssige funktion, såsom digitalisering af forsikringssektoren (InsurTech, IoT, osv.) samt indbyrdes forbindelse igennem telekommunikationskanaler (internet, mobile og trådløse forbindelser samt fjerndatanet). Dette gør selskabernes drift sårbar over for sikkerhedshændelser, herunder cyberangreb. Det er derfor vigtigt at sikre, at selskaberne er passende forberedt til at forvalte deres IKT- og sikkerhedsrisici.

8. Disse retningslinjer anerkender behovet for at være forberedt på cyberrisici[3], og at selskaberne har sunde rammer for cybersikkerhed, og de omhandler derfor også cybersikkerhed som en del af selskabets informationssikkerhedsmæssige foranstaltninger. Selvom disse retningslinjer anerkender, at cybersikkerhed bør behandles som en del af et selskabs overordnede IKT- og sikkerhedsrisikostyring,

---

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Rapporten, der blev offentliggjort af EIOPA som svar på Europa-Kommissionens fintechhandlingsplan, kan findes her.

[3] Der findes en definition af cyberrisici på engelsk i FSB Cyber Lexicon, 12. november 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

er det vigtigt at påpege, at cyberangreb har bestemte karakteristika, der skal tages hensyn til for at sikre, at informationssikkerhedsmæssige foranstaltninger mindsker cyberrisici i tilstrækkelig grad:

a) Cyberangreb er ofte vanskelige at håndtere (dvs. at identificere, beskytte sig mod, opdage, reagere på og komme sig fuldstændigt over) end de fleste andre kilder til IKT- og sikkerhedsrisici, og omfanget af skaderne er vanskeligt at fastlægge.

b) Nogle cyberangreb kan gøre gængse risikostyrings- og driftskontinuitetsordninger samt katastrofeberedskabsordninger ineffektive, da de kan sprede malware til sikkerhedskopisystemer for at gøre dem utilgængelige eller ødelægge sikkerhedskopidata.

c) Tjenesteleverandører, mæglere, (forvaltnings-) organer og mellemled kan blive kanaler, som spreder cyberangreb. Smitsomme, lydløse trusler kan bruge sammenkoblingsmuligheder via tredjeparters telekommunikationsforbindelser til at sprede sig til et selskabs IKT-system. Et sammenkoblet selskab med en lav egen relevans kan blive sårbar og en kilde til risikospredning, hvilket kan føre til systemiske effekter. Hvis princippet om det svageste led skal overholdes, er cybersikkerhed ikke kun noget, som store markedsdeltagere eller udbydere af kritiske tjenesteydelser bør bekymre sig om.

9. Målet med disse retningslinjer er at:

a) give markedsdeltagere afklaring og gennemsigtighed omkring de forventede minimumsoplysninger og cybersikkerhedskapaciteter, dvs. sikkerhedsgrundlaget

b) undgå potentiel regelarbitrage

c) fremme ensartet tilsyn vedrørende de forventninger og processer, der finder anvendelse i forbindelse med IKT-sikkerhed og -ledelsesstyring, som en nøgle til korrekt IKT- og sikkerhedsrisikostyring.

Retningslinjer for IKT-sikkerhed og -ledelsesstyring

Indledning

1. EIOPA udsteder disse retningslinjer i medfør af artikel 16 i forordning (EU) nr. 1094/2010[4], som er rettet til tilsynsmyndighederne, for at vejlede om, hvordan forsikrings- og genforsikringsselskaber (herefter kaldet "selskaber") bør anvende ledelseskravene angivet i direktiv 2009/138/EF[5] ("Solvens II-direktivet") og i Kommissionens delegerede forordning (EU) nr. 2015/35[6] ("delegeret forordning") i forbindelse med IKT-sikkerhed og -ledelsesstyring. Disse retningslinjer bygger derfor på bestemmelserne om ledelse fastlagt i artikel 41, 44, 46, 47, 132 og 246 i Solvens II-direktivet og artikel 258 til 260, 266, 268 to 271 og 274 i den delegerede forordning. Derudover bygger disse retningslinjer også på vejledningen i EIOPA's retningslinjer for ledelsessystem (EIOPA-BoS-14/253)[7] og EIOPA's retningslinjer for outsourcing til cloududbydere (EIOPA-BoS-19/270)[8].
2. Retningslinjerne finder anvendelse på såvel de enkelte selskaber som på koncernerne.[9]
3. Kompetente myndigheder bør under overholdelse og tilsyn med overholdelse af disse retningslinjer tage hensyn til proportionalitetsprincippet[10], som bør sikre, at organisatoriske ordninger, herunder dem knyttet til IKT-sikkerhed og -ledelsesstyring, er proportionale med arten, omfanget og kompleksiteten af de relaterede risici, som selskaberne udsættes for eller kan blive udsat for.
4. Disse retningslinjer bør læses sammen med og med forbehold for Solvens II-direktivet, den delegerede forordning, EIOPA's retningslinjer for ledelsessystem og EIOPA's retningslinjer for outsourcing til cloududbydere. Det er hensigten, at disse retningslinjer skal være neutrale i forbindelse med teknologi og metode.

Definitioner

5. For begreber, der ikke er defineret i disse retningslinjer, er betydningen den, der er fastlagt i Solvens II-direktivet.
6. I disse retningslinjer gælder følgende definitioner:

[4] Forordning (EU) nr. 1094/2010 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 nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EFT L 331 af 15.12.2010, s. 48).

