itm8 A/S

Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om foranstaltninger til styring af risici pr. 3. juli 2026 i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med kunder

Juli 2026

Indhold

1. Ledelsens udtalelse

itm8 A/S (itm8) leverer tjenester dækket af NIS2 til kunder i henhold til aftale.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt itm8's tjeneste vedrørende managed services, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har udført ved vurdering af, om kravene til sikring af et højt cybersikkerhedsniveau i henhold til gældende lovgivning er overholdt.

Fuzion og InterXion er serviceleverandører, der leverer housing-ydelser til itm8, mens B4Restore og Keepit er serviceleverandører, der leverer backupydelser til itm8. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos itm8 og ikke kontrolmål og tilhørende kontroller hos Fuzion, InterXion, B4Restore og Keepit. Vores vurdering har ikke omfattet kontroller hos Fuzion, InterXion, B4Restore og Keepit.

itm8 anvender datterselskaberne itm8 Philippines Inc. og itm8 Prague S.R.O. som underleverandører til understøttelse af serviceleverancen. Underleverandørerne leverer blandt andet driftsydelser, servicedesk-support, udvikling og rådgivning, herunder 24/7-overvågning og alarmhåndtering. Selskaberne er organisatorisk integreret med og styret af den danske organisation og er underlagt de samme politikker, procedurer, sikkerhedskrav og instrukser som øvrige dele af itm8-koncernen.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos kunderne, der er forudsat i udformningen af vores kontroller, er hensigtsmæssigt designet og implementeret. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen af sådanne komplementære kontroller hos kunderne.

itm8 bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en hensigtsmæssig præsentation af itm8's managed services, der har været anvendt af kunder pr. 3. juli 2026. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan itm8's managed services var designet og implementeret, herunder redegør for:

   - De typer af tjenester, der er leveret
   - De processer i net- og informationssystemer, der er anvendt til at levere tjenesterne
   - Hvordan net- og informationssystemer behandler andre betydelige begivenheder end dem, der direkte vedrører levering af tjenester
   - De processer, der i tilfælde af brud på sikkerheden vedrørende tjenester understøtter, at kunder kan foretage anmeldelse til tilsynsmyndigheden
   - De processer, der er rettet mod begivenheder, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer
   - Relevante kontrolmål og kontroller designet og implementeret til at nå disse mål
   - Komplementære kontroller, som vi med henvisning til afgrænsningen af itm8's managed services har forudsat ville være implementeret af kunderne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for levering af tjenester

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af itm8's managed services, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og derfor ikke kan omfatte alle aspekter ved itm8's managed services, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt designet og implementeret pr. 3. juli 2026. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

c) Der er etableret og opretholdt passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer med henblik på at levere tjenester til kunder samt for at forhindre hændelser eller minimere deres indvirkning.

I relation til ovenstående vurderinger bemærkes, at reguleringen vedrørende krav til sikkerheden i net- og informationssystemer er ny og kompleks. Der har endnu ikke på alle områder udviklet sig en konsistent praksis for, hvordan de enkelte regler skal fortolkes. Selvom det er vores vurdering, at vi har etableret og opretholdt passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger, kan der således vise sig at være forhold, hvor myndigheder og samarbejdspartnere anlægger en anden vurdering.

Herning, 8. juli 2026
itm8 A/S

Frank Bech
Head of Compliance and Security

2. Uafhængig revisors erklæring om beskrivelsen af kontroller, deres design og implementering

Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om foranstaltninger til styring af risici pr. 3. juli 2026 i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med kunder

Til: itm8 A/S (itm8), og kunder

Omfang

Vi har fået som opgave at afgive erklæring om itm8's beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til managed services, der har behandlet kunders transaktioner i hele perioden fra 3. juli 2026 (beskrivelsen), og om hensigtsmæssigheden af designet og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om itm8 har designet og implementeret hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 3. Erklæringen omfatter ikke en vurdering af itm8's generelle efterlevelse af kravene i EU's direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og "Lov om foranstaltninger til sikring af højt cybersikkerhedsniveau (NIS2 loven)".

Fuzion og InterXion er serviceleverandører, der leverer housing-ydelser til itm8, mens B4Restore og Keepit er serviceleverandører, der leverer backupydelser til itm8. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos itm8 og ikke kontrolmål og tilhørende kontroller hos Fuzion, InterXion, B4Restore og Keepit. Vores undersøgelse har ikke omfattet kontroller hos Fuzion, InterXion, B4Restore og Keepit.

itm8 anvender datterselskaberne itm8 Philippines Inc. og itm8 Prague S.R.O. som underleverandører til understøttelse af serviceleverancen. Underleverandørerne leverer blandt andet driftsydelser, servicedesk-support, udvikling og rådgivning, herunder 24/7-overvågning og alarmhåndtering. Selskaberne er organisatorisk integreret med og styret af den danske organisation og er underlagt de samme politikker, procedurer, sikkerhedskrav og instrukser som øvrige dele af itm8-koncernen.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos kunderne, der er forudsat i udformningen af itm8's kontroller, er hensigtsmæssigt designet og implementeret. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen af sådanne komplementære kontroller hos kunderne.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med begrænset sikkerhed.

itm8's ansvar

itm8 er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at fastlægge kontrolmålene og anføre dem i beskrivelsen; for at identificere de risici, der truer opnåelsen af kontrolmålene; for at identificere kriterierne samt for at designe og implementere kontroller for at opnå de anførte kontrolmål. Kontrolmålene er fastlagt af itm8 og er anført i beskrivelsen.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om hensigtsmæssigheden af præsentationen af itm8's beskrivelse samt om hensigtsmæssigheden af designet og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå begrænset sikkerhed for, at beskrivelsen i alle væsentlige henseender er hensigtsmæssigt præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og implementeret.

En erklæringsopgave med begrænset sikkerhed, hvor der afgives erklæring om beskrivelsen og om hensigtsmæssigheden af designet og implementeringen af kontroller hos en NIS2-serviceleverandør, omfatter udførelse af handlinger for at opnå bevis for oplysningerne i NIS2-serviceleverandørens beskrivelse af sin tjeneste samt for kontrollernes design og implementering. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er hensigtsmæssigt præsenteret, og at kontrollerne ikke er hensigtsmæssigt designet og implementeret. En erklæringsopgave med begrænset sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt relevansen af de kriterier, som itm8 har specificeret og beskrevet i afsnit 1.

Handlingerne i en opgave med begrænset sikkerhed varierer i art og tidsmæssig placering fra, og har mindre omfang end, en opgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Iboende begrænsninger

itm8's beskrivelse er udarbejdet for at opfylde de almindelige behov hos kunderne og omfatter derfor ikke nødvendigvis alle aspekter ved managed services, som kunderne måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en NIS2-serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle brud på cybersikkerheden. Herudover er fremskrivningen til fremtidige perioder af enhver vurdering af hensigtsmæssigheden af præsentationen af beskrivelsen, eller af konklusioner om hensigtsmæssigheden af designet og implementeringen af de kontroller, der er nødvendige for at nå de tilhørende kontrolmål, undergivet risikoen for, at kontroller hos en NIS2-serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. På baggrund af kriterierne og de kontrolmål, der er beskrevet i itm8's udtalelse i afsnit 1, er det vores opfattelse, at vi ikke er blevet bekendt med forhold, der giver os anledning til at konkludere:

a) at beskrivelsen af managed services, som designet og implementeret pr. 3. juli 2026, ikke i alle væsentlige henseender er hensigtsmæssigt præsenteret

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt designet og implementeret med henblik på at opnå sikkerhed for, at de anførte kontrolmål ville være opnået, hvis de beskrevne kontroller var operationelt effektive pr. 3. juli 2026, og hvis kunderne udførte de komplementære kontroller, der er omtalt i afsnit 3.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse tests fremgår af afsnit 4.

Tiltænkte brugere og formål

Vi har af itm8 fået til opgave at afgive erklæring, og derfor er denne erklæring samt beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf tiltænkt itm8.

Vi tillader kun, at itm8 – efter eget skøn – offentliggør denne erklæring i dens fulde længde, herunder beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf. Offentliggørelse må kun ske til kunder, der har anvendt itm8's managed services pr. 3. juli 2026, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information om kontroller, som kunder selv har anvendt ved vurdering af, om kravene til sikring af et højt cybersikkerhedsniveau i henhold til gældende lovgivning er overholdt. PwC påtager sig intet ansvar over for kunder.

Vores erklæring må ikke anvendes til andre formål og må ikke udleveres til andre parter.

Aarhus, 8. juli 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3. Systembeskrivelse

3.1. Beskrivelse af NIS2-relateret servicelevering

Formålet med denne systembeskrivelse er at beskrive de organisatoriske og tekniske foranstaltninger, som itm8 A/S har implementeret for at understøtte overholdelse af kravene i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 (NIS2-direktivet) samt den danske gennemførelseslovgivning. Systembeskrivelsen omfatter de cybersikkerhedsforanstaltninger, som itm8 anvender i forbindelse med levering af administrerede it-tjenester, professionelle services og sikkerhedstjenester til kunder, der enten selv er omfattet af NIS2 eller stiller tilsvarende krav til deres leverandører.

