VEDLEGG 2: GRUNNLAG FOR RISIKOMATRISEN

Finanstilsynets vurdering av de mest sentrale sårbarhetene i finanssektoren, med angivelse av sannsynlighet og graden av konsekvens for det enkelte foretak, er omtalt i dette vedlegget. Med bakgrunn i observasjoner og vurderinger i kapittel 3 til 7, i tillegg punkt 8.1, utgjør vurderingene nedenfor grunnlag for risikomatrisen i figur 8.1 i kapittel 8.

Følgende definisjoner benyttes:

Sårbarhet: Svakhet i teknisk infrastruktur, funksjoner og prosesser som kan resultere i at uønskede hendelser inntreffer.

Trussel: Forhold med potensial til å forårsake en uønsket hendelse.

Risiko: Uttrykkes som kombinasjonen av sannsynligheten for at en hendelse inntreffer og konsekvensen dersom den inntreffer. Utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne aktører kan medføre økende sannsynlighet for at en hendelse inntreffer, med tilhørende konsekvenser.

Konsekvens: Følger av en uønsket hendelse.

Risikovurdering: Identifikasjon, analyse og evaluering av risiko. En risikovurdering legger grunnlag for foretakets risikoreduserende tiltak og prioritering av disse.

Styringsmodell og internkontroll

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved foretakets styringsmodell og internkontroll som middels. Sannsynligheten for at de tre forsvarslinjene gjennom sin aktivitet ikke avdekker alvorlige svakheter i foretakets internkontroll, vurderes som middels og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at mangler i etterlevelsen av lover og regler ikke oppdages som følge av manglende kontroll av foretakets operative ledelse, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at viktige krav i styrende dokumenter ikke implementeres og operasjonaliseres, herunder kontroller, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at risikostyringsfunksjonen ikke har tilstrekkelig IKT-kompetanse til å ivareta sin andrelinjefunksjon på IKT-området, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at etterlevelsesfunksjonen ikke avdekker alvorlige svakheter i operative enheters kontroll, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at foretakets styre og ledelse ikke har informasjon som bekrefter eller avkrefter etterlevelse av interne og eksterne krav, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at foretakets styre og ledelse ikke bidrar til at IT-investeringer understøtter foretakets strategi og behov, og forståelse av risikobildet innen IKT-området som er nødvendig for å sikre en stabil og sikker IKT-drift, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for uklare roller mellom foretakets første- og andrelinjeforsvar som fører til alvorlige svakheter i overvåkingen av og kontrollen med foretakets styring og kontroll, vurderes som middels og med begrenset til middels konsekvens.
- Sannsynligheten for at alvorlige sårbarheter ikke avdekkes som følge av mangelfull risikostyring mellom operative enheter og risikostyringsfunksjonen i andrelinjen, vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for at alvorlige svakheter i internkontrollen ikke avdekkes av internrevisjonen som følge av mangelfull kompetanse og risikoforståelse hos foretakets internrevisjon, vurderes som lav og med moderat konsekvens.

- Sannsynligheten for alvorlige organisatoriske utfordringer som følge av svak endringsledelse vurderes som middels og med moderat konsekvens.

Kompetanse og kompetansestyring

Finanstilsynet anser den samlede risikoen, på nåværende tidspunkt, knyttet til sårbarheter ved kompetanse og kompetansestyring som middels. Sannsynligheten for at uønskede hendelser oppstår eller at uønskede hendelser ikke blir håndtert tilstrekkelig som en konsekvens av manglende kompetanse i Norge, vurderes som middels og konsekvensen som begrenset til moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at styre og ledelse ikke har tilstrekkelig oversikt over ansattes kompetanse, og heller ikke har oversikt over nåværende og framtidige behov som følge av mangelfull kompetansestyring, vurderes som lav til middels og med begrenset til moderat konsekvens.
- Sannsynligheten for at mangelfull kompetansestyring i foretak medfører tap av og/eller manglende kompetanse for å ivareta en forsvarlig drift, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at manglende sikkerhetskompetanse i foretaket medfører vesentlige operasjonelle risikoer, vurderes som middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for driftsavbrudd og utilgjengelige tjenester som følge av mangelfull kompetanse vurderes som lav og med moderat til høy konsekvens.
- Sannsynligheten for at informasjonssikkerhetsbrudd inntreffer som følge av mangelfull tilgang på sikkerhetskompetanse, vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for at mangelfull kompetanse i foretaket om tjenester som utvikles og driftes av leverandører, medfører brudd på lover og regler, vurderes som lav til middels og med begrenset konsekvens.
- Sannsynligheten for en økt avhengighet av leverandører i utlandet som følge av mangel på ressurser og et økt behov i Norge, vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for at manglende forståelse av risikoene ved bruk av skytjenester fører til uønskede hendelser, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at manglende kompetanse innen ny teknologi, som RPA, AI og blokkjede, medfører at vesentlige operasjonelle risikoer ved bruk ikke avdekkes, vurderes som middels og med begrenset til moderat konsekvens.