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

[6] Kommissionens delegerede forordning (EU) 2015/35 af 10. oktober 2014, der supplerer Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 12 af 17.1.2015, s. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Artikel 212, stk. 1, i direktiv 2009/138/EF.

[10] Artikel 29, stk. 3, i direktiv 2009/138/EF.

Aktivejer	Person eller enhed med ansvar for og ret til et informations- og IKT-aktiv.
Tilgængelighed	Indebærer at være tilgængelig og anvendelig på anmodning(aktualitet) af en godkendt enhed.
Fortrolighed	Indebærer at oplysninger ikke gøres tilgængelige eller afsløres for uautoriserede enkeltpersoner, enheder, processer eller systemer.
Cyberangreb	Enhver form for hacking, som fører til et offensivt/skadeligt forsøg på at ødelægge, afsløre, ændre, deaktivere, stjæle eller få uautoriseret adgang til eller gøre uautoriseret brug af et informationsaktiv, som er rettet mod IKT-systemer.
Cybersikkerhed	Beskyttelse af informations og/eller informationssystemers fortrolighed, integritet og tilgængelighed igennem cybermediet.
IKT-aktiv	Et aktiv bestående af enten software eller hardware, som findes i forretningsmiljøet.
IKT-projekter	Ethvert projekt eller en del heraf, når IKT-systemer og -tjenester ændres, erstattes eller gennemføres.
IKT-risici og sikkerhedsrisiko	En tabsrisiko (et delkomponent af driftsrisici) som følge af fortrolighedsbrud, manglende integritet af systemer og data, deres utilstrækkelighed eller utilgængelighed eller manglende evne til at ændre IKT inden for rimelige tids- og omkostningsrammer, når miljøkravene eller de forretningsmæssige krav ændrer sig (dvs. fleksibilitet). Dette omfatter cyberisici og informationssikkerhedsrisici som følge af utilstrækkelige eller ikke-funktionelle interne processer eller eksterne hændelser, herunder cyberangreb eller utilstrækkelig fysisk sikkerhed.
Informationssikkerhed	Beskyttelse af informationers og/eller informationssystemers fortrolighed, integritet og tilgængelighed. Andre egenskaber, såsom ægthed, ansvarlighed, uafviselighed og pålidelighed, kan derudover også inddrages.
IKT-tjenesteydelser	Tjenesteydelser leveret via IKT-systemer og tjenesteudbydere til en eller flere interne eller eksterne brugere.

IKT-systemer	Et sæt af applikationer, tjenester, informationsteknologiaktiver, IKT-aktiver eller andre komponenter, der behandler informationer, hvilket omfatter driftsmiljøet.
Informationsaktiv	En samling af oplysninger i enten fysisk eller elektronisk form, som er værd at beskytte.
Integritet	Sikring af nøjagtighed og fuldstændighed.
Drifts- eller sikkerhedshændelse	En entydig begivenhed eller en række hændelser, der ikke er planlagt, som har eller sandsynligvis vil have en negativ indvirkning på IKT-systemer og -tjenester med hensyn til integritetet, tilgængelighed og fortrolighed.
Tjenesteyder	En tredjepartsenhed, der udfører en procedure, tjenesteydelse eller aktivitet eller dele deraf under en outsourcingaftale.
Gennemtrængningsprøvning på baggrund af trusler	Et kontrolleret forsøg på at kompromittere en enheds cyberrobusthed ved at simulere taktikker, teknikker og procedurer, som benyttes af aktører i virkeligheden. Det er baseret på et målrettet trusselsbillede og fokuserer på personer, processer og teknologi hos en enhed med minimal forkundskab og indvirkning på driften.
Sårbarhed	En svaghed, modtagelighed eller mangel ved et aktiv eller en foranstaltning, som kan udnyttes af én eller flere trusler.

7. Disse retningslinjer finder anvendelse fra den 1. juli 2021.

Retningslinje 1 – Proportionalitet

8. Selskaberne bør gøre brug af disse retningslinjer på en måde, som er proportional med arten, omfanget og kompleksiteten af de risici, der er en del af deres virksomhed.

Retningslinje 2 – IKT inden for ledelsesstyringssystemet

9. Administrations-, forvaltnings- eller tilsynsorganet ("AMSB") bør sikre, at selskabernes ledelsessystem, navnlig risikostyringssystemet og det interne kontrolsystem, haandteres selskabernes IKT- og sikkerhedsrisici i tilstrækkelig grad.

10. AMSB bør sikre, at selskabets ansatte er tilstrækkeligt stort og kvalificeret til løbende at understøtte deres operationelle IKT-behov, IKT- og risikostyringsprocesser og sikre gennemførelsen af deres IKT-strategi. Desuden bør

personale regelmæssigt modtage passende uddannelse i IKT- og sikkerhedsrisici, herunder informationssikkerhed, som fastlagt i retningslinje 13.

11. AMSB bør sikre, at de tildelte ressourcer er tilstrækkelige til at opfylde ovenstående krav.

Retningslinje 3 - IKT-strategi

12. AMSB har det overordnede ansvar for at opstille og godkende selskabernes skriftlige IKT-strategi som en del af og i overensstemmelse med deres overordnede forretningsstrategi samt for at føre tilsyn med kommunikation og implementering i forbindelse hermed.