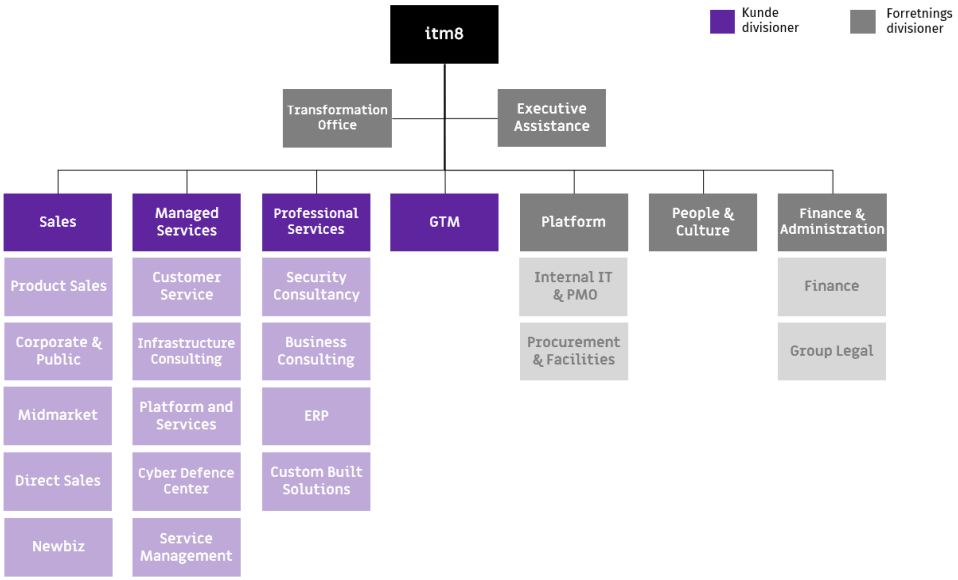
itm8 leverer hosting og drift, support, databaseadministration, konfiguration og udvikling, sikkerhedsservices, applikationsservices samt konsulentydelser. Som leverandør af administrerede it-tjenester og administrerede sikkerhedstjenester er itm8 selv omfattet af NIS2-direktivets anvendelsesområde og har derfor implementeret et samlet sæt af risikostyringsforanstaltninger, der både opfylder itm8's egne forpligtelser og understøtter kundernes overholdelse af direktivet.

Rammen for cybersikkerhedsforanstaltningerne er forankret i itm8's ledelsessystem for informationssikkerhed (ISMS), der er certificeret efter ISO/IEC 27001:2022. Denne systembeskrivelse beskriver, hvorledes de ti kategorier af risikostyringsforanstaltninger i NIS2-direktivets er omsat til praktiske kontroller hos itm8.

3.2. Beskrivelse af serviceorganisationen

itm8 A/S har gennemgået en markant udvikling og er blevet en mere struktureret organisation, der leverer administrerede it-tjenester og professionelle services. itm8 A/S Danmark er etableret på baggrund af 12 selvstændige it-virksomheder, som alle er ejet af itm8-koncernen. Alle 12 virksomheder er nu juridisk og organisatorisk fusioneret ind i itm8 A/S, som ud over de danske lokationer også omfatter itm8's globale leverancelokationer i Tjekkiet og Filippinerne. Som en naturlig del af fusionen foregår der en stor transition i at konsolidere og ensarte services, processer og systemer.

Alle virksomheder er fusioneret ind i itm8 A/S' kundeorienterede afdelinger, der driver serviceleverancer, mens forretningsdivisioner sikrer nødvendig administrativ og operationel støtte. Denne opbygning gør itm8 i stand til at levere integrerede og pålidelige tjenester, der lever op til høje krav inden for informationssikkerhed, kvalitet og compliance til en bred vifte af kunder.



Denne uafhængige revisionserklæring fokuserer på de services, som leveres fra itm8's kundedivisioner Managed Services og Professional Services, hvor leverancen omfatter net- og informationssystemer, der enten anvendes af kunder omfattet af NIS2, eller hvor selve tjenesten falder ind under NIS2-direktivets anvendelsesområde.

Erklæringen omfatter desuden itm8 A/S' globale leveranceorganisation, som ud over Danmark inkluderer itm8 Tjekkiet og itm8 Filippinerne.

Kundedivisioner

De kundeorienterede divisioner udgør itm8's primære serviceområder, hvor hver division er dedikeret til specifikke ekspertiseområder:

- **Managed Services —** Med fokus på cloud-løsninger og it-infrastruktur hjælper denne division kunder med at implementere robuste hosting- og driftsstrategier. Divisionen omsætter kundernes forretningsstrategier til skalerbare cloud- og infrastrukturløsninger gennem platformsevalueringer, design af sikkerhedspolitikker, migrationer, modernisering og 24/7-support. Managed Services indeholder desuden Cyber Defense Center, som er en afdeling, der tilbyder omfattende sikkerhedstjenester, herunder løbende SIEM-loghåndtering, sårbarhedsvurderinger og realtidshændelseshåndtering via et 24x7 Security Operation Center.

- **Professional Services —** Denne division driver digital innovation for kunderne og tilbyder ERP-integration, SharePoint og Microsoft-løsninger samt unikke produkter udviklet af Team Products, såsom Send Secure-platformen og Tandlægejournalsystemet (TK2), for at optimere forretningsprocesser.

Forretningsdivisioner

Som støtte til disse kerneområder leverer itm8's forretningsdivisioner såsom People and Culture, Finans, Marketing, Jura, Intern IT og Compliance & Security en solid base for effektiv servicelevering. Disse divisioner er afgørende for itm8's driftsmæssige integritet og sikrer, at alle kundeorienterede aktiviteter er i overensstemmelse med itm8's standarder og lovgivningsmæssige krav.

Sammen skaber disse divisioner en robust struktur, der gør itm8 i stand til at levere specialiserede tjenester af høj kvalitet, der understøtter kundernes strategiske mål samt deres forpligtelser under NIS2.

3.3. NIS2 anvendelsesområde og klassifikation

itm8 A/S er identificeret som omfattet af NIS2-direktivet i kraft af koncernens aktiviteter inden for datacentertjenester, udbyder af cloudcomputing-tjenester, administrerede it-tjenester (managed services) og administrerede sikkerhedstjenester (managed security services). itm8 klassificeres som væsentlig enhed i henhold til NIS2-direktivets bilag I, kategorien for udbydere af administrerede tjenester og administrerede sikkerhedstjenester.

itm8's egen klassifikation, omfang og samspil med relevante myndigheder, herunder den nationale CSIRT-funktion og den kompetente tilsynsmyndighed, er dokumenteret i itm8's NIS2-compliance-program. Programmet ejes af Compliance & Security-afdelingen og opdateres mindst én gang årligt eller ved væsentlige ændringer i regulatoriske krav eller organisationens aktiviteter.

itm8 leverer desuden tjenester til kunder, der selv er omfattet af NIS2 som væsentlige eller vigtige enheder. itm8 understøtter disse kunders compliance gennem leverandørbaserede sikkerhedsforanstaltninger, kontraktuelle forpligtelser, ISAE-erklæringer og løbende rapportering.

3.4. Cybersikkerhedsstyring

Ledelsessystemet for informationssikkerhed (ISMS) hos itm8 er designet til at opfylde kravene i ISO/IEC 27001:2022 og er det rammeværk, hvori NIS2-direktivets risikostyringsforanstaltninger er integreret. Topledelsen har det overordnede ansvar for cybersikkerhed og NIS2-compliance og har godkendt itm8's informationssikkerhedspolitik.

I overensstemmelse med NIS2-direktivets artikel 20 har topledelsen ansvaret for at godkende cybersikkerhedsforanstaltningerne, føre tilsyn med deres gennemførelse og kan stilles til ansvar for manglende overholdelse. Ledelsens medlemmer deltager i cybersikkerhedstræning, som svarer til kravene for ledelsesorganer i NIS2-direktivet, og fremmer tilsvarende vidensopbygning i hele organisationen.

Compliance & Security-afdelingen, der arbejder under delegation fra ledelsen, har ansvaret for at overvåge implementeringen, kontrollen og den løbende forbedring af cybersikkerheds- og compliance-programmet på tværs

af organisationen. Afdelingen koordinerer med Cyber security- og Legal-kommissionerne for at håndtere både tekniske og juridiske aspekter af cybersikkerheden.

3.5. Risikostyringsforanstaltninger

itm8 har implementeret de risikostyringsforanstaltninger, der følger af NIS2-direktivets artikel 21, stk. 2. Foranstaltningerne tager udgangspunkt i ISO/IEC 27001:2022-kontroller og er tilpasset omfanget af de tjenester, itm8 leverer, samt den risiko, som tjenesterne udsætter kunder og samfundskritisk infrastruktur for. Nedenstående afsnit beskriver, hvordan hver af de ti kategorier er forankret hos itm8.

3.5.1. Kontrolmål 1 - Risikovurdering

itm8 anvender en struktureret tilgang til risikostyring som en integreret del af virksomhedens ISMS. Der gennemføres regelmæssigt risikovurderinger af implementerede kontroller, behandlingsaktiviteter og leverandører baseret på en sandsynligheds-/konsekvensmodel. Trusler, der overstiger itm8's maksimalt acceptable risikoniveau, håndteres gennem en risikobehandlingsplan med henblik på at reducere eller eliminere den tilknyttede risiko. Risikovurderinger dokumenteres og opdateres mindst én gang årligt eller ved væsentlige ændringer.

Den overordnede informationssikkerhedspolitik samt de tilhørende 15 emnespecifikke politikker udgør grundlaget for cybersikkerhedsforanstaltningerne. Politikkerne ejes af Compliance & Security-afdelingen, gennemgås mindst én gang årligt og kommunikeres til relevante interessenter.