Leverandørstyring

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved leverandørstyring som middels til høy. Sannsynligheten for uønskede hendelser vurderes som middels til høy og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at vesentlige avvik i leverandørens internkontroll ikke oppdages av foretaket, vurderes som middels til høy og med moderat til alvorlig konsekvens.
- Sannsynligheten for at sikkerhetsbrudd inntreffer som følge av mangelfull oppfølging og forankring av sikkerhetskravene hos leverandøren, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for uforsvarlig lang reetableringstid ved alvorlige driftsavbrudd som følge av uklare roller og ansvar i samhandlingen med leverandøren og mellom leverandørene, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for utilgjengelige tjenester som følge av manglende overvåking av kvaliteten på tjenesten, vurderes som lav og med moderat konsekvens.
- Sannsynligheten for uønsket leverandøravhengighet som følge av mangelfulle reguleringer (eksempelvis uttredelsesbestemmelser) i avtalen vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for uønsket leverandøravhengighet som følge av foretakets mangelfulle kompetanse om foretakets utkontrakterte tjenester vurderes som middels til høy og med begrenset til middels konsekvens.

- Sannsynligheten for at manglende (periodisk) risikovurdering ikke avdekker svak bærekraft hos leverandøren, for eksempel som følge av en krevende likviditetssituasjon (konkursrisiko), utfordrende ressurssituasjon eller andre forhold som kan true leverandørens leveranseevne, vurderes som lav og med moderat konsekvens.
- Sannsynligheten for at alvorlige svakheter i en leverandørs internkontroll ikke avdekkes gjennom en leverandørs valgte revisors arbeid med uavhengig revisjonserklæring, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for manglende kvalitetssikring av tjenester anskaffet fra ulike leverandører og underleverandører som følge av mangelfull oppfølging og kompetanse, samt forankring av egne krav hos leverandøren og underleverandørene, vurderes som middels til høy og med moderat konsekvens.

Digital kriminalitet

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter og trusler som kan føre til skade som følge av digital kriminalitet, som høy. Samlekarakteren er ikke endret i årets rapport, men Finanstilsynet vurderer at risikoen er noe forhøyet fra 2021 med bakgrunn i økt kriminell aktivitet, spesielt rettet mot kunder av foretakene. Sannsynligheten for uønskede hendelser vurderes som høy og konsekvensen som alvorlig. Dette er basert på følgende vurderinger:

- Sannsynligheten for at alvorlige svakheter i et foretaks forsvarsverk ikke avdekkes som følge av mangelfull eller manglende sikkerhetstest, vurderes som middels til høy og med alvorlig konsekvens.
- Sannsynligheten for at et foretak har vesentlige feil i sikkerhetskonfigureringen av kritiske systemer som følge av manglende gradering av systemene, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at et foretak har vesentlige feil i sikkerhetskonfigureringen av skytjenester, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at foretak rammes av løsepengevirus med tap av forretningskritiske data som følge av skadevare (kryptering), vurderes som middels og med kritisk konsekvens.
- Sannsynligheten for at foretaket ikke avdekker kriminelle som har etablert et digitalt fotfeste på innsiden av nettverket før skade avverges, vurderes som middels med kritisk konsekvens.
- Sannsynligheten for at kriminelle lykkes med å utnytte sårbarheter i nettverk og applikasjoner før de oppdages (til patch foreligger), vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at alvorlige sikkerhetshull ikke blir tidsnok tettet som følge av mangelfulle sikkerhetsoppdateringer (patch management), inklusive hos leverandører og underleverandører, vurderes som middels med alvorlig konsekvens.
- Sannsynligheten for svake punkter i forsvarsverket fordi foretaket ikke har kontroll med sårbarhetsstyringen av software og hardware med tilhørende konfigurasjon, vurderes som middels med alvorlig konsekvens.
- Sannsynligheten for at nye applikasjoner eller endringer i eksisterende applikasjoner settes i produksjon med alvorlige sikkerhetshull, inklusive hos leverandører og underleverandører, vurderes som middels med alvorlig konsekvens.
- Sannsynligheten for at tredjeparts applikasjoner som tredjepart integrerer i eller mellom foretakets systemer og foretakets kunder, fører til uønskede sikkerhetshendelser, vurderes som middels til høy med moderat til alvorlig konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører utgjør en vesentlig sårbarhet som følge av uaktsomhet og manglende kompetanse om sikker bruk av foretakets systemer, vurderes som lav til middels og med alvorlig konsekvens
- Sannsynligheten for at kriminelle eller fremmed etterretning forsøker å rekruttere ansatte eller personell hos leverandører for å få tilgang til informasjon om sårbarheter i digital infrastruktur eller annen informasjon om foretaket, eller for at ansatte i foretaket / personell hos leverandører gjennom trusler ufrivillig benyttes som redskap for digitale angrep, vurderes som middels og med alvorlig konsekvens.

- Sannsynligheten for at ansatte gjennom sosial manipulering ufrivillig benyttes som middel for digitalt angrep, vurderes som høy og med alvorlig konsekvens.
- Sannsynligheten for at kunder av foretaket gjennom sosial manipulering ufrivillig benyttes som middel for de kriminelles økonomiske vinning, vurderes som høy og med moderat konsekvens.
- Sannsynligheten for at kunder av foretaket gjennom sosial manipulering frivillig benyttes som middel for de kriminelles økonomiske vinning, vurderes som middels med moderat konsekvens.
- Sannsynligheten for at utro medarbeidere utnytter svakheter i systemet for økonomisk vinning, vurderes som lav til middels og med begrenset konsekvens.
- Sannsynligheten for at utro ansatte i foretaket eller personell i leverandørers utviklingsmiljø plasserer ondsinnet kode i forretningskritiske applikasjoner, vurderes som lav og med moderat konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører hjelper kriminelle med å sluse kriminelle transaksjoner gjennom et foretaks systemer, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at personinformasjon, herunder informasjon om foretaks ansatte og personell hos leverandører som har roller som kan være av interesse for og utnyttes av kriminelle, kommer kriminelle i hende, vurderes som middels til høy og med alvorlig konsekvens.
- Sannsynligheten for at foretak benytter kommunikasjonsmåter som også benyttes av kriminelle ved forsøk på sosial manipulering, vurderes som middels og med begrenset til moderat konsekvens.
- Sannsynligheten for at svakheter ved etablering og bruk av sikkerhetsmekanismer fører til nye angrepsflater kriminelle vil benytte, vurderes som middels og med moderat konsekvens.

Informasjonslekkasje

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter og trusler som kan føre til skade som følge av informasjonslekkasje, som middels til høy. Finanstilsynet observerer at foretakene har blitt bedre på arbeidet med å forhindre informasjonslekkasjer og jobber aktivt med området for å sikre sine verdier. Sannsynligheten for uønskede hendelser vurderes som middels til høy og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at klassifisert dokumentasjon sendes uautorisert ut av foretaket som følge av manglende klassifisering og kontroll, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende kontroll ved utsendelse av e-post, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende kontroll ved bruk av USB-lagringsmedier, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende kontroll av personell hos leverandører, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon som kan benyttes til å skade foretaket, sendes eller formidles uautorisert, bevisst eller ubevisst, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører opererer som innsidere og overleverer eller sender konfidensiell informasjon, eksempelvis liste over e-postadresser og påloggingsinformasjon, til kriminelle, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende kontroll eller feil ved utsendelse av informasjon til kunder, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie på grunn av bruk av bærbart utstyr utenfor kontorets nettverk, vurderes som middels til høy og med moderat konsekvens.