13. IKT-strategien bør som minimum definere:

    a) hvordan selskabernes IKT bør udvikles, så den effektivt støtter og implementerer deres forretningsstrategi, inklusive udviklingen af den organisatoriske opbygning, forretningsmodeller, IKT-systemet og nøgleafhængigheder over for tjenesteudbydere

    b) udviklingen af IKT-arkitekturen, inklusive afhængigheder over for tjenesteudbydere

    c) klare målsætninger for informationssikkerhed med fokus på IKT-systemer og -tjenester, personale og processer.

14. Selskaberne bør sikre, at IKT-strategien implementeres, vedtages og kommunikeres rettidigt til al relevant personale og tjenesteudbydere, alt efter omstændighederne.

15. Selskaberne bør oprette en proces til at overvåge og måle effektiviteten af implementeringen af IKT-strategien. Den proces bør gennemgås og ajourføres regelmæssigt.

Retningslinje 4 – IKT og sikkerhedsrisici inden for risikostyringssystemet

16. AMSB har det overordnede ansvar for at etablere et effektivt system til at forvalte IKT- og sikkerhedsrisici som en del af selskabets samlede risikostyringssystem. Dette omfatter bestemmelse af risikotolerancen for disse risici, i medfør af selskabets risikostrategi, og en regelmæssig skriftlig rapport om resultatet af risikostyringsprocessen, der er adresseret til AMSB.

17. Som en del af deres overordnede risikostyringssystem bør selskaberne i forbindelse med IKT- og sikkerhedsrisici (ved fastsættelse af IKT-beskyttelseskravene som beskrevet nedenfor) som minimum overveje følgende:

    a) Selskaberne bør med regelmæssige ajourføringer kortlægge deres forretningsprocesser og -aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver) med henblik på at udpege, hvor vigtige de er og deres indbyrdes afhængighed vedrørende IKT- og sikkerhedsrisici.

    b) Selskaberne bør udpege og måle alle relevante IKT- og sikkerhedsrisici, de udsættes for, og klassificere de identificerede forretningsprocesser og -aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver) ud fra, hvor kritisk en karakter, de har. Selskaberne bør også som minimum vurdere beskyttelseskravene til fortrolighed, integritet og tilgængelighed for disse forretningsprocesser og -

aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver) Aktivejere, som er ansvarlige for aktivernes klassifikation, bør udpeges.

c) De metoder, som bruges til at bestemme kritikaliteten samt det krævede beskyttelsesniveau, navnlig vedrørende beskyttelsesmålene for integritet, tilgængelighed og fortrolighed, bør sikre, at de resulterende beskyttelseskrav er konsistente og fyldestgørende.

d) Målingen af IKT- og sikkerhedsrisici bør udføres på baggrund af de definerede kriterier for IKT- og sikkerhedsrisici under hensyntagen til kritikaliteten i deres forretningsprocesser og -aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver), omfanget af kendte sårbarheder og tidligere hændelser, som har påvirket selskabet.

e) Vurderingen af IKT- og sikkerhedsrisici bør udføres og dokumenteres regelmæssigt. Denne vurdering bør også udføres inden enhver ændring af infrastruktur, processer eller procedurer, som påvirker forretningsprocesser og -aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver).

f) På baggrund af deres risikovurdering bør selskaberne som minimum definere og implementere foranstaltninger til at forvalte de identificerede IKT- og sikkerhedsrisici og beskytte informationsaktiver i overensstemmelse med deres klassificering. Dette bør inkludere en definition af foranstaltninger til at forvalte de resterende risici.

18. Resultaterne af styringsprocessen for IKT- og sikkerhedsrisici bør godkendes af AMSB og inkluderes i processen med driftsmæssig risikostyring som en del af selskabets samlede risikostyring.

Retningslinje 5 – Revision

19. Selskabernes ledelse, systemer og processer for deres IKT- og sikkerhedsrisici bør kontrolleres periodisk i overensstemmelse med selskabernes revisionsplan[11] af revisorer med tilstrækkelig viden, færdigheder og ekspertise inden for IKT- og sikkerhedsrisici til uafhængigt at kunne give en forsikring om deres effektivitet til AMSB. Hyppigheden af og fokus på sådanne revisioner bør stå i et rimeligt forhold til de relevante IKT-risici og sikkerhedsrisici.

Retningslinje 6 – Informationssikkerhedspolitik og -foranstaltninger

20. Selskaberne bør udarbejde en skriftlig informationssikkerhedspolitik, som er godkendt af AMSB og definerer de regler og principper på højt niveau, der beskytter fortroligheden, integriteten og tilgængeligheden af selskabernes oplysninger med henblik på at støtte gennemførelsen af en IKT-strategi.

21. Politikken bør omfatte en beskrivelse af de vigtigste roller og ansvarsområder i forbindelse med styring af informationssikkerhed, og den bør fastsætte krav til personale, processer og teknologi i forbindelse med informationssikkerhed, idet det anerkendes, at medarbejdere på alle niveauer har et ansvar for at sikre selskabernes informationssikkerhed.

[11] Artikel 271 i den delegerede forordning.

22. Politikken bør kommunikeres inden for selskabet og bør gælde for alt ansatte. Alt efter omstændighederne bør informationssikkerhedspolitikken eller dele af den også kommunikeres og gælde for tjenesteudbydere.

23. På baggrund af politikken bør selskaberne etablere og implementere mere specifikke sikkerhedsprocedurer og informationssikkerhedsforanstaltninger for *bl.a.* at mindske de IKT- og sikkerhedsrisici, de udsættes for. Disse procedurer og informationssikkerhedsforanstaltninger bør inkludere alle processerne angivet i disse retningslinjer, hvor det er relevant.

