EIOPA-BoS-20/600

Riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik

Eiopa – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Tyskland – tel. + 49 69-951119-20;
Fax + 49 69-951119-19, e-post: info@eiopa.europa.eu webbplats: www.eiopa.europa.eu

Innehållsförteckning

Bakgrund

1. Enligt artikel 16 i förordning (EU) nr 1094/2010 får Eiopa utfärda riktlinjer och rekommendationer riktade till behöriga myndigheter och finansinstitut i syfte att upprätta en konsekvent, ändamålsenlig och effektiv tillsynspraxis och säkerställa en gemensam, enhetlig och konsekvent tillämpning av unionsrätten.

2. I enlighet med artikel 16.3 i den förordningen ska behöriga myndigheter och finansinstitut med alla tillgängliga medel söka följa dessa riktlinjer och rekommendationer.

3. Eiopa har identifierat ett behov av att ta fram särskild vägledning om säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (IKT) med avseende på artiklarna 41 och 44 i direktiv 2009/138/EG inom ramen för den analys som gjorts som svar på Europeiska kommissionens handlingsplan för fintech (COM(2018) 0109 final), Eiopas plan för enhetlig tillsyn för 2018–2019[1] och till följd av samspel med flera andra intressenter[2].

4. Såsom rapporteras i det gemensamma rådgivningsdokumentet från de europeiska tillsynsmyndigheterna till Europeiska kommissionen *speglas inte vikten av att sörja för hantering av IKT-risker (inbegripet cyberrisker) på rätt sätt* i Eiopas riktlinjer för företagsstyrningssystem. Det saknas vägledning beträffande viktiga inslag som i allmänhet anses ingå i tillbörlig säkerhet och företagsstyrning avseende IKT.

5. En analys av den nuvarande (lagstiftningsmässiga) situationen i EU med avseende på ovannämnda gemensamma rådgivningsdokument visade att en majoritet av EU:s medlemsstater har infört nationella regler för säkerhet och företagsstyrning avseende IKT. Även om kraven liknar varandra är regelverket fortfarande fragmenterat. Dessutom visade en undersökning av gällande tillsynspraxis att det finns stora skillnader i praxis – från ”ingen särskild tillsyn” till ”stark tillsyn” (inbegripet ”skrivbordskontroller” och ”inspektioner på plats”).

6. Vidare ökar komplexiteten inom IKT och förekomsten av IKT-relaterade incidenter (inbegripet cyberincidenter), liksom de negativa effekterna av sådana incidenter för företags operativa verksamhet. Av detta skäl är hantering av IKT-risker och säkerhetsrisker av avgörande betydelse för ett företag för att det ska uppnå sina strategiska, företagsmässiga och operativa mål liksom målen i fråga om anseende.

7. I försäkringssektorn – både i traditionella och innovativa affärsmodeller – ökar dessutom tilltron på IKT för tillhandahållandet av försäkringstjänster och för företagens normala operativa funktionssätt, t.ex. digitalisering av försäkringssektorn (InsurTech, sakernas internet etc.) och sammankoppling via telekommunikationskanaler (internet, mobila och trådlösa anslutningar och icke-lokala datornät). Detta gör företags verksamhet sårbar för säkerhetsincidenter, däribland cyberattacker, och det är därför viktigt att se till att de är tillräckligt förberedda för att hantera sina IKT-risker och säkerhetsrisker.

8. Genom att erkänna behovet av att företag förbereder sig inför cyberrisker[3] och har en sund cybersäkerhetsram omfattar dessa riktlinjer även cybersäkerhet som en del av företagens åtgärder för informationssäkerhet. Enligt dessa riktlinjer bör cybersäkerhet hanteras som en del av ett företags allmänna hantering av IKT-

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

[2] Den rapport som Eiopa offentliggjort som svar på Europeiska kommissionens handlingsplan för fintech finns här.

[3] För en definition av cyberrisk, se FSB:s cyberlexikon av den 12 november 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

risker och säkerhetsrisker, men det är viktigt att påpeka att cyberattacker har vissa särskilda egenskaper, enligt nedan, vilka bör beaktas för att se till att informationssäkerhetsåtgärderna minskar cyberriskerna på lämpligt sätt:

a) Cyberattacker är ofta svårare att hantera (dvs. att identifiera, säkra, upptäcka, bemöta och helt återhämta sig från) än de flesta andra källor till IKT-risker och säkerhetsrisker. Det är också svårt att fastställa skadornas omfattning.

b) Vissa cyberattacker kan göra allmänna åtgärder för riskhantering och driftskontinuitet liksom rutiner för katastrofåterhämtning verkningslösa, eftersom de kan sprida sabotageprogram till reservsystem för att göra dem oåtkomliga eller förstöra säkerhetskopior.

c) Tjänsteleverantörer, mäklare, (managing) agents och mellanhänder kan fungera som kanaler för spridning av cyberattacker. Smittsamma tysta hot kan använda sammankopplingsmöjligheter via tredjeparts telekommunikationslänkar för att sprida sig till ett företags IKT-system. Ett sammankopplat företag med liten egen relevans kan därför bli sårbart och en källa till riskspridning som kan leda till systemeffekter. Vid iakttagande av principen om den svagaste länken bör cybersäkerhet inte bara vara en fråga för stora marknadsaktörer eller kritiska tjänsteleverantörer.

9. Dessa riktlinjer syftar till att

a) förse marknadsaktörerna med förtydliganden och öppenhet om minsta förväntade information och cybersäkerhetskapacitet, dvs. grundläggande säkerhetsnivå,

b) undvika eventuellt regleringsarbitrage,

c) främja en enhetlig tillsyn vad gäller förväntningar och tillämpliga processer med avseende på säkerhet och företagsstyrning avseende IKT som ingång till en korrekt hantering av IKT-risker och säkerhetsrisker.

Riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik

Inledning

1. I enlighet med artikel 16 i förordning (EU) nr 1094/2010[4] utfärdar Eiopa dessa riktlinjer riktade till tillsynsmyndigheterna för att ge vägledning om hur försäkrings- och återförsäkringsföretag (gemensamt kallade *företag*) bör tillämpa kraven på företagsstyrning som föreskrivs i direktiv 2009/138/EG[5] (nedan kallat *Solvens II-direktivet*) och i kommissionens delegerade förordning (EU) 2015/35[6] (nedan kallad *den delegerade förordningen*) inom ramen för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (IKT). I detta syfte bygger riktlinjerna på bestämmelserna om företagsstyrning i artiklarna 41, 44, 46, 47, 132 och 246 i Solvens II-direktivet och artiklarna 258–260, 266, 268–271 och 274 i den delegerade förordningen. Riktlinjerna bygger även på den vägledning som ges av Eiopa i dess *Riktlinjer för företagsstyrningssystem* (EIOPA-BoS-14/253)[7] och *Riktlinjer om uppdragsavtal med molntjänstleverantörer* (EIOPA-BoS-19/270)[8].
2. Riktlinjerna gäller både enskilda företag och i tillämpliga delar på gruppnivå[9].
3. Behöriga myndigheter bör, när de efterlever eller övervakar efterlevnad av dessa riktlinjer, ta hänsyn till proportionalitetsprincipen[10], som ska säkerställa att åtgärder för företagsstyrning, också de som gäller säkerhet och företagsstyrning avseende IKT, står i proportion till arten, omfattningen och komplexiteten för de motsvarande risker som företag står eller kan ställas inför.
4. Dessa riktlinjer bör läsas tillsammans med och utan att de påverkar tillämpningen av Solvens II-direktivet, den delegerade förordningen, Eiopas riktlinjer för företagsstyrningssystem och Eiopas riktlinjer om uppdragsavtal med molntjänstleverantörer. Riktlinjerna är avsedda att vara teknik- och metodneutrala.

Definitioner

5. Termer som inte definieras i dessa riktlinjer har den betydelse som anges i Solvens II-direktivet.
6. I dessa riktlinjer gäller följande definitioner:

[4] Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48).

[5] Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

[6] Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II) (EUT L 12, 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 212.1 i direktiv 2009/138/EG.

[10] Artikel 29.3 i direktiv 2009/138/EG.

Tillgångsägare	Person eller enhet med ansvar och befogenhet för en informationstillgång och IKT-tillgång.
Tillgänglighet	Egenskapen att vara tillgänglig och användbar på begäran (aktualitet) av en behörig enhet.
Konfidentialitet	Egenskap att information varken tillgängliggörs eller lämnas ut till obehöriga personer, enheter, processer eller system.
Cyberattack	Alla former av hackande som leder till ett offensivt/skadligt försök att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller på ett obehörigt sätt använda en informationstillgång som riktar sig mot IKT-system.
Cybersäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem via ett cybermedium.
IKT-tillgång	En programvaru- eller maskinvarutillgång som finns i affärsmiljön.
IKT-projekt	Ett projekt eller en del av ett projekt där IKT-system och IKT-tjänster ändras, byts ut eller införs.
IKT-risk och säkerhetsrisk	Som en delkomponent i operativ risk; risk för förlust som beror på brott mot konfidentialiteten, på att integriteten hos system och data inte fungerar, på att system och data är olämpliga eller otillgängliga, eller på oförmåga att ändra på IKT:n inom rimlig tid och till rimliga kostnader när miljö- eller verksamhetskraven förändras (dvs. flexibilitet). Detta inkluderar cyberrisker och informationssäkerhetsrisker till följd av otillräckliga eller icke-funktionella interna processer eller externa händelser, däribland cyberattacker eller otillräcklig fysisk säkerhet.
Informationssäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem. Därtill kan även andra egenskaper vara aktuella, såsom autenticitet, ansvar, oavvislighet och tillförlitlighet.
IKT-tjänster	Tjänster som tillhandahålls via IKT-system och tjänsteleverantörer till en eller flera interna eller externa användare.

IKT-system	Uppsättning program, tjänster, it-tillgångar, IKT-tillgångar eller andra komponenter som hanterar information, vilket inkluderar driftsmiljön.
Informationstillgång	En samling uppgifter, antingen materiella eller immateriella, som är värda att skyddas.
Integritet	Egenskap för noggrannhet och fullständighet.
Operativa incidenter eller säkerhetsincidenter	En enskild händelse eller en serie sammanhängande oplanerade händelser som har eller sannolikt kommer att ha en negativ inverkan på IKT-systemens och IKT-tjänsternas integritet, tillgänglighet och konfidentialitet.
Tjänsteleverantör	En enhet från tredje part som utför en process, tjänst eller verksamhet, eller delar därav, inom ramen för ett uppdragsavtal.
Hotstyrd penetrationsprovning	Ett kontrollerat försök att äventyra en enhets cyberresiliens genom att simulera taktiker, metoder och rutiner hos verkliga fientliga aktörer. Den grundas på riktade underrättelser om hot och fokuserar på en enhets personal, processer och teknik, med minimal förkunskap om och inverkan på verksamheten.
Sårbarhet	En svaghet, känslighet eller brist i en tillgång eller kontroll som kan utnyttjas av ett eller flera hot.

7. Dessa riktlinjer ska tillämpas från och med den 1 juli 2021.

Riktlinje 1 – Proportionalitet

8. Företag bör tillämpa dessa riktlinjer på ett sätt som står i proportion till arten, omfattningen och komplexiteten av verksamhetens inneboende risker.

Riktlinje 2 – IKT i företagsstyrningssystemet

9. Förvaltnings-, lednings- eller tillsynsorganet bör se till att företagsstyrningssystemet, särskilt systemet för riskhantering och internkontroll, hanterar företags IKT-risker och säkerhetsrisker på lämpligt sätt.