IKT-drift

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved IKT-drift som middels. Finanstilsynet observerte at vurderer at risikoen er noe redusert fra 2021 med bakgrunn i den bedrede tilgjengeligheten til

betalingstjenester og kunderettede løsninger. Sannsynligheten for uønskede hendelser vurderes som middels og konsekvensen som moderat til alvorlig. Dette er basert på følgende vurderinger:

- Sannsynligheten for ustabile og/eller utilgjengelige tjenester som følge av økt grad av integrasjon mellom ulike tjenesteleverandører, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for driftsproblemer som følge av feil i felles infrastruktur vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for driftsproblemer som følge av manglende kompetanse og tilstrekkelig helhetlig forståelse for og oversikt over arkitektur og de digitale forretningsprosessene, vurderes som middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for redusert datakvalitet som følge av kompleks integrasjon mellom tjenesteleverandører vurderes som lav og med moderat konsekvens.
- Sannsynligheten for driftsproblemer som følge av mangelfull endringsstyring (maskinvare, applikasjoner, databaser, operativsystem m.m.) vurderes som middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for at avtalt tid for retting av kritiske feil ikke overholdes som følge av kompleksitet i systemporteføljen med integrasjon mellom nye og gamle systemer, vurderes som lav til middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for at overvåking av IT-miljøet ikke avdekker unormale forhold ved driften (f.eks. utgåtte sertifikater, databaser, minnelekkasjer og elektroniske komponenter), vurderes som middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for driftsproblemer grunnet manglende oppfølging av teknisk gjeld vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for at testsystemet ikke er tilstrekkelig likt produksjonssystemet, vurderes som middels til høy og med moderat til alvorlig konsekvens.

Beredskap og krisehåndtering

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved beredskap og krisehåndtering som middels til høy. Sannsynligheten for uønskede hendelser som medfører at kriseløsning for kritiske forretningsprosesser må iverksettes, vurderes som svært lav til lav og konsekvensen som alvorlig til kritisk dersom denne ikke fungerer som forutsatt. Dette er basert på følgende vurderinger:

- Sannsynligheten for at foretakets kriseløsning ikke er etablert i henhold til foretakets behov som følge av manglende eller mangelfulle forretningsmessige konsekvensanalyser og krav, vurderes som middels til høy og med kritisk konsekvens dersom kriseløsningen må iverksettes.
- Sannsynligheten for at foretak og dets medarbeidere ikke er tilstrekkelig forberedt på å håndtere en alvorlig situasjon som følge av mangelfull trening og øvelser, vurderes som middels og med kritisk konsekvens.
- Sannsynligheten for at et foretaks krisehåndtering og dets leverandørs krisehåndering ikke er tilstrekkelig samordnet og koordinert ved en alvorlig hendelse, vurderes som middels og med kritisk konsekvens.
- Sannsynligheten for at foretak ikke klarer å håndtere en alvorlig hendelse på en god måte som følge av uklare roller og ansvar internt og mellom foretaket og leverandører, vurderes som lav til middels og med alvorlig konsekvens.
- Sannsynligheten for at kriseløsningen ikke fungerer som forventet som følge av mangler i teknisk oppsett og infrastruktur og testing av kriseløsningene, samt i evalueringen, vurderes som lav til middels og med kritisk konsekvens.
- Sannsynligheten for manglende oppdateringer, inklusive sikkerhetsoppdateringer, av kriseløsningen vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at et foretak som blir rammet av et alvorlig digitalt angrep, ikke vil være i stand til å håndtere situasjonen på en god måte som følge av manglende beredskapsplan for cyberangrep og mangel på trening og øvelse, vurderes som middels og med kritisk konsekvens.