Retningslinje 7 – Informationssikkerhedsfunktion

24. Selskaberne bør inden for deres ledelsessystem og i henhold til proportionalitetsprincippet etablere en informationssikkerhedsfunktion, hvor en udpeget person pålægges ansvaret. Selskabet bør sikre, at denne informationssikkerhedsfunktion er uafhængig og objektiv ved at sørge for, at den er behørigt adskilt fra IKT-udvikling og -driftsprocesser. Disse funktioner bør rapportere til AMSB.

25. Informationssikkerhedsfunktionens opgaver er typisk at:

    a) støtte AMSB med udpegelse og ajourføring af informationssikkerhedspolitikken for selskaberne og kontrollere dens anvendelse

    b) rapportere og rådgive AMSB regelmæssigt og på ad hoc-basis om informationssikkerhedens status og udvikling

    c) overvåge og gennemgå implementeringen af informationssikkerhedsforanstaltningerne

    d) sikre, at informationssikkerhedskravene overholdes, når tjenesteudbydere benyttes

    e) sikre, at alle medarbejdere og tjenesteudbydere, som har adgang til informationer og systemer, oplyses tilstrækkeligt om informationssikkerhedspolitikken, for eksempel gennem uddannelse og informationsmøder

    f) koordinere undersøgelse af driftsmæssige og sikkerhedsrelaterede hændelser og rapportere dem, der er relevante, til AMSB.

Retningslinje 8 – Logisk sikkerhed

26. Selskaberne bør definere, dokumentere og implementere procedurer for logisk adgangskontrol eller logisk sikkerhed (identitets- og adgangsstyring) i overensstemmelse med beskyttelseskravene som defineret i retningslinje 4. Disse procedurer bør implementeres, håndhæves, overvåges og periodisk gennemgås og bør også omfatte kontrol til 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 princippet om funktionsadskillelse: selskaberne bør forvalte adgangsrettigheder, herunder fjernadgang til informationsaktiver og deres støttesystemer, på et "need to know"-grundlag. Brugerne bør tildeles minimumsadgangsrettigheder, der er strengt nødvendige for udførelsen af deres opgaver ("least privilege"-princippet), dvs. for at forhindre uberettiget adgang til data, eller at en bruger

tildeles kombinationer af adgangsrettigheder, som kan anvendes til at omgå kontrolforanstaltninger (princippet om "funktionsadskillelse").

b) Brugeransvarlighed: Selskaberne bør så vidt muligt begrænse brugen af generiske og delte brugerkonti og sikre, at brugere på ethvert tidspunkt kan identificeres og spores tilbage til en ansvarlig fysisk person eller en godkendt opgave for de handlinger, der udføres i IKT-systemerne.

c) Privilegerede adgangsrettigheder: Selskaberne bør gennemføre stærke kontrolforanstaltninger i forhold til privilegeret systemadgang ved strengt at begrænse og nøje føre tilsyn med konti med mere omfattende systemadgang (f.eks. administratorkonti).

d) Fjernadgang: For at opnå sikker kommunikation og reducere risikoen bør fjernadgang til kritiske IKT-systemer kun tildeles efter "need to know"-princippet, og når der anvendes stærke autentificeringsløsninger.

e) Logføring over brugeraktiviteter: Brugeres aktiviteter bør logføres og overvåges på en måde, der er proportionel med risikoen, og som minimum omfatter privilegerede brugeres aktiviteter. Adgangslogs bør sikres for at forhindre uautoriseret ændring eller sletning og bør opbevares i en periode, der modsvarer den kritiske karakter af de identificerede forretningsfunktioner, understøttende processer og informationsaktiver, uden at dette berører opfyldelsen af opbevaringskravene i EU-lovgivningen og den nationale lovgivning. Selskaberne bør bruge disse oplysninger til at identificere og undersøge uregelmæssige aktiviteter, der er blevet påvist i forbindelse med udbud af tjenester.

f) Adgangsstyring: Adgangsrettigheder bør tildeles, fjernes og ændres rettidigt, jf. i forvejen fastsatte godkendelsesrutiner med deltagelse af den berørte ejer af informationsaktivet. Hvis adgangen ikke længere er nødvendig, bør adgangsrettighederne omgående ophæves.

g) Adgangsvurdering: Adgangsrettighederne bør gennemgås regelmæssigt for at sikre, at brugerne ikke har for omfattende rettigheder, og at adgangsrettighederne trækkes tilbage/fjernes, når der ikke længere er behov for dem.

h) Tildeling, ændring og tilbagekaldelse af adgangsrettigheder bør dokumenteres på en måde, som fremmer forståelse og analyse.

i) Autentificeringsmetoder: Selskaberne 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, der gives adgang til. Dette bør som minimum omfatte stærke kodeord eller stærkere autentificeringsmetoder (f.eks. tofaktorgodkendelse) baseret på den relevante risiko.

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

Retningslinje 9 – Fysisk sikkerhed

28. Selskabernes fysiske sikkerhedsforanstaltninger (f.eks. beskyttelse mod strømsvigt, brand, vand og uautoriseret fysisk adgang) bør defineres, dokumenteres og implementeres for at beskytte deres lokaliteter, datacentre og følsomme områder mod uautoriseret adgang og fra miljøfarer.

29. 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 trækkes tilbage/fjernes.

30. 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.