3.5.2. Kontrolmål 2 - Hændelseshåndtering

itm8 håndterer cybersikkerhedshændelser gennem en struktureret Incident Management-proces, som omfatter særskilte procedurer for både større hændelser og sikkerhedshændelser. Procedurerne beskriver roller, ansvar og de nødvendige trin til at vurdere, reagere på, begrænse og lære af hændelser.

Cyber Defense Center leverer døgnbemandet overvågning (24x7) gennem et Security Operations Center (SOC) og driver SIEM-logstyring, som registrerer og overvåger aktiviteter på interne systemer og kundemiljøer i overensstemmelse med de aftalte ydelser. Der indsamles systematisk bevismateriale under hændelseshåndteringen for at understøtte analyse og dokumentation. Tidsstempling sikres gennem synkronisering af systemernes ure, så hændelser kan korreleres pålideligt på tværs af systemer.

Erfaringer og læring fra hændelser indgår som en obligatorisk del af afslutningen af hændelser for at sikre, at læringspunkter omsættes til konkrete forbedringer, der reducerer sandsynligheden for, at lignende hændelser opstår igen.

3.5.3. Kontrolmål 2 - Logning og overvågning

Adgang til kundesystemer og kritiske interne systemer er begrænset til autoriserede brugere baseret på et arbejdsrelateret behov. Al adgang til kundesystemer foretaget af itm8's medarbejdere logges, herunder oplysninger om tidspunkt, bruger, tildelte rettigheder og det tilgåede system. Logdata opbevares i mindst seks måneder, hvorefter de slettes på sikker vis. Kravene til logning omfatter blandt andet:

- Login til administrationsplatformen for adgang til kundesystemer.
- Login til kundeservere.
- Login til specifikke systemer og tjenester leveret af itm8.

User Management-afdelingen gennemfører flere kontroller og gennemgange i løbet af året for at sikre overholdelse af politikker for adgangsstyring. Cyber Defense Center overvåger løbende logdata gennem SIEM-løsningen og iværksætter undersøgelser samt hændelseshåndtering ved afvigelser fra normal aktivitet.

3.5.4. Kontrolmål 3 - Forretningskontinuitet og krisestyring

itm8's styring af forretningskontinuitet er designet til at sikre fortsat drift og organisatorisk robusthed. Beredskabs- og kontinuitetsplanerne beskriver kommunikationsstrategier, roller og procedurer for opretholdelse af forretningskritiske funktioner under driftsforstyrrelser eller større hændelser, herunder cyberangreb og infrastruktursvigt. Planerne testes og opdateres mindst én gang årligt.

Kriseberedskabet aktiveres på baggrund af definerede eskalationskriterier og involverer virksomhedens øverste ledelse, Compliance & Security-afdelingen, Cyber Defense Center samt relevante drifts- og supportfunktioner.

3.5.5. Kontrolmål 3 - Backup og redundans

itm8 har etableret omfattende og sikre backupfaciliteter med redundante sikkerhedskopier, der administreres af en ISO/IEC 27001-certificeret tredjepartsleverandør. Backupdata opbevares i geografisk adskilte faciliteter for at sikre tilgængelighed i tilfælde af større driftsforstyrrelser.

Der er etableret procedurer for katastrofehåndtering og genetablering af kritiske IT-understøttede forretningsprocesser, herunder gendannelse af backupdata. Formålet er at understøtte en rettidig genopretning af systemer og data, så driften kan genoptages efter alvorlige hændelser eller nedbrud.

3.5.6. Kontrolmål 4 - Leverandørstyring

itm8 håndterer leverandørrelationer med fokus på cybersikkerhed. Aftaler med leverandører indeholder, hvor det er muligt og relevant, sikkerhedsbilag, og leverandørernes driftsmæssige praksis overvåges løbende med henblik på at identificere potentielle risici og problemstillinger. En formel onboardingproces for leverandører sikrer, at leverandører kategoriseres og vurderes, inden der indgås aftaler.

Der gennemføres løbende risikovurderinger af kritiske leverandører for at håndtere potentielle risici. Risikovurderingerne omfatter blandt andet en vurdering af leverandørens cybersikkerhedsmodenhed, tidligere sikkerhedshændelser, gennemgang af erklæringer såsom ISAE 3402 og ISAE 3000 samt en vurdering af leverandørens egen forsyningskæde, hvor dette er relevant.

Hvis en leverandør ikke leverer en standardiseret erklæring, eller hvis der identificeres væsentlige observationer, følges der op gennem en kontrolvurdering og om nødvendigt gennem leverandørtilsyn. Cloud Security-strategien beskriver sikkerhedsmæssige overvejelser ved anvendelse af cloudtjenester, herunder strategier for håndtering af leverandørafhængighed samt exit-strategier.

3.5.7. Kontrolmål 5 - Sikkerhed ved anskaffelse, udvikling og vedligeholdelse af netværks- og informationssystemer

itm8 håndterer applikations- og systemsikkerhed i overensstemmelse med kontrollerne i ISO/IEC 27001:2022. Der er implementeret en Secure Development Life Cycle (SDLC), som integrerer sikkerhedskrav tilpasset applikationernes kritikalitet. Sikker systemarkitektur og sikre kodningsprincipper anvendes for at reducere sårbarheder, og der udføres sikkerhedstest i både udviklings- og acceptfasen for at validere applikationerne, inden de overgår til produktion. Udviklings-, test- og produktionsmiljøer holdes adskilt.

Adgang til kildekode er begrænset til medarbejdere med et arbejdsbetinget behov, og outsourcet udvikling er underlagt specifikke sikkerhedskrav og retningslinjer. Patch management-processen sikrer, at softwareopdateringer og sikkerhedsrettelser implementeres på en sikker måde og inden for de kontraktmæssigt aftalte tidsfrister.

Change management er en integreret del af tilgangen og omfatter risikovurdering af ændringer. Kritiske ændringer behandles og gennemgås på CAB-møder (Change Advisory Board) for at sikre, at potentielle påvirkninger identificeres, vurderes og håndteres inden implementering.

3.5.8. Kontrolmål 5 - Sårbarhedsstyring

itm8 har etableret processer og kontroller til løbende identifikation, vurdering og håndtering af tekniske sårbarheder i virksomhedens infrastruktur, systemer og applikationer. Sårbarheder identificeres gennem en kombination af sikkerhedsovervågning, automatiserede scanninger, sikkerhedsadviseringer fra leverandører samt trusselsinformation fra relevante kilder.

Identificerede sårbarheder vurderes på baggrund af risiko og potentiel påvirkning af fortrolighed, integritet og tilgængelighed, hvorefter passende afhjælpende foranstaltninger iværksættes. Kontroller og processer sikrer, at sårbarheder håndteres rettidigt og i overensstemmelse med deres kritikalitet med henblik på at reducere risikoen for sikkerhedshændelser og kompromittering af systemer og data.

3.5.9. Kontrolmål 6 - Vurdering af implementerede sikkerhedsforanstaltninger

For at sikre, at cybersikkerhedsforanstaltningerne er effektive, overvåger, måler og evaluerer itm8 løbende sine sikkerhedsprocesser. Et struktureret program for intern revision gennemgår systematisk alle elementer i ISMS'et over en treårig periode. Resultaterne heraf kombineres med ledelsens gennemgange og øvrige målinger og anvendes som grundlag for løbende forbedringer.

itm8 indhenter desuden uafhængige eksterne erklæringer og certificeringer, herunder ISO/IEC 27001-certificering samt ISAE 3402- og ISAE 3000-erklæringer (GDPR), der dækker relevante tjenesteydelser. Observationer og afvigelser identificeret gennem revisioner anvendes som input til kvartalsvise Continuous Improvement Meetings (CIM) i Compliance & Security-afdelingen, hvor der træffes beslutninger om korrigerende handlinger og prioritering af forbedringsinitiativer.

3.5.10. Kontrolmål 6 - Teknisk sikkerhedstestning

itm8 gennemfører tekniske sikkerhedstest af systemer, applikationer og infrastruktur med henblik på at identificere sårbarheder og validere effektiviteten af de implementerede sikkerhedskontroller.

Testaktiviteterne kan omfatte sårbarhedsvurderinger, penetrationstest, konfigurationsgennemgange samt verifikation af implementerede sikkerhedsforanstaltninger. Identificerede observationer og sårbarheder risikovurderes og håndteres gennem etablerede afhjælpningsprocesser. Der følges løbende op på disse, indtil passende korrigerende handlinger er gennemført og dokumenteret.

3.5.11. Kontrolmål 7 - Grundlæggende cyberhygiejnepraksis

itm8 opretholder et cybersikkerhedsprogram, der fremmer god cyberhygiejne på tværs af organisationen.

De tekniske kontroller, der understøtter cyberhygiejnen, omfatter sårbarhedsstyring, patch management, malwarebeskyttelse, standarder for sikker konfiguration, identitets- og adgangsstyring samt løbende sikkerhedsovervågning. Disse foranstaltninger understøtter overholdelse af kravene i NIS2-direktivet og bidrager til den samlede robusthed og modstandsdygtighed i virksomhedens informationssystemer og tjenester.

3.5.12. Kontrolmål 7 - Cybersikkerhedstræning

itm8 arbejder med strukturerede programmer for sikkerhedstræning og test af medarbejdere. Programmerne påbegyndes ved ansættelse som en del af onboardingforløbet og fortsætter herefter løbende gennem planlagte træningsmoduler samt test af organisationens modstandsdygtighed over for phishingangreb.

