FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Retningslinjer for IKT-sikkerhet og –governance

Guidelines on information and communication technology security and governance (EIOPA 12. October 2020)

Gjennomgang av "EIOPA GL on Information and communication technology security and governance"

Jarleif Lødøen, IKT Seminar for forsikring 6. desember 2021

Agenda

Guidelines on information and communication technology security and governance

1. Introduksjon – Nyhetsmelding
2. Formål med retningslinjene
3. Bakgrunn for utvikling av GL
4. Om retningslinjene
5. De 7 hovedområdene i retningslinjene
6. Detaljgjennomgang av retningslinjene
7. Implementering i norsk rett
8. Relevante nyhetsbrev og nettsteder
9. Tilbakemelding og spørsmål

1. Introduksjon – Nyhetsmelding

Utfordringen starter allerede med oversettelse av tittel:

- **"EIOPA Guidelines on Information and communication technology security and governance"**

Kortversjon engelsk:

- **"Guidelines on ICT security and governance"**

Kortversjon norsk:

- **"Retningslinjer for IKT-sikkerhet og styring og kontroll med IKT"**
- **"Retningslinjer for IKT-sikkerhet og –governance"**

Finanstilsynet valgte sistnevnte variant når nyheten om retningslinjene ble publisert: Link…

Som referanse til retningslinjene vil også begrepene Guidelines og GL bli benyttet i det videre

Nyhetsmeldingen på FT sine nettsider

Den europeiske forsikringstilsynsmyndigheten (EIOPA) har fastsatt retningslinjer for IKT-sikkerhet og -governance "Guidelines on information and communication technology security and governance" 12. oktober 2020. Retningslinjene gjelder fra 1. juli 2021.

Retningslinjene retter seg mot forsikringsforetak. Formålet med retningslinjene er å klargjøre kravene til håndtering av IKT-sikkerhetsrisiko i foretakene, fastsette minimumskrav til forventede nivåer for informasjons- og cybersikkerhet og unngå potensiell regulatorisk arbitrasje (foretak skal underlegges samme regulatoriske krav til tjenestene i alle EU/EØS-land).

Norge har siden 2003 hatt IKT-forskriften som regulerer de områder som retningslinjene omfatter. Det er Finanstilsynets vurdering at de nye retningslinjene fra EIOPA er dekkende for de områdene foretakene skal vurdere risiko for, og at de gir en nyttig utdyping på områder som reguleres av IKT-forskriften.

Retningslinjene gir veiledning om hvordan bestemmelsene knyttet til operasjonell risiko i direktiv 2009/138/EC (Solvens II), utfyllende regler for Solvens II i delegert kommisjonsforordning 2015/35 og EIOPAs retningslinjer for styring og kontroll (EIOPA BoS 14/253), samt EIOPAs retningslinjer for utkontraktering til skytjenesteleverandører (EIOPA BoS 19/270), skal forstås.

Finanstilsynet har bekreftet at retningslinjene vil bli fulgt i Norge fra samme dato som retningslinjene skal gjelde i EU, 1. juli 2021.

Finanstilsynet vil oppdatere sin tilsynspraksis og forventninger til behandling av IKT-sikkerhetsrisiko i tråd med de nye retningslinjene.

Finanstilsynet vil arrangere et Webinar med gjennomgang av hvilke konsekvenser de nye retningslinjene vil ha for forsikringsbransjen i Norge. Nærmere informasjon vil bli lagt ut på våre nettsider.

Link til GL: Guidelines on information and communication technology security and governance
Link til svar fra høringsrunden: Høringssvar

2. Formål med retningslinjene

a) provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;
b) avoid potential regulatory arbitrage;
c) foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

Norsk: (fra nyhetsmeldingen)

"Formålet med retningslinjene er å klargjøre kravene til håndtering av IKT-sikkerhetsrisiko i foretakene, fastsette minimumskrav til forventede nivåer for informasjons- og cybersikkerhet og unngå potensiell regulatorisk arbitrasje (foretak skal underlegges samme regulatoriske krav til tjenestene i alle EU/EØS-land)"

3. Bakgrunn for utvikling av retningslinjene

Detaljert beskrivelse av bakgrunn for utvikling av de nye retningslinjene fremgår av

- **Kapittel "Background" på sidene 4 og 5**
- **Kapittel "Introduction", punkt 1 på side 7 – noen spesifikke regelreferanser**