Retningslinje 10 – Sikkerhed for IKT-drift

31. Selskaberne bør implementere procedurer, der sikrer fortrolighed, integritet og tilgængelighed for IKT-systemer og -tjenester med henblik på at minimere de konsekvenser, som sikkerhedsproblemer har for levering af IKT-tjenester. Disse procedurer bør på passende vis omfatte følgende foranstaltninger:

    a) identifikation af potentielle sårbarheder, som bør evalueres og afhjælpes ved at sikre, at IKT-systemer er opdateret, herunder software, der leveres af selskaberne til deres interne og eksterne brugere, ved at installere kritiske sikkerhedspatches, inklusive opdateringer af antivirusdefinitioner, eller ved at implementere kompenserende kontroller

    b) implementering af sikre basiskonfigurationer for alle kritiske komponenter, såsom styresystemer, databaser, routere eller omkoblere

    c) implementering af netværkssegmentering, systemer til at forebygge datalækage og kryptering af netværkstrafik (i overensstemmelse med klassifikationen af informationsaktivet)

    d) implementering af "endpoint protection" (beskyttelse af endepunkter), herunder servere, arbejdsstationer og mobile enheder. Selskaberne bør vurdere, om et endepunkt opfylder de sikkerhedsstandarder, som de har fastlagt, før det tildeles adgang til virksomhedens netværk

    e) sikring af, at mekanismer til integritetskontrol er på plads til at bekræfte integriteten af IKT-systemer

    f) kryptering af data i hvile og i transit (i overensstemmelse med klassifikationen af informationsaktiver).

Retningslinje 11 – Sikkerhedsovervågning

32. Selskaberne bør etablere og implementere procedurer og processer for løbende at overvåge aktiviteter, som påvirker selskabernes informationssikkerhed. Overvågningen bør som minimum omfatte følgende:

    a) interne og eksterne faktorer, herunder forretningsfunktioner og administrative IKT-funktioner

    b) transaktioner fra tjenesteudbydere, andre enheder og interne brugere

    c) potentielle interne og eksterne trusler.

33. På baggrund af overvågningen bør selskaberne implementere passende og effektive kapacitet til at opdage, rapportere om og imødegå uregelmæssige aktiviteter og trusler, såsom fysisk eller logisk indtrængen, brud i forhold til fortrolighed, informationsaktivernes integritet og tilgængelighed, skadelig kode og alment kendte sårbarheder for software og hardware.

34. Rapporterne fra sikkerhedsovervågningen bør hjælpe selskaberne med at forstå arten af både driftsmæssige og sikkerhedsmæssige hændelser, identificere tendenser og støtte selskabernes interne undersøgelser og gøre dem i stand til at træffe passende beslutninger.

Retningslinje 12 – Gennemgange, vurderinger og test af informationssikkerhed

35. Selskaberne skal foretage en række forskellige gennemgange, vurderinger og test af informationssikkerhed for at sikre en effektiv identifikation af sårbarheder for deres IKT-systemer og -tjenester. F.eks. kan selskaberne foretage gabanalyser i forhold til informationssikkerhedsstandarder, gennemgange af overensstemmelse, interne og eksterne revisioner af informationssystemer eller gennemgange af fysisk sikkerhed.

36. Selskaberne bør etablere og implementere rammer for test af informationssikkerhed, som validerer robustheden og effektiviteten af informationssikkerhedsforanstaltningerne. Selskaberne bør sikre, at disse rammer tager højde for trusler og sårbarheder, som identificeres gennem trusselsovervågning og vurderingsprocessen for IKT-risici og sikkerhedsrisici.

37. Testning bør udføres på en sikker måde og af uafhængige testere med tilstrækkelig viden, færdigheder og ekspertise inden for testning af informationsmæssige sikkerhedsforanstaltninger.

38. Selskaberne bør regelmæssigt gennemføre test. Testningens omfang, hyppighed og metode (såsom gennemtrængningsprøvning, herunder gennemtrængningsprøvning på baggrund af trusler) bør modsvare det identificerede risikoniveau. Testning af kritiske IKT-systemer og sårbarhedsscanninger børe gennemføres hvert år.

39. Selskaberne 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. Selskaberne bør overvåge og evaluere resultaterne af de udførte sikkerhedstest og opdatere deres sikringsforanstaltninger i overensstemmelse hermed uden unødig forsinkelse, når der er tale om kritiske IKT-systemer.

Retningslinje 13 – Informationssikkerhedsuddannelse og informationskurser

40. Selskaberne bør etablere uddannelsesprogrammer om informationssikkerhed for al personale, herunder AMSB, for at sikre, at de er uddannet til at varetage deres arbejdsopgaver og ansvarsområder, og dermed reducere menneskelige fejl, tyveri, svindel, misbrug eller tab. Selskaberne bør sikre, at uddannelsesprogrammerne regelmæssigt tilbyder uddannelse til al personale.

41. Selskaberne bør etablere og implementere periodiske informationskurser om sikkerhed for at uddanne deres personale, herunder AMSB, i, hvordan informationssikkerhedsrelaterede risici håndteres.

Retningslinje 14 – IKT-driftsledelse

42. Selskaberne bør forvalte deres IKT-drift på baggrund af IKT-strategien. Det bør defineres i dokumenter, hvordan selskaberne benytter, overvåger og kontrollerer IKT-systemerne og IKT-tjenesterne, herunder dokumentering af kritiske IKT-processer, -procedurer og -drift.

43. Selskaberne bør implementere lognings- og overvågningsprocedurer for kritisk IKT-drift for at gøre det muligt at opdage, analysere og rette fejl.