10. Förvaltnings-, lednings- eller tillsynsorganet bör se till att företagen har tillräckligt många anställda med lämplig kompetens för att kontinuerligt stödja företagens operativa IKT-behov och hanteringsprocesser för IKT-risker och säkerhetsrisker samt för att säkerställa genomförandet av deras IKT-strategi. Personalen bör regelbundet få lämplig utbildning om IKT-risker och säkerhetsrisker, däribland om informationssäkerhet, enligt vad som anges i riktlinje 13.

11. Förvaltnings-, lednings- eller tillsynsorganet bör se till att de resurser som tilldelas är tillräckliga för att uppfylla kraven ovan.

Riktlinje 3 – IKT-strategi

12. Förvaltnings-, lednings- eller tillsynsorganet har ett övergripande ansvar för att fastställa och godkänna företagens skriftliga IKT-strategi som en del av och i överensstämmelse med deras övergripande affärsstrategi, liksom för att utöva tillsyn över dess kommunikation och genomförande.
13. Av IKT-strategin bör det åtminstone framgå
    a) hur företagens IKT bör utvecklas för att effektivt stödja och genomföra deras affärsstrategi, inbegripet utveckling av den organisatoriska strukturen, affärsmodeller, IKT-system och nyckelberoenden gentemot tjänsteleverantörer,
    b) hur IKT-arkitekturen utvecklas, inbegripet beroenden gentemot tjänsteleverantörer,
    c) tydliga informationssäkerhetsmål med fokus på IKT-system, IKT-tjänster, personal och processer.
14. Företag bör se till att IKT-strategin genomförs, antas och kommuniceras till all den personal och alla de tjänsteleverantörer som berörs, enligt vad som är tillämpligt och relevant, och i rätt tid.
15. Företag bör införa en process för att övervaka och mäta effektiviteten i genomförandet av IKT-strategin. Denna process bör granskas och uppdateras regelbundet.

Riktlinje 4 – IKT-risker och säkerhetsrisker i riskhanteringssystemet

16. Förvaltnings-, lednings- eller tillsynsorganet har det övergripande ansvaret för att införa ett effektivt system för hantering av IKT-risker och säkerhetsrisker som en del av företagets allmänna riskhanteringssystem. Detta inbegriper fastställande av risktolerans för dessa risker, i enlighet med företagets riskstrategi, och en regelbunden skriftlig rapport om resultaten av riskhanteringsprocessen riktad till förvaltnings-, lednings- eller tillsynsorganet.
17. När det gäller IKT-risker och säkerhetsrisker bör företag (vid fastställande av IKT-skyddskraven som beskrivs nedan), som en del av det allmänna riskhanteringssystemet, beakta åtminstone följande:
    a) Företag bör göra och regelbundet uppdatera en kartläggning av sina affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar) för att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker.
    b) Företag bör identifiera och mäta alla relevanta IKT-risker och säkerhetsrisker som de exponeras för och klassificera identifierade affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar) utifrån kritikalitet. Företag bör även bedöma skyddskraven för, åtminstone, konfidentialitet, integritet och tillgänglighet avseende dessa affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Tillgångsägare, som ansvarar för klassificeringen av tillgångarna, bör identifieras.

c) De metoder som används för att fastställa kritikaliteten och den erfordrade skyddsnivån, särskilt vad gäller skyddsmålen för integritet, tillgänglighet och konfidentialitet, bör säkerställa att de resulterande skyddskraven är konsekventa och heltäckande.

d) Mätningen av IKT-risker och säkerhetsrisker bör göras på grundval av de definierade kriterierna för IKT-risker och säkerhetsrisker, med hänsyn till kritikaliteten i affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar), omfattningen av kända sårbarheter och tidigare incidenter som påverkat företaget.

e) Bedömningen av IKT-risker och säkerhetsrisker bör göras och dokumenteras regelbundet. Denna bedömning bör också göras före större förändringar i infrastruktur, processer eller rutiner, vilket påverkar affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar).

f) Företag bör – med utgångspunkt i riskbedömningen – åtminstone definiera och införa åtgärder för att hantera identifierade IKT-risker och säkerhetsrisker samt skydda informationstillgångar i enlighet med deras klassificering. Detta bör innefatta fastställande av åtgärder för att hantera kvarstående risker.

18. Resultaten av hanteringsprocessen för IKT-risker och säkerhetsrisker bör godkännas av förvaltnings-, lednings- eller tillsynsorganet och inkluderas i processen för operativ riskhantering som en del av företagens allmänna riskhantering.

Riktlinje 5 – Revision

19. Företags styrning, system och processer för IKT-risker och säkerhetsrisker bör genomgå periodiska revisioner, i linje med företagens revisionsplan[11], av revisorer med tillräcklig kunskap, kompetens och expertis inom IKT-risker och säkerhetsrisker för att kunna lämna en oberoende försäkran om deras effektivitet till förvaltnings-, lednings- eller tillsynsorganet. Intervall och fokus för sådana revisioner bör stå i proportion till relevanta IKT-risker och säkerhetsrisker.

Riktlinje 6 – Policy och åtgärder för informationssäkerhet

20. Företag bör fastställa en skriftlig informationssäkerhetspolicy som godkänts av förvaltnings-, lednings- eller tillsynsorganet och där överordnade principer och regler definieras för att skydda konfidentialitet, integritet och tillgänglighet vad gäller företagens information, för att stödja genomförandet av IKT-strategin.

21. Policyn bör innehålla en beskrivning av informationssäkerhetsledningens viktigaste roller och ansvarsområden och den bör fastställa krav för personal, processer och teknik i förhållande till informationssäkerhet, och samtidigt tillstå att personal på alla nivåer ansvarar för att säkerställa företagens informationssäkerhet.