Retningslinjene skal blant annet gi veiledning for hvordan ulike områder innen IKT skal forstås i forhold til bestemmelsene:

- **operasjonell risiko i direktiv 2009/138/EC (Solvens II) – Link…**
- **utfyllende regler for Solvens II i delegert kommisjonsforordning 2015/35 – Link…**
- **EIOPAs retningslinjer for governance (styring og kontroll) (EIOPA BoS 14/253) – Link…**
- **EIOPAs retningslinjer for utkontraktering til skytjenesteleverandører (EIOPA BoS 19/270) – Link…**

4. Om retningslinjene

- **Bestemmelsene gjelder for 30 EØS-land, og det var utfordringer i å håndtere kulturforskjeller når retningslinjene ble utviklet;**
  - **To fraksjoner :**
    - **Foreskrivende syn (oversatt fra engelsk "preskriptive") → "alt" må detaljspesifiseres**
    - **GL beskriver rammer for foretakene → ansvarliggjøring av foretakene**
- **Intensjon om å unngå å repetere regelverk som allerede eksisterer (må konferere Solvency II, Guidelines on system of governance etc. sammen med GL)**
- **Teknologi- og metodenøytral ordlyd - skal tåle at det kommer endringer i teknologi, metode, organisering, beste praksis mm.**
- **Proporsjonalitetsprinsippet "Guideline 1 – Proportionality"**

  "*Undertakings should apply these Guidelines in a manner which is proportionate to the nature, scale and complexity of the risks inherent in their business*"

I praksis gjør dette at foretakene kan vurdere inn praktiske hensyn i forhold til den risiko man vurderer: " commensurate with the relevant ICT and security risks". Kan unngå å "skyte spurv med kanon"

- **GL 1 ble introdusert etter høringsrunden for presisering**

5. De 7 hovedområdene i retningslinjene

1. **Styring og kontroll (governance) og strategi**
   Etablere styring og kontroll for å sikre gjennomføring av IKT-strategien
2. **Informasjonssikkerhet**
   Beskytte konfidensialitet, integritet og tilgjengelighet for kunde- og forretningsdata
3. **IKT- og sikkerhetsrisikostyring**
   Sikre at IKT- og sikkerhetsrisikoer blir identifisert og håndtert på riktig måte
4. **IKT driftsledelse**
   Implementere effektiv og trygg IKT-drift
5. **IKT-prosjekt og endringsledelse**
   Administrere prosjekter og endringer effektivt for å sikre forretnings- og sikkerhetsmål
6. **Forretningskontinuitet**
   Opprettholdelse av forretningsprosesser ved avvik
7. **Utkontraktering**
   Beskyttelse av utkontrakterte IT-tjenester på riktig måte

6. Detaljgjennomgang av retningslinjene

- → I gjennomgangen benyttes «ledelse» som begrep for «administrative, management or supervisory body (AMSB)"
- → I presentasjonen benyttes begrepet *"forretningsprosesser, roller, data og utstyr"* der GL lyder *"business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets)*". Dette for å korte ned teksten.
- → Definisjoner finnes i GL: Her gjengis assets med bakgrunn i at dette inngår i det som representerer "forretningsprosesser, roller, data og utstyr"
  - ICT asset = An asset of either software or hardware that is found in the business environment
  - Information asset = A collection of information, either tangible or intangible, that is worth protecting

→ Referanse til IKT-forskriften, eksempel: §2

Guideline 1 - 2

Guideline 1 – Proportionality

- Foretaket bør anvende retningslinjene på en måte som står i forhold til risikoene for virksomheten:
  - «Undertakings should apply these Guidelines in a manner which is proportionate to the nature, scale and complexity of the risks inherent in their business»

Guideline 2 – ICT within the system of governance

§2

- Ledelsens ansvar for å etablere et styringssystem, med internkontroll og risikostyring, som i tilstrekkelig grad håndterer foretakets IKT- og sikkerhetsrisikoer
- Foretakets ansvar for å etablere tilstrekkelig kapasitet og kunnskap for å håndtere IKT, risikoen med IKT, og implementering av IKT-strategien
- Ledelsens ansvar for å gi tilstrekkelig opplæring til ansatte som beskrevet i «Guideline 13 – Information security training and awareness»