44. Selskaberne bør opretholde en ajourført fortegnelse over deres IKT-aktiver. Fortegnelsen over IKT-aktiver bør være tilstrækkelig detaljeret til at sikre hurtig identifikation af et IKT-aktiv, dets placering, sikkerhedsklassifikation og ejerforhold.

45. Selskaberne bør overvåge og styre IKT-aktivernes livscyklus for at sikre, at de fortsat opfylder og understøtter forretnings- og risikostyringskrav. Selskaberne bør overvåge, om deres leverandører eller interne udviklere yder support til deres IKT-aktiver, og hvorvidt alle relevante patches og opgraderinger installeres på grundlag af en dokumenteret proces. Risici som følge af forældede eller ikkeunderstøttede IKT-aktiver bør evalueres og mindskes. Afviklede IKT-aktiver bør behandles og bortskaffes på sikker vis.

46. Selskaberne 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.

47. Selskaberne bør fastlægge og implementere procedurer for sikkerhedskopiering og gendannelse af data og IKT-systemer for at sikre, at de kan gendannes efter behov. Omfanget og hyppigheden af sikkerhedskopier 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 sikkerhedskopierings- og gendannelsesprocedurer bør foretages regelmæssigt.

48. Selskaberne bør sikre, at sikkerhedskopier af dataene og IKT-systemet lagres på én eller flere placeringer, som ikke er den primære lokalitet. Disse placeringer skal være sikre og tilstrækkeligt langt væk fra den primære lokalitet til, at de ikke udsættes for de samme risici.

Retningslinje 15 – Håndtering af IKT-hændelser og -problemer

49. Selskaberne bør etablere og implementere en proces for hændelses- og problemhåndtering med henblik på at overvåge og logge operationelle eller sikkerhedsmæssige hændelser og gøre det muligt for selskaberne at fortsætte eller genoptage kritiske forretningsfunktioner og -processer, når der opstår driftsforstyrrelser.

50. Selskaberne bør bestemme passende kriterier og grænser for at klassificere en begivenhed som en operationel eller sikkerhedsmæssig hændelse samt tidlige varslingsindikatorer som muliggør tidlig påvisning af disse hændelser.

51. For at minimere virkningen af utilsigtede hændelser og muliggøre rettidig genopretning bør selskaberne etablere passende processer og organisatoriske strukturer for at sikre en konsekvent og integreret overvågning, håndtering og opfølgning på operationelle og sikkerhedsmæssige hændelser, der sikrer, at de grundlæggende årsager identificeres og behandles, og at korrigerende foranstaltninger træffes for at forhindre, at hændelsen gentages. Processen for hændelses- og problemhåndtering bør som minimum fastlægge:

    a) procedurer for identifikation, sporing, registrering, kategorisering og klassificering af hændelser efter en prioritetsrækkefølge, der er defineret af selskabet, og baseret på forretningens kritikalitet og serviceaftaler

    b) roller og ansvar for forskellige hændelsesscenarier (f.eks. fejl, reduceret funktionalitet og cyberangreb)

c) en procedure for problemhåndtering med henblik på at identificere, analysere og løse den grundlæggende årsag til en eller flere hændelser. Selskaberne bør analysere operationelle og sikkerhedsmæssige hændelser, 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:

   i. at hændelser med potentielt stor negativ indvirkning på kritiske IKT-systemer og IKT-tjenester indberettes til den relevante øverste ledelse

   ii. at AMSB underrettes på ad hoc-basis i tilfælde af væsentlige hændelser, og som minimum underrettes om konsekvenserne, reaktionen og de yderligere kontrolforanstaltninger, der bliver indført som følge 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, inklusive hændelsesrapportering, til eksterne parter (f.eks. kunder, andre markedsdeltagere, relevante (tilsyns-) myndigheder, alt efter hvad der er relevant, og i overensstemmelse med gældende lovgivning).

Retningslinje 16 – IKT-projektstyring

52. Selskaberne bør implementere en IKT-projektmetode (herunder uafhængige overvejelser om sikkerhedskrav) med en passende ledelsesproces og ledelse af projektgennemførelsen for effektivt at støtte gennemførelsen af IKT-strategien via IKT-projekter.

53. Selskaberne bør behørigt overvåge og afbøde de risici, der følger af porteføljen af IKT-projekter, idet der også bør tages hensyn til de risici, der kan opstå som følge af indbyrdes afhængigheder mellem forskellige projekter og fra flere projekters afhængighed af de samme ressourcer og/eller den samme ekspertise.

Retningslinje 17 – Erhvervelse og udvikling af IKT-systemer

54. Selskaberne bør udvikle og gennemføre en proces for styring af erhvervelse, udvikling og vedligeholdelse af IKT-systemer med henblik på at sikre, at fortroligheden, integriteten og tilgængeligheden af de data, som skal behandles, sikres fuldt ud, og at de definerede beskyttelseskrav er opfyldt. Denne proces bør udformes på grundlag af en risikobaseret tilgang.

55. Selskaberne bør sikre, at de funktionelle og ikke-funktionelle krav (herunder informationssikkerhedskrav) og tekniske mål er klart defineret, inden systemanskaffelse og udviklingsaktiviteter finder sted.

56. Selskaberne bør sikre, at foranstaltninger er på plads til at forhindre utilsigtet ændring eller tilsigtet manipulation af IKT-systemerne under udvikling.

57. Selskaberne bør have en metode til test og godkendelse af IKT-systemer, IKT-tjenester og informationssikkerhedsforanstaltninger.