22. Policyn bör spridas inom företaget och bör gälla all personal. När så är tillämpligt och relevant bör informationssäkerhetspolicyn eller delar av den också vidarebefordras till och gälla för tjänsteleverantörer.

23. På grundval av policyn bör företag utarbeta och införa mer specifika rutiner och åtgärder för informationssäkerhet, för att bland annat minska de IKT-risker och säkerhetsrisker som företagen exponeras för. Dessa rutiner och

[11] Artikel 271 i den delegerade förordningen.

informationssäkerhetsåtgärder bör inbegripa alla de processer som beskrivs i dessa riktlinjer, enligt vad som är tillämpligt.

Riktlinje 7 – Informationssäkerhetsfunktion

24. Företag bör, inom ramen för sina företagsstyrningssystem och i enlighet med proportionalitetsprincipen, inrätta en informationssäkerhetsfunktion vars ansvarsområden tilldelas en särskild person. Företagen bör säkerställa informationssäkerhetsfunktionens oberoende och objektivitet genom att på lämpligt sätt åtskilja den från processer för IKT-utveckling och IKT-verksamhet. Funktionen bör rapportera till förvaltnings-, lednings- eller tillsynsorganet.

25. Informationssäkerhetsfunktionens uppgifter är i normalfallet att

    a) stödja förvaltnings-, lednings- eller tillsynsorganet i samband med fastställande och upprätthållande av informationssäkerhetspolicyn för företag och kontrollera dess införande,

    b) regelbundet och på ad hoc-basis rapportera till och vägleda förvaltnings-, lednings- eller tillsynsorganet om informationssäkerhetens status och utveckling,

    c) övervaka och granska genomförandet av informationssäkerhetsåtgärderna,

    d) se till att informationssäkerhetskraven följs vid användning av tjänsteleverantörer,

    e) se till att alla anställda och tjänsteleverantörer med åtkomst till information och system har tillräcklig kännedom om informationssäkerhetspolicyn, t.ex. genom utbildning i och informationsmöten om informationssäkerhet,

    f) samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera relevanta granskningar till förvaltnings-, lednings- eller tillsynsorganet.

Riktlinje 8 – Logisk säkerhet

26. Företag bör definiera, dokumentera och införa rutiner för logisk åtkomstkontroll eller logisk säkerhet (identitets- och åtkomsthantering) i linje med skyddskraven, vilka definieras i riktlinje 4. Dessa rutiner bör införas, verkställas, övervakas och periodiskt granskas, och bör även inbegripa kontroller för övervakning av anomalier. Rutinerna bör åtminstone införa följande element, där termen ”användare” också omfattar tekniska användare:

    a) Behovsenlig behörighet, princip för begränsad behörighet och principen om åtskillnad mellan funktioner: Företag bör hantera åtkomsträttigheter, däribland fjärråtkomst, till informationstillgångar och deras stödsystem utifrån behovsenlig behörighet. Användare bör beviljas minimala åtkomsträttigheter som är absolut nödvändiga för att utföra arbetsuppgifterna (princip för begränsad behörighet), det vill säga för att förhindra ogrundad åtkomst till data eller att kombinationer av åtkomsträttigheter beviljas som kan användas för att kringgå kontroller (principen om åtskillnad mellan funktioner).

    b) Användaransvar: Företag bör begränsa, så långt det är möjligt, användning av allmänna och delade användarkonton och se till att användarna alltid kan identifieras och spåras tillbaka till en ansvarig fysisk person eller en godkänd uppgift för de åtgärder som vidtas i IKT-systemen.

c) Privilegierade åtkomsträttigheter: Företag bör införa stränga kontroller av privilegierad åtkomst till system genom att strikt begränsa och noggrant övervaka konton med avancerad systemåtkomst (t.ex. administratörskonton).

d) Fjärråtkomst: För att säkerställa säker kommunikation och minska riskerna bör fjärradministratörsåtkomst till kritiska IKT-system endast beviljas utifrån behovsenlig behörighet och förutsatt att starka autentiseringslösningar används.

e) Loggning av användaraktivitet: Användares aktiviteter bör loggas och övervakas på ett riskproportionerligt sätt, åtminstone vad gäller privilegierade användares aktiviteter. Åtkomstloggar bör skyddas mot obehörig ändring eller radering och lagras under en period som motsvarar kritikaliteten i de identifierade affärsfunktionerna, stödprocesserna och informationstillgångarna, utan att det påverkar lagringskraven i unionslagstiftningen och den nationella lagstiftningen. Företag bör använda denna information för att underlätta identifiering och utredning av avvikande aktiviteter som har upptäckts i samband med tillhandahållandet av tjänsterna.

f) Åtkomsthantering: Åtkomsträttigheter bör beviljas, tas bort och ändras i rätt tid, enligt i förväg fastställda rutiner för godkännande där berörd ägare till informationstillgången är involverad. Om åtkomst inte längre behövs bör åtkomsträttigheterna återkallas omedelbart.

g) Åtkomstbedömning: Åtkomsträttigheter bör ses över periodiskt för att säkerställa att användare inte har för omfattande rättigheter och att åtkomsträttigheter upphävs/tas bort om de inte längre behövs.

h) Beviljande, ändring och återkallelse av åtkomsträttigheter bör dokumenteras på ett sätt som underlättar förståelse och analys.

i) Autentiseringsmetoder: Företag bör tillämpa autentiseringsmetoder som är tillräckligt tillförlitliga för att på ett adekvat och effektivt sätt säkerställa att policyer och rutiner för åtkomstkontroll följs. Autentiseringsmetoderna bör stå i proportion till kritikaliteten i de IKT-system, den information eller den process som åtkomsten avser. Detta bör åtminstone innebära starka lösenord eller starkare autentiseringsmetoder (såsom tvåfaktorsautentisering) med utgångspunkt i relevant risk.