Guideline 3

§ 2

Guideline 3 – ICT strategy

- Ledelsens ansvar for å fastsette og godkjenne en skriftlig IKT-strategi som støtter opp under forretningsstrategien
- Bør omfatte følgende forhold
  - Definere hvordan IKT skal utvikles for å støtte opp om forretningsstrategien
  - Beskrive endringer i IKT-arkitektur inkludert avhengigheter til IKT-tjenesteleverandører
  - Beskrive klare mål for informasjonssikkerhet
- Beskriver også ledelsens ansvar for oppfølging av implementeringen (bør etablere en egen prosess), og sørge for at IKT-strategien blir gjort kjent for relevant personell og leverandører

Guideline 4

§3

Guideline 4 – ICT and security risks within the risk management system

- **Beskriver ledelsens overordnede ansvar for å etablere et effektivt system for håndtering av IKT- og sikkerhetsrisikoer som del av virksomhetens overordnede risikostyringssystem (inkl. fastsettelse av risikotoleranse)**
- **Regelmessig skriftlig risikorapport til ledelsen**
- **Resultatene fra risikostyringsprosessen innen IKT og IKT-Sikkerhet bør godkjennes av ledelsen og innlemmes i den operasjonelle risikostyringen for foretaket**

Guideline 4 forts.

§3

I avsnitt nr. 17 fremgår det krav til arbeidet med risiko på IKT-området:

- Etablere, og regelmessig oppdatere, oversikter over forretningsprosesser, roller, data og utstyr og deres gjensidige avhengigheter og viktighet med tanke på IKT- og sikkerhetsrisiko
- Identifisere og måle alle relevante IKT- og sikkerhetsrisikoer med en klassifisering av de identifiserte forretningsprosesser, roller, data og utstyr med tanke på kritikalitet
- Vurdere beskyttelseskravene med tanke på konfidensialitet, integritet og tilgjengelighet for de identifiserte forretningsprosesser, roller, data og utstyr. Der asset-owner (eier av utstyr/data) er den som er ansvarlig for klassifisering
- Krav om at det bør foretas en skriftlig vurdering av IKT- og sikkerhetsrisikoer (ikke uttalt frekvens → jevnlig – IKT-forskrift = Årlig)
- Vurdering av IKT- og sikkerhetsrisiko bør også utføres før større endringer i infrastruktur, prosesser eller prosedyrer

Guideline 4 forts.

§3

- **Basert på risikovurderingene bør foretaket definere og implementere tiltak for å håndtere de identifiserte IKT- og sikkerhetsrisikoene og beskytte informasjonsmidler i samsvar med klassifiseringen. Foretaket bør også definere hvordan de skal håndtere gjenværende risiko.**

Guideline 5

Guideline 5 - Audit

- **Foretakets opplegg for styring og kontroll med IKT- og sikkerhetsrisiko bør revideres periodisk og inngå i foretakets revisjonsplaner.**
- **Frekvensen på revisjonene bør stå i forhold til relevante IKT- og sikkerhetsrisikoer**
- **Det forutsettes at de som utfører revisjonen har tilstrekkelig kunnskap, ferdigheter og ekspertise med IKT og sikkerhetsrisikoer til å kunne gi en uavhengig og pålitelig bekreftelse.**

Guideline 6 - 7

Guideline 6 – Information security policy and measures §2, §3, §5

- Foretaket bør ha en skriftlig informasjonssikkerhets policy som er godkjent av ledelsen
- Policy bør definere prinsipper og regler på et overordnet nivå med tanke på å beskytte konfidensialitet, integritet og tilgjengelighet
- Policy bør inkludere en beskrivelse av de viktigste rollene og ansvar knyttet til styring og kontroll med informasjonssikkerhet
- Basert på policyen bør det etableres og implementeres mer spesifikke prosedyrer og tiltak for informasjonssikkerhet

Guideline 7 - Information security function §2

- Etablere en informasjonssikkerhetsfunksjon der ansvaret for funksjonen blir tildelt en person
- Foretaket bør sikre uavhengigheten og objektiviteten for denne funksjonen ved å adskille den på en hensiktsmessig måte fra IKT-utviklings- og driftsprosesser

Guideline 7 forts.