Træningen består af en kombination af standardiseret sikkerhedsundervisning og målrettet træning, der er tilpasset itm8's egne retningslinjer og krav. Indholdet omfatter grundlæggende cyberhygiejne, herunder håndtering af adgangskoder, korrekt anvendelse af multifaktorgodkendelse (MFA), identifikation af social engineering, sikker håndtering af e-mails og data, brug af mobile enheder samt indberetning af mistænkelige hændelser.

Medlemmer af ledelsen modtager målrettet cybersikkerhedstræning, der omhandler ledelsens ansvar, risikobevidsthed og tilsynsforpligtelser i overensstemmelse med NIS2-direktivet.

3.5.13. Kontrolmål 8 - Kryptografi

itm8 har etableret en politik for anvendelse af kryptografiske kontroller, som understøtter beskyttelsen af informationsaktiver i overensstemmelse med organisationens risikovurderinger. Politikken omfatter valg af krypteringsalgoritmer, nøglehåndtering, anvendelse af kryptering til data under lagring og transmission samt krav til certifikatstyring. Retningslinjerne afspejler anerkendt praksis i branchen og er tilpasset de relevante kontroller i ISO/IEC 27001:2022.

Kundedata krypteres i overensstemmelse med de aftalte tjenesteydelser. Ved transmission af data anvendes etablerede sikre kommunikationsprotokoller, og ved lagring af data benyttes kryptering, hvor dette er aftalt eller påkrævet. Kryptografiske nøgler og certifikater administreres centralt og understøttes af tilhørende procedurer for hele deres livscyklus, herunder udstedelse, opbevaring, fornyelse og afvikling.

3.5.14. Kontrolmål 9 - Personalesikkerhed

itm8 gennemfører baggrundstjek af medarbejdere ved ansættelse, herunder indhentelse af straffeattester for medarbejdere i kritiske funktioner. Straffeattester fornyes hvert tredje år under ansættelsesforholdet for at opretholde et højt niveau af pålidelighed og tillid. Ansættelsesvilkårene indeholder specifikke bestemmelser vedrørende informationssikkerhed, og en disciplinær proces sikrer håndhævelse af politikkerne ved overtrædelser. Adgangsrettigheder administreres omhyggeligt ved fratrædelser eller ændringer i arbejdsfunktioner.

Politikken for adgangskontrol regulerer tildeling og fjernelse af adgang på baggrund af jobmæssige behov. Identitets- og adgangsstyring håndteres i samarbejde mellem ledere, User Management og HR og omfatter hele livscyklussen for brugeridentiteter. Privilegerede adgange begrænses til medarbejdere med et dokumenteret behov, og der er etableret specifikke regler for håndtering af privilegerede konti og autentifikationsoplysninger. Brugeradgange gennemgås mindst én gang årligt for almindelige konti og kvartalsvist for privilegerede konti.

itm8 administrerer informationer og tilknyttede aktiver gennem en central CMDB (Configuration Management Database) for konfigurationsenheder (CI'er) og kundevendte løsninger samt via Intune MDM til styring af endpoints. Politikker for acceptabel brug beskriver kravene til medarbejdernes anvendelse af virksomhedens aktiver og skal sikre en ansvarlig håndtering heraf. Procedurer for tilbagelevering, sikker bortskaffelse og genanvendelse af aktiver udgør en integreret del af de etablerede processer.

3.5.15. Kontrolmål 9 - Adgangskontrol

itm8 efterlever kontrollerne i ISO/IEC 27001:2022 med henblik på at beskytte adgangen til systemer og information. Der er implementeret en politik for adgangskontrol samt tilhørende procedurer, som sikrer en effektiv styring af brugeradgange. Identitets- og adgangsstyring håndteres i samarbejde mellem ledere, User Management og HR og omfatter hele livscyklussen for brugeridentiteter – fra oprettelse og ændringer til deaktivering og sletning.

Adgangsrettigheder tildeles på baggrund af medarbejderens arbejdsfunktion og forretningsmæssige behov, og privilegerede adgange er begrænset til personer med et dokumenteret behov herfor. Adgang til følsomme oplysninger, herunder kundedata og HR-relaterede oplysninger, begrænses og kontrolleres i overensstemmelse med etablerede politikker og retningslinjer.

3.5.16. Kontrolmål 9 – Asset management

itm8 administrerer information og tilknyttede aktiver i overensstemmelse med kravene i ISO/IEC 27001:2022. Fortegnelser over virksomhedens aktiver vedligeholdes gennem flere systemer, herunder en central CMDB (Configuration Management Database) til håndtering af konfigurationsenheder og kundevendte løsninger samt Microsoft Intune til administration af endpoint-enheder. Politikker og sikkerhedsvejledninger beskriver regler for acceptabel brug og ansvarlig håndtering af aktiver.

Procedurer for tilbagelevering af aktiver er integreret i HR-processerne for at sikre korrekt håndtering ved fratrædelse eller ændringer i medarbejderes roller og ansvarsområder. Derudover er der etableret retningslinjer for beskyttelse af aktiver uden for virksomhedens lokationer samt for sikker håndtering og opbevaring af lagringsmedier.

3.5.17. Kontrolmål 9 - Fysisk sikkerhed

itm8 opretholder fysiske sikkerhedsforanstaltninger for at beskytte virksomhedens aktiver og faciliteter. Der er etableret fysiske sikkerhedsperimetre omkring kontorer og datacentre, og fysisk adgang kontrolleres gennem anvendelse af ID-kort, PIN-koder, alarmsystemer og videoovervågning ved centrale adgangspunkter.

Kontorer, lokaler og faciliteter sikres på baggrund af deres følsomhed gennem anvendelse af sikkerhedszoner og tilpassede sikkerhedsforanstaltninger. Der er implementeret beskyttelse mod både fysiske og miljømæssige trusler med henblik på at sikre kontinuerlig drift og beskyttelse af informationer og udstyr.

Der er etableret procedurer for arbejde i sikrede områder samt krav om clean desk og clear screen, som reducerer risikoen for uautoriseret adgang til følsomme oplysninger.

Kritisk udstyr er beskyttet gennem hensigtsmæssig fysisk placering og understøttende faciliteter såsom nødgeneratorer og UPS-løsninger (nødstrømsforsyning). Udstyr vedligeholdes i overensstemmelse med producenternes anbefalinger, og kabelføring beskyttes mod manipulation, skader og uautoriseret adgang.

3.5.18. Kontrolmål 10 - Multifaktorgodkendelse

itm8 håndhæver sikker autentificering på tværs af organisationen, og multifaktorgodkendelse (MFA) anvendes som standard ved adgang til administrationsplatforme, fjernadgangsløsninger, kritiske systemer samt alle privilegerede konti. Hvor det er muligt og relevant, stilles tilsvarende krav til kunder som en del af de aftalte tjenesteydelser.

Sikker kommunikation understøttes gennem anvendelse af krypterede kommunikationskanaler til daglig kommunikation, fildeling og samarbejde. itm8 anvender etablerede platforme med stærk kryptering under transmission samt adgangskontrolmekanismer for at beskytte informationer mod uautoriseret adgang. Der anvendes desuden særskilte løsninger til kommunikation om særligt følsomme emner, herunder håndtering af sikkerhedshændelser.

I tilfælde af alvorlige hændelser kan nødkommunikation etableres via særskilt udvalgte kommunikationskanaler, som er uafhængige af den normale driftsinfrastruktur. Dette bidrager til at sikre fortsat kommunikation og koordinering, selv hvis de primære systemer påvirkes af en hændelse.

3.5.19. Kontrolmål 10 - Nødkommunikationssystemer

itm8 har etableret og testet alternative kommunikationskanaler, som kan anvendes i tilfælde af en katastrofesituation eller større hændelse, hvor de normale kommunikationskanaler ikke er tilgængelige.

Disse beredskabskommunikationsløsninger skal sikre, at kritisk kommunikation og koordinering kan opretholdes under ekstraordinære forhold, så relevante interessenter fortsat kan udveksle information og understøtte håndteringen af hændelsen.

3.6. Indberetning af hændelser

itm8 har etableret en procedure for indberetning af cybersikkerhedshændelser, der er tilpasset kravene i NIS2-direktivets artikel 23. Når en hændelse vurderes at være væsentlig, initieres følgende indberetningsforløb:

- Tidlig varsling til den nationale CSIRT-funktion eller den kompetente myndighed uden unødigt ophold og senest 24 timer efter, at itm8 er blevet bekendt med hændelsen, med en foreløbig vurdering af, om hændelsen har grænseoverskridende karakter eller skyldes ondsindede handlinger

- Hændelsesnotifikation senest 72 timer efter, at itm8 er blevet bekendt med hændelsen, med en opdateret vurdering, herunder hændelsens alvor, virkninger og kompromisindikatorer

- Slutrapport senest én måned efter hændelsesnotifikationen med en detaljeret beskrivelse af hændelsen, dens alvor og virkninger, sandsynlig årsag, gennemførte og igangværende afhjælpende foranstaltninger samt eventuelle grænseoverskridende virkninger.

Når hændelsen involverer et kundesystem, eller hvor itm8 på vegne af en kunde understøtter kundens egen NIS2- eller GDPR-indberetning, koordineres tidshorisonter og indhold via en sag i itm8's service managementsystem. itm8 bistår kunden med at opfylde kundens egne indberetningsforpligtelser i overensstemmelse med aftalen.