27. Elektronisk åtkomst genom program till data och IKT-system bör begränsas till vad som är absolut nödvändigt för att tillhandahålla tjänsten i fråga.

Riktlinje 9 – Fysisk säkerhet

28. Företags fysiska säkerhetsåtgärder (t.ex. skydd mot strömavbrott, brand, vatten och obehörig fysisk åtkomst) bör definieras, dokumenteras och genomföras för att skydda lokaler, datacentraler och känsliga områden från obehörigt tillträde och från miljöfaror.

29. Fysisk åtkomst till IKT-system bör endast beviljas behöriga personer. Behörighet bör tilldelas i enlighet med enskilda personers arbetsuppgifter och ansvarsområden och bör begränsas till de som har lämplig utbildning och som övervakas på ett lämpligt sätt. Den fysiska åtkomsten bör ses över regelbundet för att se till att onödiga åtkomsträttigheter skyndsamt upphävs/tas bort.

30. Lämpliga åtgärder för att skydda mot miljöfaror bör stå i proportion till byggnadernas betydelse och kritikaliteten i verksamheterna eller IKT-systemen i dessa byggnader.

Riktlinje 10 – Säkerhet för IKT-verksamhet

31. Företag bör införa rutiner för att säkerställa konfidentialitet, integritet och tillgänglighet vad gäller IKT-system och IKT-tjänster för att minimera den inverkan som säkerhetsfrågor har på tillhandahållandet av IKT-tjänster. Dessa rutiner bör lämpligen inkludera följande åtgärder:

    a) Identifiering av potentiella sårbarheter som bör bedömas och avhjälpas genom att säkerställa att IKT-systemen är uppdaterade, inbegripet den programvara som företag tillhandahåller sina interna och externa användare, genom att utarbeta kritiska säkerhetsfixar, inbegripet uppdaterade antivirusdefinitioner, eller genom att införa kompenserande kontroller.

    b) Införande av säkra grundkonfigurationer för alla kritiska komponenter såsom operativsystem, databaser, routrar eller växlar.

    c) Införande av nätsegmentering, förebyggande system för dataläckage och kryptering av nätverkstrafik (i enlighet med informationstillgångens klassificering).

    d) Införande av skydd för ändpunkter, däribland servrar, arbetsstationer och mobila enheter. Ett företag bör bedöma huruvida en ändpunkt uppfyller de säkerhetsstandarder som företaget har definierat, innan den ges åtkomst till företagsnätet.

    e) Säkerställande av att integritetskontrollerande mekanismer har införts för att verifiera IKT-systemens integritet.

    f) Kryptering av vilande och transiterande data (i enlighet med informationstillgångens klassificering).

Riktlinje 11 – Säkerhetsövervakning

32. Företag bör utarbeta och införa rutiner och processer för att kontinuerligt övervaka de aktiviteter som påverkar deras informationssäkerhet. Övervakningen bör åtminstone omfatta

    a) interna och externa faktorer, inklusive affärsfunktioner och administrativa IKT-funktioner,

    b) transaktioner från tjänsteleverantörer, andra enheter och interna användare,

    c) potentiella interna och externa hot.

33. På grundval av övervakningen bör företagen sätta in lämplig och effektiv kapacitet för att upptäcka, rapportera och svara på avvikande aktiviteter och hot, såsom fysiska eller logiska intrång, brott mot informationstillgångarnas konfidentialitet, integritet och tillgänglighet, skadlig kod och allmänt kända sårbarheter hos program- och maskinvara.

34. Rapporteringen från säkerhetsövervakningen bör hjälpa företagen att förstå arten av både operativa incidenter och säkerhetsincidenter, identifiera trender, stödja företagens interna utredningar och göra det möjligt för dem att fatta lämpliga beslut.

Riktlinje 12 – Granskningar, bedömning och testning av informationssäkerhet

35. Företag bör utföra en rad olika granskningar, bedömningar och testningar av informationssäkerheten för att säkerställa en effektiv identifiering av sårbarheter i sina IKT-system och IKT-tjänster. Företag kan till exempel utföra gapanalyser gentemot informationssäkerhetsstandarder, granskningar av överensstämmelse, interna och externa revisioner av informationssystemen eller fysiska säkerhetsgranskningar.

36. Företag bör fastställa och införa en testningsram för informationssäkerhet som validerar tillförlitligheten och effektiviteten i informationssäkerhetsåtgärderna och säkerställa att ramen tar hänsyn till de hot och sårbarheter som identifierats genom hotövervakning och bedömningsprocessen för IKT-risker och säkerhetsrisker.

37. Testningen bör genomföras på ett tryggt och säkert sätt och av oberoende testare med tillräcklig kunskap, kompetens och expertis inom testning av informationssäkerhetsåtgärder.

38. Företag bör genomföra tester regelbundet. Testningens omfattning, frekvens och metod (t.ex. penetrationsprovning, inbegripet hotstyrd penetrationsprovning) bör stå i proportion till identifierad risknivå. Testning av kritiska IKT-system och sårbarhetsavsökningar bör göras årligen.

39. Företag bör se till att tester av säkerhetsåtgärder utförs vid ändringar i infrastruktur, processer eller rutiner och om ändringar införs till följd av betydande operativa incidenter eller säkerhetsincidenter eller på grund av lansering av nya eller väsentligt modifierade kritiska program. Företag bör kontrollera och utvärdera resultaten av säkerhetstesterna och uppdatera sina säkerhetsåtgärder i enlighet därmed, utan onödigt dröjsmål, vad gäller kritiska IKT-system.