§2

Guideline 7 - Information security function

- Funksjonen bør rapportere direkte til ledelsen
- Typiske oppgaver for informasjonssikkerhetsfunksjonen
  - Støtte ledelsen i utvikling og vedlikehold av informasjonssikkerhetspolicy og kontrollere at den blir fulgt
  - Rapportering og rådgiving om status og utvikling innen området informasjonssikkerhet
  - Overvåke og vurdere implementeringen av informasjonssikkerhetstiltak
  - Påse at informasjonssikkerhetskravene overholdes ved utkontraktering
  - Sikre at ansatte og tjenesteleverandører er informert om sikkerhetspolicy
  - Analysere drifts- og sikkerhetshendelser med evt. rapport til ledelsen

Guideline 8

§5

Guideline 8 – Logical security

- Dokumentere og implementere prosedyrer for identitets- og tilgangsstyring i tråd med beskyttelseskravene, som definert i "Guideline 4 – ICT and security risks within the risk management system"
- Prosedyrene bør etableres, håndheves/etterleves, overvåkes og periodisk gjennomgås
- Prosedyren bør også inkludere kontroller for overvåking av uregelmessigheter
- Prosedyrene bør som et minimum inkludere:
  - Tilganger tildeles basert på prinsippet om "need-to-know, least privilege and segregation of duties"
  - Begrense bruken av delte brukerkontoer → må kunne identifisere bruker
  - Privilegerte brukertilganger – streng kontroll og overvåkning av bruk
  - Fjerntilgang (remote access) til kritiske IKT-systemer bør kun gis ved behov og når sterke autentiseringsløsninger brukes

Guideline 8 forts.

§5

Guideline 8 – Logical security

- Beslutning om logging av brukeraktivitet bør bestemmes ut fra risikovurderinger og bør som et minimum omfatte privilegerte brukere
- Tilgangsstyring - tilgangsrettigheter gis, fjernes og endres umiddelbart i forhold til behov, og i henhold til forhåndsdefinerte rutiner for godkjenning der eier av informasjonsobjektet er involvert
- Periodisk gjennomgang av behovet for tilganger
- Endringer i tilganger bør dokumenteres på en måte som gir mulighet for innsikt og analyse
- Metoder for autentisering – bør stå i forhold til kritikaliteten til IKT-systemet, informasjonen eller prosessen som er tilgjengelig. bør minimum inkludere sterke passord eller sterkere autentiseringsmetoder (som to-faktor autentisering)

➢ Elektronisk tilgang fra applikasjoner til data- og IKT-systemer bør begrenses til det minimum som kreves for å yte den aktuelle tjenesten

Guideline 9 - 10

Guideline 9 – Physical security §5

- Fysiske sikkerhetstiltak (f.eks. beskyttelse mot strømbrudd, brann, vann og uautorisert fysisk tilgang) bør defineres, dokumenteres og implementeres for å beskytte lokaler, datasentre og sensitive områder mot uautorisert tilgang, og fra miljøfarer (vind, regn/vann, snø, jordskjelv m.m.)
- Fysisk tilgang til IKT-systemer bør kun gis til autoriserte personer

Guideline 10 – ICT operations security §8

- Foretak bør implementere prosedyrer for å sikre konfidensialitet, integritet og tilgjengelighet av IKT-systemer og IKT-tjenester for å minimere konsekvensen av sikkerhetshendelser i leveransen av IKT-tjenester. Disse prosedyrene bør inkludere følgende tiltak:
  - Identifisering av sårbarheter som skal evalueres og utbedres (patch)
  - Implementere sikre basis konfigurasjonsinnstillinger for kritiske komponenter slik som OS, DB, rutere og switcher

Guideline 10 forts.

§8

- Implementere nettverkssegmentering, etablere systemer for å forebygge datalekkasje (DLP) og kryptere nettverkstrafikk
- Implementere beskyttelse av endepunkter inkludert servere, arbeidsstasjoner og mobile enheter. Vurdering av om endepunkt oppfyller sikkerhetsstandardene før det gis tilgang til bedriftsnettverket
- Kryptering av lagrede data (at rest) og data som er under transport (in transit) i henhold til kravene satt i informasjonsklassifiseringen