3.7. Tilsyn med leverandører og underleverandører

itm8 sikrer, at godkendte leverandører og underleverandører overholder relevante sikkerheds- og lovgivningskrav gennem regelmæssig overvågning. Dette omfatter indhentning af årlige it-revisionserklæringer, eksempelvis ISAE 3402 eller ISAE 3000, udført af uafhængige tredjeparter. Hvis sådanne erklæringer ikke leveres, anvender itm8 en risikobaseret tilgang baseret på Datatilsynets vejledning samt på itm8's egne tilsynskoncepter og gennemfører om nødvendigt on-site-revisioner for at verificere overholdelsen.

itm8 anvender sine datterselskaber, itm8 Philippines Inc. og itm8 Prague S.R.O., som underleverandører for at understøtte servicelevering i samarbejde med den danske organisation. Disse enheder håndterer tjenester såsom drift, servicedesk-support, udvikling og rådgivning, herunder 24/7-overvågning og alarmhåndtering. itm8 Philippines Inc. og itm8 Prague S.R.O. er 100 % integreret og styres fra den danske organisation og følger de samme sikkerhedsguidelines og instruktioner.

3.8. Overvågning og logning

Adgang til kundesystemer og kritiske interne systemer er begrænset til autoriserede brugere baseret på et arbejdsrelateret behov. Al adgang til kundesystemer fra itm8's personale logges, hvor der fanges detaljer såsom tidsstempel, bruger, privilegier og det system, der blev tilgået. Logge opbevares i mindst seks måneder, før de slettes sikkert. Logningskravene omfatter:

- Login til administrationsplatform for adgang til kundesystemer
- Login til kundeservere
- Login til specifikke systemer og tjenester leveret af itm8.

User Management-afdelingen gennemfører flere revisioner i løbet af året for at sikre overholdelse af adgangskontrolpolitikkerne. Cyber Defense Center overvåger logge løbende via SIEM-løsningen og igangsætter undersøgelser og hændelseshåndtering ved afvigelser fra normal aktivitet.

3.9. Rapportering til ledelsen

Ledelsen har ansvaret for cybersikkerheden i itm8 og sikrer overensstemmelse med organisatoriske mål, lovgivningsmæssige krav og NIS2-direktivets bestemmelser. Compliance & Security-afdelingen leverer regelmæssigt rapporter til ledelsen om it-sikkerhed, informationssikkerhed, status for cybersikkerhedshændelser samt status for NIS2-relaterede initiativer.

Ledelsen er ansvarlig for itm8's overordnede sikkerhedspolitikker, og Compliance & Security er ansvarlig for at sikre, at de nødvendige procedurer og instruktioner implementeres for at opfylde målene i politikkerne. Politikkerne gennemgås mindst én gang årligt for at opretholde relevans og effektivitet.

Risikovurderinger af kritiske informationer, infrastruktur og datasikkerhedsforhold gennemføres løbende i samarbejde med ledelsen og integrerer NIS2-compliance som en kernekomponent i itm8's informationssikkerhedsstyringssystem.

3.10. Compliance, roller og ansvar

Ansvar for informationssikkerhed og compliance hos itm8 er forankret på ledelsesniveau. Topledelsen fastlægger den strategiske retning og sikrer overensstemmelse med itm8's forpligtelser til kvalitet og lovgivningsmæssige standarder. Compliance & Security-afdelingen, der arbejder under delegation fra ledelsen, har ansvaret for at overvåge implementeringen, kontrollen og den løbende forbedring af cybersikkerheds- og compliance-programmet på tværs af organisationen.

itm8 er organiseret i specialiserede divisioner, der omfatter både kundeorienterede og forretningsstøttende funktioner. De kundeorienterede divisioner omfatter:

- Managed Services
- Professional Services.

Disse divisioner leverer skræddersyede it-tjenester og overholder samtidig itm8's høje standarder for sikker og compliant servicelevering. Forretningsunderstøttende divisioner som People and Culture, Compliance & Security og Intern IT sikrer, at de grundlæggende politikker, procedurer og rammeværker er på plads.

Gennem denne struktur sikrer Compliance & Security-afdelingen, at itm8 opretholder en sammenhængende tilgang til risikostyring og lovgivningsmæssig overholdelse af cybersikkerhed. Samtidig leverer afdelingen løbende vejledning og overvågning for at opfylde organisationens og kundernes krav. Medarbejdere på tværs af alle divisioner har ansvar for at overholde politikkerne og bidrage proaktivt til et sikkert miljø.

Kontrolmål og relaterede kontrolaktiviteter er beskrevet nærmere i afsnit 4.

3.11. Komplementære kontroller hos kunderne

Kunder, der anvender itm8's tjenester som led i deres egen overholdelse af NIS2 eller tilsvarende krav, forventes at varetage følgende komplementære kontroller:

- Vurdere og afgøre, om kundens egen virksomhed er omfattet af NIS2 som væsentlig eller vigtig enhed, og dokumentere klassifikationen.
- Sikre, at egne risikostyringsforanstaltninger er etableret i overensstemmelse med NIS2-direktivets artikel 21, og at samspillet med itm8's leverancer er afspejlet heri.
- Definere og opretholde egne politikker, herunder informationssikkerheds-, hændelses- og forretningskontinuitetspolitikker, som omfatter de tjenester, itm8 leverer.
- Sikre, at kundens egne brugere regelmæssigt gennemgås og har de korrekte adgangsprofiler i de systemer, der leveres eller driftes af itm8.
- Foretage egne risikovurderinger af leverandører, herunder itm8, og opretholde et overblik over leverandørafhængigheder.
- Sikre, at kundens egne medarbejdere modtager passende cybersikkerhedstræning, herunder uddannelse af ledelsesorganet.
- Indberette egne væsentlige hændelser til kompetente myndigheder og CSIRT-funktioner i henhold til de gældende frister og koordinere med itm8, hvor itm8's leverancer er involveret.
- Løbende gennemgå de aftalte sikkerhedsforanstaltninger og konfigurationer for kundens miljø for at sikre, at de er tilstrækkelige i forhold til kundens egne forpligtelser under NIS2.

4. Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål 1 – Politikker for risikoanalyse og informationssystemsikkerhed

Der foreligger formaliserede politikker og procedurer for at sikre, at der er fastlagt tilstrækkelig vejledning, roller og ansvar for at understøtte en struktureret og formaliseret proces til at identificere risici og forankre informationssikkerhed i organisationen.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
1.1 (1.A)	Der er defineret og implementeret en formaliseret organisationsstruktur omkring roller og ansvar for at levere NIS2-tjenester i virksomheden.	Forespurgt om, hvordan roller og ansvarsområder er defineret. Inspiceret, at der foreligger en formaliseret procedure for roller og ansvar i henhold til levering af NIS2-tjenester. Observeret, at de faktiske roller og ansvar er i overensstemmelse med proceduren.	Ingen afvigelser noteret.
1.2 (1.A)	Virksomheden har udarbejdet og implementeret en politik for informationssikkerhed i net- og informationssystemer. Virksomhedens ledelse har godkendt politik, som er kommunikeret til alle relevante interessenter (interne/eksterne), herunder virksomhedens medarbejdere. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres blandt andet på baggrund af input fra myndigheder eller/og ændret risikobillede.	Forespurgt om, hvordan informationssikkerhedspolitikken godkendes og kommunikeres til relevante interessenter. Inspiceret, at virksomheden har udarbejdet og implementeret en politik for informationssikkerhed i net- og informationssystemer. Inspiceret, at informationssikkerhedspolitikken er ledelsesgodkendt og kommunikeret til relevante interessenter. Inspiceret, at der regelmæssigt og minimum årligt foretages vurderinger af, hvordan informationssikkerhedspolitikken skal opdateres.	Ingen afvigelser noteret.
1.3 (1.A)	Informationssikkerhedspolitikken fastsætter retningslinjer for indarbejdelse af informationssikkerhedskrav, som styres af interne såvel som eksterne mekanismer, såsom virksomhedsstrategi, GDPR og NIS2-regulering. Overholdelse af politikken sikres løbende via intern/ekstern gennemgang.	Inspiceret, at informationssikkerhedspolitikken beskriver informationssikkerhedskrav, der er påkrævet både fra interne krav såvel som eksterne reguleringer. Inspiceret, at overholdelse af politikken sikres løbende via intern/ekstern gennemgang.	Ingen afvigelser noteret.

Kontrolmål 1 – Politikker for risikoanalyse og informationssystemsikkerhed

Der foreligger formaliserede politikker og procedurer for at sikre, at der er fastlagt tilstrækkelig vejledning, roller og ansvar for at understøtte en struktureret og formaliseret proces til at identificere risici og forankre informationssikkerhed i organisationen.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
1.4 (1.B)	Der foretages en risikovurdering baseret på krav fra/til kunder/leverandører og under anvendelse af en branchemæssigt anerkendt standard/metode, hvor hver identificeret risiko vurderes ud fra et NIS2-perspektiv.	Forespurgt om processen for udarbejdelse af risikovurdering. Inspiceret, at processen for udarbejdelse af vurderinger er formaliseret og ledelsesgodkendt. Inspiceret, at risikovurderingen er udført ud fra et NIS2-perspektiv, følger krav fra/til kunder/leverandører og er baseret på industrielle standarder/tilgang.	Ingen afvigelser noteret.
1.5 (1.B)	Processen sikrer, at risikovurderingen omfatter følgende aktiviteter: • Identificering af risici: Find, registrér og beskriv risici • Risikoanalyse: Fastslå årsagen/kilden til risikoen samt sandsynligheden for, konsekvensen og alvoren af risici.	Inspiceret, at risikovurderingen omfatter følgende aktiviteter: • Identificering af risici: Find, registrér og beskriv risici • Risikoanalyse: Fastslå årsagen/kilden til risikoen samt sandsynligheden for, konsekvensen og alvoren af risici.	Ingen afvigelser noteret.
1.6 (1.B)	Der udarbejdes konsekvensanalyser under hensyntagen til omfanget af skade, der er forvoldt organisationen og/eller den kritiske infrastruktur i samfundet ud fra perspektivet om tab af informationers/tjenesters tilgængelighed.	Forespurgt om processen for udarbejdelse af konsekvensanalyser. Inspiceret, at konsekvensanalyser er udarbejdet under hensyntagen til omfanget af skade, der er forvoldt organisationen og/eller den kritiske infrastruktur i samfundet ud fra perspektivet om tab af informationers/tjenesters tilgængelighed.	Samfundsmæssige konsekvenser er ikke fuldt indarbejdet i den aktuelle risikovurdering. Itm8 oplyser at de har tilpasset deres risikovurderingsprocedure, så den fremadrettet tager hensyn til samfundsmæssige konsekvenser, men at risikoanalysen ikke er opdateret siden denne tilpasning Ingen yderligere afvigelser noteret.