Riktlinje 13 – Utbildning och medvetenhet avseende informationssäkerhet

40. Företag bör införa utbildningsprogram om informationssäkerhet för all personal, däribland förvaltnings-, lednings- eller tillsynsorganet, för att säkerställa att de anställda är utbildade för att utföra sina arbetsuppgifter och ansvarsområden, i syfte att minska antalet fel som beror på den mänskliga faktorn, stölder, bedrägerier, felaktig användning och förluster. Företag bör se till att all personal regelbundet erbjuds utbildning genom utbildningsprogrammen.

41. Företag bör inrätta och genomföra periodiska säkerhetsmedvetandeprogram för att utbilda sin personal, däribland förvaltnings-, lednings- eller tillsynsorganet, om hur informationssäkerhetsrelaterade risker ska hanteras.

Riktlinje 14 – Hantering av IKT-verksamhet

42. Företag bör hantera sin IKT-verksamhet utifrån sin IKT-strategi. Det bör definieras i dokument hur företag ska driva, övervaka och kontrollera IKT-systemen och IKT-tjänsterna, inbegripet dokumentering av kritiska IKT-processer, IKT-rutiner och IKT-verksamheter.

43. Företag bör införa loggnings- och övervakningsrutiner för kritiska IKT-verksamheter för att möjliggöra upptäckt, analys och avhjälpande av fel.

44. Företag bör ha en uppdaterad förteckning över sina IKT-tillgångar. Förteckningen över IKT-tillgångar bör vara tillräckligt detaljerad för att möjliggöra snabb

identifiering av en IKT-tillgång och dess lokalisering, säkerhetsklassificering och äganderätt.

45. Företag bör övervaka och hantera livscykeln för IKT-tillgångar för att säkerställa att de även fortsättningsvis uppfyller och stöder verksamhetskraven och riskhanteringskraven. Företag bör kontrollera att IKT-tillgångarna stöds av deras leverantörer eller interna utvecklare och att alla relevanta fixar och uppgraderingar tillämpas med utgångspunkt i en dokumenterad process. De risker som härrör från föråldrade eller icke-stödda IKT-tillgångar bör bedömas och genomgå riskreducering. Avvecklade IKT-tillgångar bör bearbetas och bortskaffas på ett säkert sätt.

46. Företag bör införa planerings- och övervakningsprocesser för prestanda och kapacitet för att i tid förebygga, upptäcka och bemöta viktiga prestandaproblem i IKT-system och brister i IKT-kapacitet.

47. Företag bör definiera och införa rutiner för säkerhetskopiering och återställande av data och IKT-system för att säkerställa att de kan återställas efter behov. Omfattningen av och intervallen för säkerhetskopiering bör fastställas i linje med återhämtningskraven och kritikaliteten i data och IKT-system samt utvärderas i enlighet med utförd riskbedömning. Säkerhetskopierings- och återställanderutiner bör kontrolleras regelbundet.

48. Företag bör se till att säkerhetskopierade data och IKT-system lagras på en eller flera platser utanför det primära verksamhetsstället. Dessa platser ska vara säkra och ligga tillräckligt långt från det primära verksamhetsstället för att inte exponeras för samma risker.

Riktlinje 15 – Hantering av IKT-incidenter och IKT-problem

49. Företag bör utarbeta och införa en process för hantering av incidenter och problem för att övervaka och logga operativa incidenter och säkerhetsincidenter och göra det möjligt för företagen att fortsätta eller återuppta kritiska affärsfunktioner och affärsprocesser vid störningar.

50. Företag bör fastställa lämpliga kriterier och tröskelvärden för klassificering av händelser som operativa incidenter eller säkerhetsincidenter, liksom "early-warning"-indikatorer som bör fungera som en varning för att möjliggöra tidig upptäckt av sådana incidenter.

51. För att minimera effekterna av negativa händelser och möjliggöra ett snabbt återställande bör företag utarbeta lämpliga processer och organisatoriska strukturer för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av operativa incidenter och säkerhetsincidenter, för att se till att de bakomliggande orsakerna identifieras och hanteras och att korrigeringsåtgärder vidtas för att förhindra att sådana incidenter upprepas. Processen för hantering av incidenter och problem bör åtminstone innehålla följande:

    a) Rutiner för identifiering, spårning, loggning, kategorisering och klassificering av incidenter i enlighet med en prioritetsordning som definierats av företaget och som utgår från verksamhetens kritikalitet och serviceavtal.

    b) Roller och ansvarsområden för olika incidentscenarier (t.ex. fel, funktionsstörningar och cyberattacker).

    c) Ett problemhanteringsförfarande för identifiering, analys och åtgärdande av den bakomliggande orsaken till en eller flera incidenter. Företag bör analysera de operativa incidenter eller säkerhetsincidenter som har identifierats eller

förekommit inom och/eller utanför organisationen samt ta hänsyn till viktiga erfarenheter från dessa analyser och uppdatera säkerhetsåtgärderna därefter.

d) Effektiva interna kommunikationsplaner, däribland rutiner för incidentrapportering och eskalering – vilket även omfattar säkerhetsrelaterade kundreklamationer – för att säkerställa att

   i. incidenter med potentiellt stora negativa effekter på kritiska IKT-system och IKT-tjänster rapporteras till relevant verkställande ledning,

   ii. förvaltnings-, lednings- eller tillsynsorganet underrättas på ad hoc-basis vid väsentliga incidenter och åtminstone informeras om effekterna, hanteringen och de ytterligare kontroller som ska definieras till följd av incidenterna.

e) Rutiner för incidenthantering i syfte att mildra effekterna förknippade med incidenterna och se till att tjänsten blir funktionell och säker i tid.

f) Specifika externa kommunikationsplaner för kritiska affärsfunktioner och affärsprocesser för att

   i. samarbeta med relevanta intressenter för effektiv hantering av incidenten och effektiv återhämtning från densamma,

   ii. i tid tillhandahålla information, inbegripet incidentrapportering, till externa parter (t.ex. kunder, andra marknadsaktörer, relevanta [tillsyns]myndigheter, enligt vad som är lämpligt och i linje med tillämpliga bestämmelser).