58. Selskaberne bør på passende vis teste IKT-systemer, IKT-tjenester og informationssikkerhedsforanstaltninger med henblik på at identificere potentielle sikkerhedssvagheder, -overtrædelser og -hændelser.

59. Selskaberne bør sikre adskillelse af produktionsmiljøerne fra udviklings- og testmiljøer og andre ikkeproduktionsmiljøer.

60. Selskaberne bør gennemføre foranstaltninger til at beskytte integriteten af IKT-systemers kildekode (hvis det foreligger). De bør også grundigt dokumentere udviklingen, implementeringen, driften og/eller konfigurationen af IKT-systemerne på omfattende vis for at mindske unødvendig afhængighed af eksperter på området.

61. Selskabernes 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. forretningsadministrerede applikationer eller slutbrugerapplikationer) ud fra en risikobaseret tilgang. Selskaberne bør føre et register over disse applikationer, der understøtter kritiske forretningsfunktioner eller -processer.

Retningslinje 18 - IKT-ændringshåndtering

62. Selskaberne bør indføre og implementere en IKT-ændringshåndtering for at sikre, at alle ændringer af IKT-systemer registreres, vurderes, testes, godkendes, autoriseres og gennemføres på en kontrolleret måde. Ændringer i forbindelse med hastende IKT-ændringer eller akutte IKT-ændringer bør kunne spores og meddeles efterfølgende til den relevante aktivejer med henblik på efterfølgende analyse.

63. Selskaberne bør løbende vurdere, om ændringer i det eksisterende driftsmiljø påvirker de eksisterende sikringsforanstaltninger eller kræver indførelse af yderligere foranstaltninger for at afbøde risikoen herved. Disse ændringer bør ske i overensstemmelse med selskabernes formelle ændringshåndteringsproces.

Retningslinje 19 – Forvaltning af driftskontinuitet

64. Som en del af selskabets overordnede driftskontinuitetspolitik er AMSB ansvarlig for at opstille og godkende selskabets IKT-kontinuitetspolitik. IKT-kontinuitetspolitikken bør på passende vis kommunikeres inden for selskaberne og bør finde anvendelse for alle relevante medarbejdere og, om relevant, for tjenesteudbydere.

Retningslinje 20 – Konsekvensanalyse

65. Som del af en sund forvaltning af driftskontinuiteten bør selskaberne gennemføre en konsekvensanalyse for at vurdere selskabets eksponering for alvorlige forretningsforstyrrelser og deres potentielle konsekvenser, kvantitativt og kvalitativt, ved brug af interne og/eller eksterne data og scenarieanalyse. Konsekvensanalyse bør også tage hensyn til alvorligheden af de udpegede og klassificerede forretningsprocesser og -aktiviteter, forretningsfunktioner, roller og aktiver (f.eks. informationsaktiver og IKT-aktiver) og deres indbyrdes afhængigheder i henhold til retningslinje 4.

66. Selskaberne bør sikre, at deres IKT-systemer og IKT-tjenester er udformet og tilpasset deres konsekvensanalyse, f.eks. ved at sikre redundans af visse kritiske komponenter for at undgå driftsforstyrrelser forårsaget af hændelser, der påvirker disse komponenter.

Retningslinje 21 – Kontinuitetsplanlægning

67. Selskabernes overordnede kontinuitetsplaner bør tage hensyn til væsentlige risici, som kan have en negativ indvirkning på IKT-systemer og IKT-tjenester. Planerne bør støtte målsætninger om at beskytte og, om nødvendigt, genetablere fortrolighed, integritet og tilgængelighed for selskabets forretningsprocesser og -aktiviteter, forretningsfunktioner, -roller og -aktiver (f.eks. informationsaktiver og IKT-aktiver). Selskaberne bør samarbejde med relevante interne og eksterne interessenter, afhængigt af hvad der er passende, under udarbejdelsen af disse planer.

68. Selskaberne bør fastlægge kontinuitetsplaner for at sikre, at de kan reagere på passende vis på potentielle fejlscenarier inden for målet for genopretningstiden (det maksimale tidsforløb, i løbet af hvilket et system eller en proces skal være genoprettet efter en hændelse) og målet for genopretningspunktet (det maksimale tidsforløb, i løbet af hvilket data kan gå tabt i tilfælde af en hændelse ved et prædefineret serviceniveau).

69. Selskaberne bør overveje flere forskellige scenarier i deres kontinuitetsplan, inklusive ekstreme men plausible scenarier og cyberangrebsscenarier, og vurdere de potentielle konsekvenser ved sådanne scenarier. På grundlag af disse scenarier bør selskaberne beskrive, hvordan kontinuiteten af IKT-systemer og -tjenester samt selskabernes informationssikkerhed sikres.

Retningslinje 22 – Beredskabs- og genopretningsplaner

70. På grundlag af konsekvensanalysen og plausible scenarier bør selskaberne udarbejde beredskabs- og genopretningsplaner. Disse planer bør beskrive de forhold, der kan føre til aktivering af planerne, og de foranstaltninger, der skal træffes for at sikre tilgængelighed, kontinuitet og genopretning af, som minimum, selskabernes kritiske IKT-systemer, IKT-tjenester og data. Beredskabs- og genopretningsplanerne bør sigte mod at opfylde genopretningsmålene for selskabernes drift.