Kontrolmål 1 – Politikker for risikoanalyse og informationssystemsikkerhed

Der foreligger formaliserede politikker og procedurer for at sikre, at der er fastlagt tilstrækkelig vejledning, roller og ansvar for at understøtte en struktureret og formaliseret proces til at identificere risici og forankre informationssikkerhed i organisationen.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
1.7 (1.B)	Virksomheden opdaterer risikovurderingen og behandlingen af risici løbende og mindst én gang om året samt i tilfælde af ændringer.	Forespurgt om den formaliserede proces for løbende vurdering og opdatering af risikovurderinger. Inspiceret, at risikovurderinger er vurderet og om nødvendigt opdateret årligt. Inspiceret, at risikovurderinger er opdateret og ledelsesgodkendt årligt.	Ingen afvigelser noteret.
1.8 (1.B)	Ledelsen (bestyrelse/risikoudvalg mv.) overvåger løbende (fx månedligt/kvartalsvist) de identificerede risici, fremdriften i mitigerende handlinger samt det generelle trusselsbillede.	Forespurgt om, hvordan ledelsen overvåger de identificerede risici. Inspiceret, at ledelsen løbende overvåger de identificerede risici, fremdriften i mitigerende handlinger og det generelle trusselsbillede.	Ingen afvigelser noteret.

Kontrolmål 2 – Håndtering af hændelser (forebyggelse, opdagelse og opfølgning på hændelser)

Der foreligger formaliserede procedurer og kontroller for at sikre rettidig og behørig håndtering, herunder opdagelse, løsning af og rapportering af hændelser til kunder.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
2.1 (2.A)	Ledelsens ansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planlagt håndtering af informationssikkerhedshændelser vedrørende NIS2-tjenester. Proceduren omfatter specifik prioritering og tidsramme for håndtering af informationssikkerhedshændelser og kommunikationskanaler.	Inspiceret, at ledelsens ansvar for håndtering af hændelser er defineret. Inspiceret, at en formaliseret procedure er udarbejdet og implementeret for at sikre hurtig, effektiv og planlagt håndtering af informationssikkerhedshændelser vedrørende NIS2-tjenester. Inspiceret, at den formelle procedure indeholder information om: • Prioritering • Tidsramme for håndtering af sikkerhedshændelser • Kommunikationskanaler. Inspiceret, at proceduren er ledelsesgodkendt årligt eller ved ændringer i processen.	Ingen afvigelser noteret.
2.2 (2.A)	Der er udarbejdet en plan og en ramme for håndtering af større informationssikkerhedshændelser, som skal løses inden for en bestemt tidsfrist.	Inspiceret, at der foreligger en plan for at sikre behørig og rettidig håndtering af væsentlige informationssikkerhedshændelser.	Ingen afvigelser noteret.
2.3 (2.A)	Der anvendes et ITSM-værktøj til effektiv håndtering af dokumentation og rapportering af hændelser.	Forespurgt til processen for registrering og rapportering af informationssikkerhedshændelser. Inspiceret, at der er implementeret og anvendt et ITSM-værktøj eller tilsvarende til håndtering, dokumentering og rapportering af informationssikkerhedshændelser.	Ingen afvigelser noteret.
2.4 (2.A)	Der foreligger en ledelsesovervågningskontrol for at sikre, at hændelser løses inden for en foruddefineret tidsfrist og i overensstemmelse med ledelsens forventninger.	Forespurgt til ledelsens overvågning af informationssikkerhedshændelser. Inspiceret ved en stikprøve på informationssikkerhedshændelser, at disse er løst inden for den fastsatte tidsfrist og i overensstemmelse med ledelsens forventninger.	Ingen afvigelser noteret.

Kontrolmål 2 – Håndtering af hændelser (forebyggelse, opdagelse og opfølgning på hændelser)

Der foreligger formaliserede procedurer og kontroller for at sikre rettidig og behørig håndtering, herunder opdagelse, løsning af og rapportering af hændelser til kunder.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
2.5 (2.A, 5.B)	I tilfælde af at der indtræffer hændelser, som måtte påvirke overholdelsen af NIS2-krav, informerer virksomheden kunderne uden ugrundet ophold og ikke senere end den aftalte tidsfrist efter at være blevet opmærksom på hændelsen.	Forespurgt til proceduren for kommunikation til kunder om informationssikkerhedshændelser, der påvirker overholdelsen af NIS2-krav. Inspiceret ved en stikprøve på informationssikkerhedshændelser, at disse er blevet kommunikeret til kunderne uden ugrundet ophold og inden for den fastsatte tidsfrist.	Ingen afvigelser noteret.
2.6 (2.A)	Virksomheden udfører løbende og mindst én gang årligt tests af processen for rapportering af informationssikkerhedshændelser.	Forespurgt til proceduren for regelmæssig rapportering af informationssikkerhedshændelser. Inspiceret, at processen for rapportering af informationssikkerhedshændelser er testet mindst årligt.	Ingen afvigelser noteret.
2.7 (2.B)	Virksomheden har etableret og vedligeholder en procedure og baselines for auditlogge.	Forespurgt om logmanagementprocessen. Inspiceret, at der foreligger en formaliseret procedure, der beskriver baseline i relation til konfigurering, opsamling, beskyttelse og overvågning af logge.	Ingen afvigelser noteret.

Kontrolmål 2 – Håndtering af hændelser (forebyggelse, opdagelse og opfølgning på hændelser)

Der foreligger formaliserede procedurer og kontroller for at sikre rettidig og behørig håndtering, herunder opdagelse, løsning af og rapportering af hændelser til kunder.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
2.8 (2.B)	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende fx ændringer i logopsætninger, herunder deaktivering af logning, ændringer i systemrettigheder til brugere og fejlede forsøg på log-on til systemer, databaser og netværk.	Forespurgt om logmanagementprocessen. Inspiceret, at der foreligger en formaliseret procedure, der beskriver baseline i relation til konfigurering, opsamling, beskyttelse og overvågning af logge. Inspiceret ved en stikprøve, at følgende forhold bliver logget og overvåget i relation til systemer, databaser og netværk: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende fx ændringer i logopsætninger, herunder deaktivering af logning, ændringer i systemrettigheder til brugere og fejlede forsøg på log-on til systemer, databaser og netværk.	Ingen afvigelser noteret.
2.9 (2.B)	Logge er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Forespurgt om logmanagementprocessen. Inspiceret, at der foreligger en formaliseret procedure, der beskriver baseline i relation til konfigurering, opsamling, beskyttelse og overvågning af logge. Inspiceret ved en stikprøve på systemer og databaser, at logdata er beskyttet mod manipulation og videresendes til sys-logserver. Inspiceret, at tekniske fejl bliver gennemgået løbende.	Ingen afvigelser noteret.

Kontrolmål 2 – Håndtering af hændelser (forebyggelse, opdagelse og opfølgning på hændelser)

Der foreligger formaliserede procedurer og kontroller for at sikre rettidig og behørig håndtering, herunder opdagelse, løsning af og rapportering af hændelser til kunder.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
2.10 (2.B)	Der er etableret systemovervågning for systemer og databaser med en alarmfunktion, som udløses af relevante hændelser.	Forespurgt om logmanagementprocessen vedrørende hændelser. Inspiceret, at der foreligger en formaliseret procedure, der beskriver baseline i relation til konfigurering, opsamling, beskyttelse, alarmering og overvågning af logge. Inspiceret ved en stikprøve på systemer og databaser, at overvågning med en alarmfunktion, som udløses af relevante hændelser, er etableret for systemer og databaser.	Ingen afvigelser noteret.