Riktlinje 16 – IKT-projektledning

52. Företag bör genomföra en IKT-projektmetod (inbegripet oberoende överväganden avseende säkerhetskrav) med en lämplig styrningsprocess och ett lämpligt ledarskap för projektgenomförande, för att på ett effektivt sätt stödja genomförandet av IKT-strategin genom IKT-projekt.

53. Företag bör på ett lämpligt sätt övervaka och minska de risker som härrör från portföljen av IKT-projekt, också med hänsyn till de risker som kan följa av inbördes beroenden mellan olika projekt och från flera projekts beroenden av samma resurser och/eller sakkunskap.

Riktlinje 17 – Anskaffning och utveckling av IKT-system

54. Företag bör utarbeta och införa en process som styr anskaffning, utveckling och underhåll av IKT-system, för att säkerställa att konfidentialiteten, integriteten och tillgängligheten vad gäller de data som ska behandlas skyddas på ett heltäckande sätt och de definierade skyddskraven uppfylls. Denna process bör utformas med hjälp av en riskbaserad metod.

55. Företag bör se till att funktionella och icke-funktionella krav (inbegripet informationssäkerhetskrav) liksom tekniska mål är tydligt definierade innan systemanskaffning eller utvecklingsaktiviteter genomförs.

56. Företag bör se till att åtgärder har vidtagits för att förhindra oavsiktlig ändring eller avsiktlig manipulation av IKT-systemen under utveckling.

57. Företag bör ha infört metoder för testning och godkännande av IKT-system, IKT-tjänster och åtgärder för informationssäkerhet.

58. Företag bör på lämpligt sätt testa IKT-system, IKT-tjänster och åtgärder för informationssäkerhet för att identifiera eventuella svagheter, överträdelser och incidenter vad gäller säkerheten.

59. Företag bör säkerställa åtskillnad av produktionsmiljöer från utvecklings- och testningsmiljöer och andra icke-produktionsmiljöer.

60. Företag bör vidta åtgärder för att skydda källkodens integritet (i tillämpliga fall) i IKT-system. De ska även dokumentera utveckling, införande, drift och/eller konfiguration av IKT-systemen på ett heltäckande sätt för att reducera onödigt beroende av områdesexperter.

61. Företags processer för anskaffning och utveckling av IKT-system bör även tillämpas på IKT-system som utvecklas eller hanteras av affärsfunktionens slutanvändare utanför IKT-organisationen (t.ex. verksamhetsledda program eller datorprogram för slutanvändare) med hjälp av en riskbaserad metod. Företagen bör föra register över dessa program som stöder kritiska affärsfunktioner eller affärsprocesser.

Riktlinje 18 – IKT-ändringshantering

62. Företag bör ta fram och införa en process för IKT-ändringshantering för att säkerställa att alla ändringar i IKT-systemen registreras, bedöms, testas, godkänns, auktoriseras och genomförs på ett kontrollerat sätt. Ändringar i samband med brådskande eller akuta IKT-ändringar bör kunna spåras och meddelas i efterhand till relevant tillgångsägare för efterhandsanalys.

63. Företag bör avgöra huruvida ändringar i den befintliga driftsmiljön påverkar de befintliga säkerhetsåtgärderna eller kräver antagande av ytterligare åtgärder för att minska riskerna i fråga. Dessa ändringar bör överensstämma med företagens formella process för ändringshantering.

Riktlinje 19 – Hantering av driftskontinuitet

64. Som en del av företagens allmänna policy för driftskontinuitet ansvarar förvaltnings-, lednings- eller tillsynsorganet för att fastställa och godkänna företagens policy för IKT-kontinuitet. Policyn för IKT-kontinuitet bör spridas på lämpligt sätt inom företagen och bör gälla all relevant personal och – om så är tillämpligt – tjänsteleverantörerna.

Riktlinje 20 – Verksamhetsanalys

65. Som en del av en sund hantering av driftskontinuiteten bör företag genomföra en verksamhetsanalys för att bedöma sin exponering för allvarliga störningar i verksamheten och deras möjliga effekter – kvantitativt och kvalitativt – med hjälp av interna och/eller externa data och scenarioanalys. Verksamhetsanalysen bör även beakta kritikaliteten i identifierade och klassificerade affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar) och deras ömsesidiga beroendeförhållanden i enlighet med riktlinje 4.

66. Företag bör se till att deras IKT-system och IKT-tjänster är utformade och anpassade efter verksamhetsanalysen, exempelvis med redundans av vissa kritiska komponenter för att förhindra störningar till följd av händelser som påverkar dessa komponenter.

Riktlinje 21 – Kontinuitetsplanering

67. Företags övergripande kontinuitetsplaner bör ta hänsyn till de väsentliga risker som skulle kunna ha en negativ inverkan på IKT-system och IKT-tjänster. Planerna bör stödja mål för att skydda och – vid behov – återupprätta konfidentialiteten, integriteten och tillgängligheten i företagens affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Under framtagandet av dessa planer bör företag samordna med relevanta interna och externa intressenter efter behov.

68. Företag bör införa kontinuitetsplaner för att säkerställa att de kan vidta lämpliga åtgärder vid eventuella felscenarier inom ett mål för återställningstid (den maximala tid inom vilken ett system eller en process ska återställas efter en incident) och ett mål för återställning av data (den maximala period under vilken data kan förloras vid en incident på en fördefinierad servicenivå).

69. Företag bör beakta flera olika scenarier i sina kontinuitetsplaner, däribland extrema men möjliga scenarier och scenarier med cyberattacker, och bedöma potentiella effekter av sådana scenarier. Utifrån dessa scenarier bör företag beskriva hur kontinuiteten i IKT-system och IKT-tjänster samt företags informationssäkerhet ska säkerställas.