Geopolitiske forhold

Finanstilsynet anser risikoen knyttet til sårbarheter overfor utenlandske aktører som leverer kritiske IKT-tjenester til foretakene i Norge, som middels til høy. Det var store endringer i geopolitiske forhold i 2022 med krigen i Ukraina. Foretakene har informert Finanstilsynet om at krigen har endret trusselbildet i et cybersikkerhetsperspektiv, men samtidig har det ikke vært rapportert noen økning hendelser. Sannsynligheten for uønskede hendelser der utenlandske leverandører blir avskåret fra å levere sine tjenester, vurderes som lav og konsekvensen som alvorlig. Dette er basert på følgende vurderinger:

- Sannsynligheten for at et foretaks beredskapspersonell ikke vil være i stand til å opprettholde sikker og stabil drift der utenlandske leverandører ikke er tilgjengelige, vurderes som lav og med alvorlig konsekvens.
- Sannsynligheten for at et foretaks beredskapspersonell ikke vil være i stand til å opprettholde sikker og stabil drift ved alvorlige IKT-hendelser der utenlandske leverandører ikke er tilgjengelige, vurderes som lav til middels og med alvorlig konsekvens.
- Sannsynligheten for kommunikasjonsbrudd med utlandet hvor konsekvensen er at utenlandske leverandører er avskåret fra å utføre kritiske IKT-tjenester, vurderes som lav og med alvorlig konsekvens.
- Sannsynligheten for at foretak blir rammet av geopolitiske forhold knyttet til IKT-drift, vurderes som lav til middels og med alvorlig konsekvens.

Endringsstyring

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved endringsstyring som middels. Sannsynligheten for uønskede hendelser vurderes som middels og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for utilgjengelige tjenester som følge av ikke-funksjonelle endringer (endring i konfigurasjon av driftskomponenter) vurderes som middels og med moderat konsekvens.
- Sannsynligheten for svakheter i rutinene for endringshåndtering (herunder mangelfull testing) vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at det ikke er etablert tilstrekkelige kontroller for å identifisere endringer, funksjonelle og ikke-funksjonelle, som er satt i produksjon uten at endringsprosessen er fulgt, såkalte uautoriserte endringer, vurderes som middels og med moderat til alvorlig konsekvens.
- Sannsynligheten for at funksjonelle endringer (programvare) introduserer sårbarheter i foretakets forsvarsverk, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at en høy endringstakt grunnet ny forretningsfunksjonalitet og regulatoriske krav medfører at løsninger settes i produksjon uten nødvendig kvalitetssikring, vurderes som middels og med moderat konsekvens.

Tilgangsstyring

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved tilgangsstyring som middels til høy. Samlekarakteren er ikke endret i årets rapport, men Finanstilsynet vurderer at risikoen er noe forhøyet fra 2021 med bakgrunn i rapporterte hendelser og gjennomførte tilsyn. Sannsynligheten for uønskede hendelser vurderes som middels til høy og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at ansatte med utvidede tilgangsrettigheter utfører ulovlige handlinger, vurderes som lav til middels og med moderat konsekvens.
- Sannsynligheten for at personell hos en leverandør med utvidede tilgangsrettigheter utfører ulovlige handlinger, vurderes som middels og med alvorlig konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører har tilgangsrettigheter uten at foretakets ledelse er klar over dette, vurderes som middels til høy og med moderat konsekvens.

- Sannsynligheten for at ansatte eller personell hos leverandører har utvidede tilgangsrettigheter uten at ledelsen er klar over dette, vurderes som middels til høy og med moderat til alvorlig konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull tilgangsstyring og -kontroll med ansattes tilganger, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at konfidensiell og/eller gradert informasjon kommer på avveie som følge av sikkerhetsbrudd hos leverandøren, vurderes som middels til høy og med moderat konsekvens.
- Sannsynligheten for at personell hos leverandøren, eller dens underleverandør, bryter regler i utførelsen av driftsoppgaver, vurderes som middels til høy og med alvorlig konsekvens.

Datakvalitet

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved datakvalitet som middels. Sannsynligheten for uønskede hendelser vurderes som middels og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at beslutninger tas på feil grunnlag, vurderes som middels og med moderat konsekvens.
- Sannsynligheten for at AML-systemet ikke fanger opp alle betalingstransaksjoner, vurderes som middels til høy og med moderat konsekvens.