Guideline 11

§2, §5

Guideline 11 – Security monitoring

- **Foretaket bør etablere og implementere prosedyrer og prosesser for kontinuerlig overvåkning av aktiviteter som påvirker foretakenes informasjonssikkerhet.**
- **Med utgangspunkt i overvåkningen bør foretaket etablere hensiktsmessige og effektive kapabiliteter for å oppdage, rapportere og respondere på unormale aktiviteter og trusler, slik som fysisk eller logisk inntrenging, brudd på konfidensialitet, integritet og tilgjengelighet av informasjonsressurser, ondsinnet kode og offentlig kjente sårbarheter for programvare og maskinvare**
- **Rapportene fra overvåkningen skal hjelpe foretaket til å forstå typen av hendelser, identifisere trender og bør gi informasjon til å støtte foretakets interne undersøkelser og gjennom dette utgjøre et informativt beslutningsgrunnlag**

Guideline 12

§2, §8

Guideline 12 – Information security reviews, assessment and testing

- **Foretaket bør utføre ulike sikkerhetsgjennomganger, vurderinger og tester, for å sikre effektiv identifisering av sårbarheter i IKT-systemer og -tjenester. Eksempel utføre gap-analyser mot informasjonssikkerhetsstandarder, compliance-gjennomganger, interne og eksterne revisjoner av informasjonssystemene eller fysiske sikkerhetsgjennomganger**
- **Foretaket bør etablere og implementere et rammeverk for testing av informasjonssikkerhet som validerer robustheten og effektiviteten til informasjonssikkerhetstiltakene og sikre at rammeverket inkluderer trusler og sårbarheter som er identifisert gjennom trusselovervåking og risikovurderingene for IKT- og IKT-sikkerhet**
- **Testing bør utføres på en trygg og sikker måte utført av uavhengige testere med tilstrekkelig kunnskap, ferdigheter og ekspertise i å teste informasjonssikkerhetstiltak**

Guideline 12 forts.

§2, §8

Guideline 12 – Information security reviews, assessment and testing

- **Foretak bør utføre tester periodisk. Omfanget, frekvensen og metoden for testing (som penetrasjonstesting, inkludert trusseldrevet penetrasjonstesting (TLPT)) bør stå i forhold til det risikonivået som er identifisert. Testing av kritiske IKT-systemer og sårbarhetsskanning bør utføres årlig**
- **Foretak bør sikre at det gjennomføres test av sikkerhet ved endringer i infrastruktur, prosesser eller prosedyrer og dersom endringer gjøres på grunn av større operasjonelle hendelser eller sikkerhetshendelser. Test av sikkerheten bør også gjøres for nye eller vesentlig endrede kritiske applikasjoner. Foretak bør overvåke og evaluere testresultatene, og bør ved behov iverksette sikkerhetstiltak**

Guideline 13 - 14

Guideline 13 – Information security training and awareness §5

- Foretaket bør avholde kurs i informasjonssikkerhet for samtlige ansatte (inklusive ledelse) periodisk
- Foretaket bør ha periodiske sikkerhetsbevissthetsprogrammer for å utdanne sine ansatte (inkludert ledelse) i hvordan de skal håndtere informasjonssikkerhetsrelaterte risikoer

Guideline 14 – ICT operations management §8, §11, §13

- Dokumentasjon i foretaket bør definere hvordan virksomheten styrer, overvåker og kontrollerer IKT-systemene og IKT-tjenestene, herunder dokumentasjon av kritiske IKT-prosesser, prosedyrer og operasjoner.
- Foretak bør implementere logging og overvåkingsprosedyrer for kritiske IKT-operasjoner for å kunne oppdage, analysere og korrigere feil
- Foretaket bør ha en oppdatert oversikt over IKT-utstyr som inneholder tilstrekkelig informasjon for å kunne identifisere utstyret, utstyrets plassering, sikkerhetsklassifisering og eierskap

Guideline 14 forts.