Kontrolmål 3 – Driftskontinuitet, såsom backupstyring, reetablering efter en katastrofe og krisestyring

Der foreligger formaliserede procedurer og kontroller for at sikre fortsat drift og tilgængelighed af tjenester i tilfælde af en katastrofe.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
3.1 (3.A)	Virksomheden har implementeret en formelt godkendt og dokumenteret driftskontinuitetsplan, som omfatter udformning af en modstandsdygtig teknisk infrastruktur, etablering af krisehåndteringsressourcer samt koordinering og vedligeholdelse af driftskontinuitetsplaner og -foranstaltninger.	Inspiceret, at der er etableret en formel og ledelsesgodkendt driftskontinuitetsplan, samt at den omfatter udformning af en modstandsdygtig teknisk infrastruktur, etablering af krisehåndteringsressourcer samt koordinering og vedligeholdelse af driftskontinuitetsplaner. Inspiceret, at teknisk infrastruktur samt krisehåndteringsressourcer bliver testet mindst én gang årligt.	Ingen afvigelser noteret.
3.2 (3.A)	Der udarbejdes og dokumenteres en driftskontinuitetsplan til at understøtte NIS2-relaterede tjenester. Planen beskriver procedurerne for at reagere på, reetablere, genoptage og genoprette driften af de relaterede tjenester til et foruddefineret niveau for de relevante tjenester. Driftskontinuitetsplanen testes minimum én gang årligt.	Inspiceret, at driftskontinuitetsplanen indeholder procedurer for at reagere på, reetablere, genoptage og genoprette driften af de relaterede tjenester til et foruddefineret niveau for de relevante NIS2-tjenester. Inspiceret, at driftskontinuitetsplanen testes mindst én gang årligt.	Ingen afvigelser noteret.
3.3 (3.A)	Virksomheden har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.	Inspiceret it-katastrofeplanen og driftskontinuitetsplanen. Inspiceret, at planerne indeholder krav til informationssikkerhed i tilfælde af en krise.	Ingen afvigelser noteret.

Kontrolmål 3 – Driftskontinuitet, såsom backupstyring, reetablering efter en katastrofe og krisestyring

Der foreligger formaliserede procedurer og kontroller for at sikre fortsat drift og tilgængelighed af tjenester i tilfælde af en katastrofe.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
3.4 (3.B)	Der er etableret en ledelsesgodkendt backupprocedure. Proceduren indeholder hyppighed af backup, lokation og overvågningskontroller til at håndtere fejl i planlagte backups.	Inspiceret, at der foreligger en formaliseret backupprocedure. Inspiceret, at backupproceduren indeholder information om hyppighed af backup, lokation for backup samt overvågning af fejlede backupjobs. Inspiceret, at backupproceduren er godkendt af ledelsen. Inspiceret ved en stikprøve, at der er foretaget backup. Inspiceret ved en stikprøve på fejlede backupjobs, at der er fulgt op herpå, og at fejlen er løst.	Ingen afvigelser noteret.
3.5 (3.B)	Backup af informationer, der vedrører relevante systemer og data, vedligeholdes og testes regelmæssigt og i overensstemmelse med proceduren.	Inspiceret, at der foreligger en formaliseret procedure for regelmæssige genetableringstests. Inspiceret ved en stikprøve på genetableringstests, at testen er blevet gennemført succesfuldt. Inspiceret, at i tilfælde af fejl identificeret ved genetableringstests er fejlen undersøgt og løst, samt at backupproceduren er tilpasset, hvis nødvendigt.	Ingen afvigelser noteret.
3.6 (3.B)	Backupdata opbevares på en anden lokation end driftsmiljøerne. Adgang og den logiske forbindelse mellem backup og driftsmiljøerne er begrænset.	Inspiceret, at backup opbevares på en lokation, der er fysisk adskilt fra driftsmiljøerne. Inspiceret, at der er etableret funktionsadskillelse mellem backup- og produktionsdata. Inspiceret, at den logiske forbindelse mellem backup- og driftsmiljøerne er begrænset til prædefinerede tidsvinduer.	Ingen afvigelser noteret.

Kontrolmål 3 – Driftskontinuitet, såsom backupstyring, reetablering efter en katastrofe og krisestyring

Der foreligger formaliserede procedurer og kontroller for at sikre fortsat drift og tilgængelighed af tjenester i tilfælde af en katastrofe.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
3.7 (3.C)	Virksomheden har identificeret krav til tilgængeligheden af NIS2-relaterede tjenester og informationssystemer gennem design og implementering af systemarkitektur med passende redundans for at opfylde disse krav.	Forespurgt til kravene til tilgængelighed af NIS2-relaterede tjenester. Inspiceret, at informationssystemer er designet med passende kontroller i relation til redundans for at opfylde krav til tilgængelighed af NIS2-tjenester.	Ingen afvigelser noteret.
3.8 (3.C)	Virksomheden har implementeret kontroller til at sikre tilstrækkelig redundans for at opfylde krav om tilgængelighed, herunder tilgængeligheden af en alternativ facilitet (dvs. et sted for genetablering efter katastrofe), som ikke er udsat for de samme trusler som den primære facilitet, hvor det måtte være relevant.	Forespurgt til tilgængeligheden af en alternativ facilitet til at fortsætte driften i tilfælde af større uheld eller katastrofer, hvor den primære facilitet ikke er tilgængelige. Inspiceret, at der er indgået aftale om en alternativ facilitet med henblik på at kunne fortsætte driften i tilfælde af krise.	Ingen afvigelser noteret.
3.9 (3.D)	En krisestyringsplan baseret på en risikovurdering er implementeret og godkendt af ledelsen. Planen vedligeholdes og omfatter procedurer til at opretholde cybersikkerhed under kriser, definerer roller og ansvarsområder (inkl. relevante leverandører) samt kommunikationskanaler og tidslinjer til myndigheder/CSIRT.	Inspiceret, at der er implementeret en ledelsesgodkendt plan, som omfatter procedurer til at opretholde cybersikkerhed under kriser, definerer roller og ansvarsområder (inkl. relevante leverandører) samt kommunikationskanaler og tidslinjer til myndigheder/CSIRT.	Ingen afvigelser noteret.
3.10 (3.D)	Krisestyringsplanen bliver afprøvet og opdateret løbende (mindst årligt) og/eller ved større ændringer. Resultatet af testen bliver dokumenteret. Relevante forbedringstiltag bliver registeret og efterfølgende implementeret.	Inspiceret, at krisestyringsplanen bliver afprøvet og opdateret løbende (mindst årligt) og/eller ved større ændringer. Inspiceret, at resultat af testen bliver dokumenteret, samt at relevante forbedringstiltag bliver registeret og efterfølgende implementeret.	Ingen afvigelser noteret.

Kontrolmål 3 – Driftskontinuitet, såsom backupstyring, reetablering efter en katastrofe og krisestyring

Der foreligger formaliserede procedurer og kontroller for at sikre fortsat drift og tilgængelighed af tjenester i tilfælde af en katastrofe.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
3.11 (3.D)	Virksomheden har implementeret en proces til at håndtere og anvende informationer om eksempelvis sikkerhedshændelser, sårbarheder, trusler og foranstaltninger, der modtages fra den nationale CSIRT, eller, hvor relevant, den sektoransvarlige myndighed.	Inspiceret, at virksomheden har implementeret en proces til at håndtere og anvende informationer om eksempelvis sikkerhedshændelser, sårbarheder, trusler og foranstaltninger, der modtages fra den nationale CSIRT, eller, hvor relevant, den sektoransvarlige myndighed.	Ingen afvigelser noteret.

Kontrolmål 4 – Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem virksomheden og dens direkte leverandører eller tjenesteudbydere

Der foreligger formaliserede procedurer og kontroller for at sikre, at relevante og direkte tjenesteudbydere (herunder underleverandører) igennem hele leverandørkæden identificeres og overvåges for at sikre overholdelse af virksomhedens sikkerhedskrav og serviceleveranceaftaler.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
4.1 (4)	Virksomheden har implementeret formaliserede procedurer og processer for at sikre, at den informationssikkerhedsrisiko, der er forbundet med de væsentlige eksterne NIS2-relaterede leverandører (som fx strøm, teknisk bistand, cloud-leverandører, OT, outsourcet udvikling m.m.), er dokumenteret.	Forespurgt om processen for løbende vurdering af informationssikkerhedsrisici i relation til eksterne NIS2-relaterede leverandører. Inspiceret, at en formaliseret procedure er designet og implementeret for at sikre periodisk vurdering af informationssikkerhedsrisici i relation til væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at proceduren godkendes af ledelsen en gang årligt eller ved ændringer i processen. Inspiceret, at informationssikkerhedsrisici i relation til eksterne NIS2-relaterede leverandører evalueres og opdateres minimum en gang årligt.	Ingen afvigelser noteret.
4.2 (4)	Virksomheden har implementeret en proces for at sikre, at væsentlige eksterne NIS2-relaterede leverandører overholder virksomhedens sikkerhedskrav og -foranstaltninger.	Forespurgt om processen for identifikation og overvågning af væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at en formaliseret procedure er udarbejdet og implementeret for at sikre, at virksomhedens sikkerhedskrav er kommunikeret til væsentlige eksterne NIS2-relaterede leverandører.	Ingen afvigelser noteret.
4.3 (4)	Virksomheden overvåger løbende væsentlige eksterne NIS2-relaterede leverandører for at sikre overholdelse af sikkerhedsforanstaltninger, håndtering af hændelser, væsentlige ændringer mv.	Forespurgt om processen for identifikation og overvågning af væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, ved en stikprøve, at virksomheden har udført overvågning af væsentlige eksterne NIS2-relaterede leverandører for at sikre efterlevelse af sikkerhedskrav.	Ingen afvigelser noteret.