Riktlinje 22 – Hanterings- och återställningsplaner

70. Utifrån verksamhetsanalysen och möjliga scenarier bör företag utarbeta hanterings- och återställningsplaner. I dessa planer bör det anges vilka förhållanden som kan föranleda aktivering av planen och vilka åtgärder som ska vidtas för att säkerställa integritet, tillgänglighet, kontinuitet och återställande avseende åtminstone företags kritiska IKT-system, IKT-tjänster och data. Hanterings- och återställningsplanerna bör syfta till att uppfylla återställningsmålen för företagens verksamhet.

71. Hanterings- och återställningsplanerna bör ta hänsyn till både kortsiktiga och – vid behov – långsiktiga återställningsmöjligheter. Planerna bör åtminstone

    a) fokusera på att återställa driften av viktiga IKT-tjänster, affärsfunktioner, stödprocesser, informationstillgångar och deras ömsesidiga beroendeförhållanden för att undvika att företagets verksamhet påverkas negativt,

    b) dokumenteras och tillgängliggöras för affärs- och stödenheter samt vara lättillgängliga i akuta situationer, och de ska innehålla tydliga definitioner av roller och ansvarsområden,

    c) uppdateras löpande enligt erfarenheter från incidenter, tester, nyligen identifierade risker och hot samt ändrade mål och prioriteringar för återställande.

72. Planerna bör även beakta alternativa möjligheter i situationer där återställande på kort sikt kanske inte är möjligt på grund av kostnader, risker, logistik eller oförutsedda omständigheter.

73. Som en del av hanterings- och återställningsplanerna bör företag beakta och införa kontinuitetsåtgärder för att minska riskerna för funktionsavbrott hos tjänsteleverantörerna, vilka är av avgörande betydelse för företags kontinuitet med avseende på IKT-tjänster (i linje med bestämmelserna i Eiopas riktlinjer för företagsstyrningssystem och riktlinjer om uppdragsavtal med molntjänstleverantörer).

Riktlinje 23 – Testning av planer

74. Företag bör testa sina kontinuitetsplaner och se till att driften av deras kritiska affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar) liksom IKT-tillgångar och deras ömsesidiga beroendeförhållanden (också de som tillhandahålls av tjänsteleverantörer) testas regelbundet utifrån företagens riskprofil.

75. Kontinuitetsplaner bör uppdateras regelbundet på grundval av testresultaten, aktuella underrättelser om hot och erfarenheter från tidigare händelser. Alla relevanta ändringar av återställningsmål (däribland mål för återställningstid och mål för återställning av data) och/eller ändringar i affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar) bör också inkluderas.

76. Testning av kontinuitetsplanerna bör visa att de kan upprätthålla verksamhetens bärkraft till dess att kritiska verksamheter återupprättas enligt en fördefinierad servicenivå eller inverkanstolerans.

77. Testresultaten bör dokumenteras och eventuella brister som identifierats bör analyseras, hanteras och rapporteras till förvaltnings-, lednings- eller tillsynsorganet.

Riktlinje 24 – Kriskommunikation

78. I händelse av störningar eller akuta situationer, och under genomförandet av kontinuitetsplanerna, bör företag se till att de har infört effektiva kriskommunikationsåtgärder så att alla relevanta interna och externa intressenter, inklusive relevanta tillsynsmyndigheter – när så föreskrivs i nationell lagstiftning – liksom relevanta tjänsteleverantörer, informeras i tid och på ett lämpligt sätt.

Riktlinje 25 – Utkontraktering av IKT-tjänster och IKT-system

79. När IKT-tjänster och IKT-system utkontrakteras bör företag se till att relevanta krav för sådana tjänster och system uppfylls, utan att det påverkar tillämpningen av Eiopas riktlinjer om uppdragsavtal med molntjänstleverantörer.

80. I det fall kritiska eller viktiga funktioner utkontrakteras bör företag se till att tjänsteleverantörens avtalsförpliktelser (t.ex. kontrakt, servicenivåavtal och bestämmelser om uppsägning i relevanta kontrakt) omfattar åtminstone följande:

    a) Lämpliga och proportionerliga mål och åtgärder för informationssäkerhet, däribland krav såsom minimikrav för informationssäkerhet, specifikationer av företags datalivscykel, revisions- och åtkomsträttigheter och krav beträffande placering av datacentraler samt datakrypteringskrav, nätverkssäkerhet och processer för säkerhetsövervakning.

    b) Servicenivåavtal för att säkerställa IKT-tjänsternas och IKT-systemens kontinuitet och prestandamål under normala omständigheter liksom under omständigheter som anges i beredskapsplaner i händelse av avbrott.

    c) Hanteringsrutiner för operativa incidenter och säkerhetsincidenter, bl.a. eskalering och rapportering.

81. Företag bör övervaka och försäkra sig om dessa tjänsteleverantörers efterlevnadsnivå med avseende på deras mål och åtgärder för säkerhet samt prestandamålen.

Regler för efterlevnad och rapportering

82. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1094/2010. I enlighet med artikel 16.3 i den förordningen ska behöriga myndigheter och företag med alla tillgängliga medel söka följa riktlinjer och rekommendationer.

83. De behöriga myndigheter som följer eller har för avsikt att följa dessa riktlinjer bör införliva dem i sina ramar för regler och tillsyn på ett lämpligt sätt.

84. De behöriga myndigheterna ska, inom två månader från det att de översatta versionerna har offentliggjorts, bekräfta till Eiopa om huruvida de följer eller avser att följa dessa riktlinjer, och ange skälen till att de eventuellt inte följer dem.

85. Om Eiopa inte har fått något svar inom denna tidsfrist kommer behöriga myndigheter att anses inte följa rapporteringen och rapporteras i enlighet med detta.

Slutbestämmelse om översyn

86. Dessa riktlinjer ska vara föremål för översyn av Eiopa.