§8, §11, §13

- Foretak bør overvåke og administrere livssyklusen til IKT-utstyr for å sikre at utstyret innfrir forretnings- og risikostyringskrav, at utstyret støttes av leverandører og interne utviklere, samt at alle relevante oppdateringer og oppgraderinger er installert. Risiko knyttet til utdatert eller ikke-støttede IKT-utstyr bør vurderes og minimeres. Utrangerte IKT-utstyr bør behandles og avhendes på en sikker måte
- Implementering av ytelses- og kapasitetsplanleggings- og overvåkingsprosesser
- Foretak bør definere og implementere sikkerhetskopiering og gjenopprettingsplaner for data og IKT-systemer slik at man har trygghet for at de kan gjenopprettes ved behov. Testing av sikkerhetskopierings- og gjenopprettingsprosedyrene bør utføres periodisk
- Sikkerhetskopier av data og IKT-systemer lagres på ett eller flere steder utenfor primæranlegget - tilstrekkelig langt unna primæranlegget slik at man unngår samme risiko

Guideline 15

§9

Guideline 15 - ICT incident and problem management

- **Foretaket bør etablere og implementere en hendelses- og problemhåndteringsprosess inkludert en hendelsesresponsprosess for overvåkning og logging av drifts- og sikkerhetshendelser Hendelsesresponsprosess skal bidra til at foretaket har mulighet for kontinuitet, eller rask gjenoppretting av kritiske forretningsfunksjoner og prosesser når det oppstår avvik**
- **Foretaket bør sørge for oppfølging av hendelser for å sikre at de grunnleggende årsakene blir identifisert, behandlet og at korrigerende tiltak iverksettes for å forhindre at hendelsen skjer igjen**
- **Etablere prosedyrer for identifisering, sporing, logging, kategorisering og klassifisere hendelser i henhold til en prioritet definert av foretaket og basert på forretningskritikalitet;**
- **Etablere interne og eksterne kommunikasjonsplaner - varsling av hendelse og eskaleringsprosedyrer**

Guideline 16 - 17

Guideline 16 – ICT project management §2, §6

- **Foretaket bør implementere en IKT-prosjektmetodikk med styringsprosess og prosjektimplementeringsledelse**
- **Foretaket bør overvåke og redusere risikoer som stammer fra porteføljen av IKT-prosjekter, samt risikoer som kan oppstå ved gjensidig avhengighet mellom ulike prosjekter, og for ressurser som benyttes i flere prosjekter samtidig**

Guideline 17 - ICT systems acquisition and development §2, §6

- **Foretaket bør utvikle og implementere en prosess for anskaffelse, utvikling og vedlikehold av IKT-systemer. Dette bør sikre at konfidensialitet, integritet, tilgjengelighet for dataene som skal behandles er tilstrekkelig sikret og at definerte krav til beskyttelse er innfridd. Prosessen utformes basert på en risikobasert tilnærming**

Guideline 17 forts.

§2, §6

Guideline 17 - ICT systems acquisition and development

- **Før systemanskaffelser eller utviklingsaktiviteter skjer bør funksjonelle og ikke-funksjonelle (inkludert krav til informasjonssikkerhet) og tekniske krav være klart definert**
- **Det bør være etablert tiltak for å hindre utilsiktede endringer eller tilsiktede manipuleringer av IKT-systemene under utvikling**
- **Det bør være etablert en metodikk for testing og godkjenning**
- **Produksjonsmiljøer bør holdes adskilt fra utviklings-, test- og andre ikke-produksjonsmiljøer**
- **Tiltak for å beskytte integriteten til kildekoden.**
- **Prosessene for anskaffelse og utvikling gjelder også for IKT-systemer utviklet eller administrert av sluttbrukere utenfor IKT-organisasjonen iht. en risikobasert tilnærming. Applikasjonene bør føres i eget register dersom de utgjør forretningskritiske funksjoner eller prosesser**

Guideline 18

§9

Guideline 18 - ICT change management

- **Foretaket bør etablere og implementere en endringshåndteringsprosess for å sikre at alle endringer i IKT-systemer registreres, vurderes, testes, godkjennes, autoriseres og implementeres på en kontrollert måte. Dette inkluderer også IKT-endringer i såkalte haste- eller nødsituasjoner, der det også bør være sporbarhet, slik at system-/asset-eier kan foreta analyser i ettertid**
- **Foretaket bør ha kontroll med om endringer i det eksisterende driftsmiljøet påvirker eksisterende sikkerhetstiltak, og om dette eventuelt krever risikoreduserende tiltak. Slik endringene bør følge foretakets formelle endringshåndteringsprosess**

Guideline 19 - 20

Guideline 19 – Business continuity management §11

- Som del av foretakets overordnede policy for forretningskontinuitet (Business Continuity Policy) har ledelsen har ansvar for å fastsette og godkjenne foretakets IKT-kontinuitetspolicy, samt sørge for at denne blir gjort kjent