71. Beredskabs- og genopretningsplanerne bør tage højde for både kort- og, om nødvendigt, langsigtede genopretningsmodeller. Planerne bør, som minimum:

    a) fokusere på at genoprette driften af vigtige IKT-tjenester, forretningsfunktioner, støtteprocesser, informationsaktiver og deres indbyrdes afhængigheder for at undgå negative konsekvenser for selskabets funktion

    b) være dokumenteret og gøres tilgængelige for forretnings- og støtteenhederne og umiddelbart tilgængelige i tilfælde af en nødsituation, herunder en tydelig definition af roller og ansvarsområder

    c) opdateres løbende i overensstemmelse med erfaringerne fra hændelser, test, nyligt identificerede risici og trusler og ændrede genopretningsmål og -prioriteter.

72. 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.

73. Som en del af beredskabs- og genopretningsplanerne bør selskaberne overveje og implementere kontinuitetsforanstaltninger for at afbøde fejl ved tjenesteudbydere, som er af afgørende betydning for kontinuiteten af selskabernes IKT-tjenester (i overensstemmelse med EIOPA's retningslinjer for ledelsessystem og retningslinjer for outsourcing til cloududbydere).

Retningslinje 23 – Testning af planer

74. Selskaberne bør teste deres kontinuitetsplan og sikre, at driften af deres kritiske forretningsprocesser og -aktiviteter, forretningsfunktioner, roller og aktiver (dvs. informationsaktiver) og IKT-aktiver og deres indbyrdes afhængigheder (herunder dem, som tjenesteudbydere leverer) testes regelmæssigt på baggrund af selskabernes risikoprofil.

75. Kontinuitetsplaner bør ajourføres regelmæssigt på grundlag af testresultaterne, det aktuelle trusselsbillede og erfaringerne fra tidligere hændelser. Alle relevante ændringer af genopretningsmål (herunder målet for genopretningstiden og målet for genopretningspunktet) og/eller ændringer af forretningsprocesser og -aktiviteter, forretningsfunktioner, roller og aktiver (dvs. informationsaktiver og IKT-aktiver) bør også inkluderes.

76. Testning af kontinuitetsplaner bør vise, at de er i stand til at opretholde virksomhedens levedygtighed, indtil kritiske driftsfunktioner genoprettes, på baggrund af et foruddefineret serviceniveau eller konsekvenstolerance.

77. Testresultaterne bør dokumenteres, og eventuelle identificerede mangler som følge af testene bør analyseres, afhjælpes og rapporteres til AMSB.

Retningslinje 24 – Krisekommunikationer

78. I tilfælde af forstyrrelser eller nødsituationer og under gennemførelsen af kontinuitetsplanerne bør selskaberne sikre, at de har effektive krisekommunikationsforanstaltninger, således at alle relevante interne og eksterne interessenter, herunder relevante tilsynsmyndigheder, hvis dette kræves jf. national lovgivning, samt relevante tjenesteudbydere, informeres på en rettidig og hensigtsmæssig måde.

Retningslinje 25 – Outsourcing af IKT-tjenester og IKT-systemer

79. Med forbehold for EIOPA's retningslinjer for outsourcing til cloududbydere bør selskaberne sikre, at de relevante krav til IKT-tjenesten eller IKT-systemet opfyldes, når IKT-tjenester og IKT-systemer outsources.

80. I tilfælde af outsourcing af kritiske eller vigtige funktioner bør selskaberne sikre, at tjenesteudbyderens kontraktlige forpligtelser (f.eks. aftaler på kontrakt- eller serviceniveau og opsigelsesbestemmelser i de relevante kontrakter) som minimum omfatter følgende:

    a) passende og proportionale foranstaltninger og målsætninger for informationssikkerhed, herunder krav, såsom minimale informationssikkerhedskrav, specifikationer af selskabernes datalivscyklus, revisions- og adgangsrettigheder samt eventuelle krav vedrørende placering af datacentre og datakrypteringskrav, netværkssikkerhed og sikkerhedsovervågningsprocesser

    b) serviceniveauaftaler for at sikre kontinuiteten af IKT-tjenester og IKT-systemer og præstationsmål under normale omstændigheder samt dem, som findes i beredskabsplaner i tilfælde af serviceafbrydelser

c) procedurer for håndtering af operationelle hændelser og sikkerhedshændelser, herunder eskalering og rapportering.

81. Selskaberne bør kontrollere og anmode om bekræftelse på disse tjenesteudbyderes efterlevelse af sikkerhedsmålene, foranstaltningerne og præstationsmålene.

Bestemmelser om efterlevelse og indberetning

82. Dette dokument indeholder retningslinjer udstedt i henhold til artikel 16 i forordning (EU) nr. 1094/2010. I henhold til artikel 16, stk. 3, i nævnte forordning skal de kompetente myndigheder og selskaberne bestræbe sig mest muligt på at efterleve retningslinjer og henstillinger.

83. Kompetente myndigheder, der efterlever eller agter at efterleve disse retningslinjer, bør på passende måde indarbejde dem i deres lovgivnings- eller tilsynsramme.

84. De kompetente myndigheder skal over for EIOPA bekræfte, om de efterlever eller agter at efterleve disse retningslinjer, og i modsat fald angive begrundelsen for den manglende efterlevelse inden for to måneder efter udstedelsen af de oversatte versioner.

85. Hvis de kompetente myndigheder ikke har reageret inden udløbet af denne frist, vil det blive betragtet som manglende efterlevelse af indberetningskravet, hvilket vil blive indberettet.

Afsluttende bestemmelse om revision

86. Disse retningslinjer vil blive revideret af EIOPA.