Guideline 20 – Business impact analysis (BIA) §11

- Foretaket bør gjennomføre en forretningsmessig konsekvensanalyse for å identifisere foretakets eksponering for alvorlige avbrudd, og de potensielle konsekvensene, kvantitativt og kvalitativt. Vurdering bør også omfatte kritikaliteten til de identifiserte og klassifiserte forretningsprosesser, roller, data og utstyr, og gjensidige avhengigheter i samsvar med GL 4.
- Foretaket bør sikre at IKT-systemer og IKT-tjenester er utformet og tilpasset den forretningsmessige konsekvensanalysen, med eksempelvis redundans for visse kritiske komponenter for å hindre avbrudd

Guideline 21

Guideline 21 – Business continuity planning (BCP) §11

- De forretningsmessige kontinuitetsplanene (Business Continuity Plans (BCP)) bør vurdere de vesentlige risikoene som kan ha en negativ innvirkning på IKT-systemer og IKT-tjenester. Planene bør støtte opp om målsetninger om å beskytte og, om nødvendig, gjenopprette konfidensialitet, integritet og tilgjengelighet for forretningsprosesser, roller, data og utstyr. Foretaket bør etablere BCP sammen med de relevante interne og eksterne interessentene
- Foretaket bør fastsette BCP for å sikre hensiktsmessige handlinger i forhold til de potensielle feilscenariene
  - innen maksimal tid for reetablering (Recovery Time Objective (RTO)
  - maksimalt tap av data, målt i tid, som kan bli tapt etter en hendelse (Recovery Point Objective (RPO))
- Foretaket bør vurdere ulike scenarier i sine BCPer, inkludert ekstreme, men plausible scenarier og cyberangrepsscenarier. Utfra scenariene bør foretaket beskrive hvordan kontinuitet og informasjonssikkerhet bør sikres

Guideline 22

§11

Guideline 22 – Response and recovery plans

- **Basert på konsekvensanalysen og scenariene bør virksomheter utvikle respons- og gjenopprettingsplaner. Planene bør fastsette kravene for aktivering av planen og de tiltak som skal iverksettes som skal sikre integritet, tilgjengelighet, kontinuitet og gjenoppretting av (i det minste) foretakenes kritiske IKT-systemer, IKT-tjenester og data. Respons- og gjenopprettingsplanene bør ta sikte på å oppfylle gjenopprettingsmålene (RTO og RPO)**
- **Respons- og gjenopprettingsplanene bør vurdere kortsiktige, og eventuelt langsiktige, alternativer for gjenoppretting. Planene bør minst:**
  - **fokusere på gjenoppretting av driften av viktige IKT-tjenester, forretningsfunksjoner, støtteprosesser, informasjonsressurser**
  - **være dokumentert og gjort tilgjengelig for forretnings- og støtteenhetene, og bør være enkelt tilgjengelig i nødstilfeller. Planen bør ha klare definisjoner av roller og ansvar**

Guideline 22 forts

§11

Guideline 22 – Response and recovery plans

- **Respons- og gjenopprettingsplanene bør kontinuerlig oppdateres basert på erfaringer fra hendelser, tester, nylig identifiserte risikoer og trusler, og endringer i gjenopprettingsmål og prioriteringer**
- **Planene bør også vurdere alternativer dersom gjenoppretting ikke er mulig på kort sikt grunnet kostnader, risiko, logistikk eller uforutsette omstendigheter**
- **Som del av respons- og gjenopprettingsplanene bør foretaket vurdere og implementere kontinuitetstiltak for å håndtere avbrudd hos de viktigste tjenesteleverandørene ift. forretningsmessig tjenestekontinuitet**

Guideline 23

§11

Guideline 23 – Testing of plans

- **Foretak bør teste sine BCP-er og sikre at driften av forretningsprosesser, roller, data og utstyr regelmessig testes basert på foretakenes risikoprofil.**
- **BCP-er bør oppdateres regelmessig, basert på testresultater, gjeldende trusselvurdering og erfaringer fra tidligere hendelser. Eventuelle endringer i gjenopprettingsmål og/eller endringer forretningsprosesser, roller, data og utstyr bør også inkluderes.**
- **BCP-testing skal vise at foretaket er i stand til å opprettholde virksomheten inntil kritiske operasjoner er reetablert på et forhåndsdefinert tjenestenivå**
- **Testresultater bør dokumenteres og identifiserte mangler bør analyseres, adresseres og rapporteres til ledelsen.**

Guideline 24 - 25

Guideline 24 - Crisis communications §9, §11

- I tilfelle avbrudd eller nødsituasjon, og under implementeringen av BCP-ene, bør foretaket sikre at de har etablert krisekommunikasjonstiltak slik at relevante interne og eksterne interessenter, inkludert relevante tilsynsmyndigheter og relevante tjenesteleverandører informeres på en rettidig og hensiktsmessig måte.

Guideline 25 – Outsourcing of ICT services and ICT systems §2, §12

- Uten begrensing ift. EIOPAs retningslinjer om outsourcing til skytjenesteleverandører, bør foretaket sikre at IKT-tjenester og IKT-systemer som utkontrakteres oppfyller alle relevante krav til IKT-tjenesten eller IKT-systemet.

Guideline 25 forts.

§2, §12

Guideline 25 – Outsourcing of ICT services and ICT systems

- Ved outsourcing av kritiske eller viktige funksjoner bør foretaket sørge for at kontraktsmessige forpliktelser (f.eks. kontrakt, servicenivåavtaler, oppsigelsesbestemmelser i de relevante kontraktene) minst omfatter:
  - hensiktsmessige og forholdsmessige informasjonssikkerhetsmål og -tiltak, inkludert minimumskrav til informasjonssikkerhet, spesifikasjoner av foretakenes datalivssyklus, revisjons- og tilgangsrettigheter samt eventuelle krav til plassering av datasentre og krav til datakryptering, nettverkssikkerhet og sikkerhetsovervåkingsprosesser
  - tjenestenivåavtaler for å sikre kontinuitet og ytelsesmål under normale omstendigheter, og i tilfelle tjenesteavbrudd
  - prosedyrer for håndtering av operasjonelle og sikkerhetshendelser, inkludert eskalering og rapportering
- Foretaket bør overvåke og få bekreftet etterlevelse av sikkerhetsmål, tiltak og ytelsesmål hos tjenesteleverandøren

7. Implementering i norsk rett

FT må bekrefte at man akter å følge den enkelte retningslinjen, og hvordan man akter å innlemme dette i norsk rett – comply/explain-prosedyre.

Her er FT sin informasjon for å bekrefte etterlevelse

- **Finanstilsynet har bekreftet at retningslinjene vil bli fulgt i Norge fra samme dato som retningslinjene skal gjelde i EU, 1. juli 2021.**
- **Norge har siden 2003 hatt IKT-forskriften som regulerer de områder som retningslinjene omfatter. Videre gir Finansforetaksloven og Finanstilsynsloven utfyllende bestemmelser.**
- **Det er Finanstilsynets vurdering at de nye retningslinjene fra EIOPA er dekkende for de områdene foretakene skal vurdere risiko for, og at de gir en nyttig utdyping på områder som reguleres av IKT-forskriften og lovgiving.**
- **Finanstilsynet vil oppdatere sin tilsynspraksis og forventninger til behandling av IKT-sikkerhetsrisiko i tråd med de nye retningslinjene.**
- **Finanstilsynet vil arrangere et Webinar (dette) med gjennomgang av de nye retningslinjene for forsikringsbransjen i Norge.**

8. Relevante nyhetsbrev og nettsteder

- Nyhetsbrev
  - Norske
    - Finanstilsynet.no: https://www.finanstilsynet.no/nyhetsvarsel/pamelding/
    - Lovdata – Europalov: https://www.europalov.no/nyhetsbrev
    - Finans Norge (link nederst på siden): https://www.finansnorge.no/
  - EU
    - EIOPA - https://ec.europa.eu/newsroom/eiopa/user-subscriptions/2078/create
    - EC - EU-Kommisjonen – Shaping Europe's Digital Future - https://digital-strategy.ec.europa.eu/en/newsletters

- Nettsteder
  - Finanstilsynet - https://www.finanstilsynet.no/nyhetsarkiv/?l=no
  - Lovdata – Europalov - https://www.europalov.no
  - EIOPA - https://www.eiopa.europa.eu/news-events_en
  - EC – EU-Kommisjonen - https://digital-strategy.ec.europa.eu/en/news