Kontrolmål 4 – Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem virksomheden og dens direkte leverandører eller tjenesteudbydere

Der foreligger formaliserede procedurer og kontroller for at sikre, at relevante og direkte tjenesteudbydere (herunder underleverandører) igennem hele leverandørkæden identificeres og overvåges for at sikre overholdelse af virksomhedens sikkerhedskrav og serviceleveranceaftaler.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
4.4 (4)	Kontrakter med væsentlige eksterne NIS2-relaterede leverandører indeholder passende sikkerhedskrav, der er baseret på risici, som er identificeret i forbindelse med risikovurderingen af serviceleverandøren.	Forespurgt, om processen for risikovurdering af væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at den anvendte ramme for risikovurdering indeholder krav om vurdering i forhold til relevante sikkerhedskrav. Inspiceret ved en stikprøve, at sikkerhedskrav afledt af risikovurderingen er indarbejdet i kontrakten med væsentlige eksterne NIS2-relaterede leverandører.	Ingen afvigelser noteret.
4.5 (4)	Afhjælpende handlinger til at håndtere identificerede risici relateret til væsentlige eksterne NIS2-relaterede leverandører planlægges og implementeres rettidigt.	Forespurgt om processen for begrænsning af risici relateret til af væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at risikobegrænsende aktiviteter er planlagte og implementerede for væsentlige eksterne NIS2-relaterede leverandører.	Ingen afvigelser noteret.
4.6 (4)	Relevante erklæringer fra væsentlige eksterne NIS2-relaterede leverandører er underlagt årlig gennemgang. Såfremt der identificeres betydelige svagheder, gennemføres der passende undersøgende handlinger, og der implementeres risikobegrænsende handlinger vedrørende svaghederne.	Forespurgt om processen for identifikation og overvågning af væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at der foreligger en formaliseret procedure for at sikre, at relevante revisionserklæringer for væsentlige eksterne NIS2-relaterede leverandører bliver indhentet og inspiceret. Inspiceret ved en stikprøve, at relevante revisionserklæringer er indhentet og gennemgået for væsentlige eksterne NIS2-relaterede leverandører. Inspiceret, at der er foretaget en vurdering af identificerede svagheder for at sikre, at risikobegrænsende handlinger bliver planlagt og udført.	Ingen afvigelser noteret.

Kontrolmål 5 – Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

Der foreligger formaliserede procedurer og kontroller for at sikre, at kritiske aktiver på behørig vis udvikles, vedligeholdes og beskyttes mod sårbarheder over for interne og eksterne trusler.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.1 (5.A)	Netværksinfrastruktur og tilhørende dokumentation vedligeholdes og er opdateret, herunder netværksdiagrammer og konfigureringsfiler til enheder (fx routere og switches).	Inspiceret, at der foreligger formaliseret dokumentation i form af netværksdiagram samt overblik over andet relevant netværksudstyr som fx routere og switches. Inspiceret, at dokumentationen i relation til netværksdiagram og konfigurering er opdateret.	Ingen afvigelser noteret.
5.2 (5.A)	Netværksenheder er konfigureret/hærdet i henhold til anerkendte branchestandarder for styrkelse af konfigureringsskabeloner.	Inspiceret, at der foreligger en baseline for hærdning af netværksenheder baseret på en anerkendt standard (fx CIS18). Inspiceret ved en stikprøve på netværksenheder, at disse er konfigureret i overensstemmelse med baseline.	Ingen afvigelser noteret.
5.3 (5.A)	Interne netværk er segmenteret for at begrænse adgang til systemer og databaser.	Forespurgt om praksis og processer vedrørende segmentering af netværket. Inspiceret netværksdiagram, der viser, at det interne netværk er segmenteret. Inspiceret konfigurationsfiler og regelsæt i netværksenheder, som skal sikre en effektiv netværkssegmentering.	Ingen afvigelser noteret.
5.4 (5.A)	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Forespurgt om ændringshåndteringsprocessen i relation til systemer, databaser eller netværk. Inspiceret, at der foreligger en formaliseret procedure, der beskriver processen for håndtering af ændringer og patches. Inspiceret ved en stikprøve på ændringer, at implementerede ændringer og patches er styret og dokumenteret i henhold til den formaliserede procedure.	Ingen afvigelser noteret.

Kontrolmål 5 – Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

Der foreligger formaliserede procedurer og kontroller for at sikre, at kritiske aktiver på behørig vis udvikles, vedligeholdes og beskyttes mod sårbarheder over for interne og eksterne trusler.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.5 (5.A)	Virksomheden har implementeret en ledelsesgodkendt procedure til sikring af cybersikkerhed på følgende områder: • Ved anskaffelse af it-produkter eller tjenester fra tredjepart • Ved udvikling og vedligeholdelse af net- og informationssystemer • Ved afvikling/bortskaffelse af net- og informationssystemer. Proceduren tager udgangspunkt i virksomhedens politik for informationssikkerhed samt politik for risikostyring og leverandørstyring.	Inspiceret, at virksomheden har implementeret en ledelsesgodkendt procedure til sikring af cybersikkerhed på følgende områder: • Ved anskaffelse af it-produkter eller tjenester fra tredjepart • Ved udvikling og vedligeholdelse af net- og informationssystemer • Ved afvikling/bortskaffelse af net- og informationssystemer. Inspiceret, at proceduren tager udgangspunkt i virksomhedens politik for informationssikkerhed samt politik for risikostyring og leverandørstyring.	Ingen afvigelser noteret.
5.6 (5.A)	Livscyklusstyring gennemgås løbende og opdateres i forbindelse med periodiske eller væsentlige ændringer.	Inspiceret, at livscyklusstyring gennemgås løbende og opdateres i forbindelse med periodiske eller væsentlige ændringer.	Ingen afvigelser noteret.
5.7 (5.B)	Der foreligger formaliserede procedurer, og der er regelmæssige vurderinger af robustheden af de systemer og processer, som virksomheden bruger ved levering af NIS2-tjenester.	Inspiceret, at der foreligger en formaliseret procedure for løbende vurdering af robustheden af virksomhedens systemer og processer i relation til NIS2-tjenester. Inspiceret, at proceduren løbende opdateres og godkendes af ledelsen.	Ingen afvigelser noteret.
5.8 (5.B)	Virksomheden har implementeret en proces for styring af tekniske sårbarheder og vedligeholder kompetencer/mekanismer, der kan identificere eksisterende sårbarheder i forhold til NIS2-tjenester.	Forespurgt om processen for vurdering af sårbarheder. Inspiceret, at der foreligger en formaliseret procedure, og at relevante kompetencer/mekanismer anvendes for at sikre, at sårbarheder vurderes og håndteres løbende.	Ingen afvigelser noteret.

Kontrolmål 5 – Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

Der foreligger formaliserede procedurer og kontroller for at sikre, at kritiske aktiver på behørig vis udvikles, vedligeholdes og beskyttes mod sårbarheder over for interne og eksterne trusler.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.9 (5.B)	Der foretages løbende sårbarhedsscanninger af aktiver, der anvendes til NIS2-tjenester.	Forespurgt om processen for håndtering af sårbarheder. Inspiceret, at der foretages løbende sårbarhedsscanninger af aktiver, der anvendes til NIS2-tjenester, og at identificerede sårbarheder identificeres, risikovurderes, prioriteres og løses rettidigt.	Ingen afvigelser noteret.

Kontrolmål 6 – Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberrelaterede risici og trusler identificeres, overvåges og udbedres rettidigt.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.1 (6.A)	En ledelsesgodkendt procedure er implementeret for at sikre, at de implementerede sikkerhedsforanstaltninger fortsat er tilstrækkelige i forhold til relevante risici og interne krav. Proceduren skal vurdere, om informationssikkerhedspolitikken er i overensstemmelse med interne krav, gældende lovgivning og relevante gennemførelsesretsakter (fx EU 2024/2690).	Inspiceret, at der foreligger en ledelsesgodkendt procedure, der sikrer, at de implementerede sikkerhedsforanstaltninger fortsat er tilstrækkelige i forhold til relevante risici, interne krav, gældende lovgivning og relevante gennemførelsesretsakter.	Under vores revision har vi konstateret, at ledelsesgodkendelse af styrende dokumenter ikke i alle tilfælde er tilstrækkeligt dokumenteret. Itm8 har ændret relevant procedure for fremadrettet at styrke dokumentationen heraf. Ingen yderligere afvigelser noteret.
6.2 (6.A)	Proceduren definerer roller, metoder og værktøjer til at udføre vurderinger, herunder risikobaserede tekniske tests (fx scanninger og penetrationstests). Proceduren indeholder krav til vurdering af overholdelse af juridiske/regulatoriske krav, efterlevelse af politikker samt foranstaltningernes effektivitet og vedligeholdelse for de enkelte beskyttede aktiver; de omfatter også bevaring af dokumentation og en proces til afhjælpning af ineffektive foranstaltninger (ejere, frister og opfølgning).	Inspiceret, at proceduren definerer roller, metoder og værktøjer til at udføre vurderinger, herunder risikobaserede tekniske tests (fx scanninger og penetrationstests). Inspiceret, at proceduren indeholder krav til vurdering af overholdelse af juridiske/regulatoriske krav, efterlevelse af politikker samt foranstaltningernes effektivitet og vedligeholdelse for de enkelte beskyttede aktiver, herunder bevaring af dokumentation og en proces for opfølgning på manglende eller ineffektive foranstaltninger.	Ingen afvigelser noteret.
6.3 (6.A)	Proceduren er koblet til virksomhedens informationssikkerhedspolitik, risikovurdering og hændelseshåndtering. Proceduren bliver løbende gennemgået og opdateret ved større ændringer i forretningen og trusselsbilledet.	Inspiceret, at proceduren er udarbejdet med udgangspunkt i virksomhedens informationssikkerhedspolitik, risikovurdering og hændelseshåndtering. Inspiceret, at proceduren er gennemgået og opdateret ved større ændringer i forretningen og trusselsbilledet.	Ingen afvigelser noteret.

Kontrolmål 6 – Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberrelaterede risici og trusler identificeres, overvåges og udbedres rettidigt.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.4 (6.B)	Der udføres periodiske tests ud af væsentlig infrastruktur og væsentlige applikationer ud fra en risikobaseret tilgang til testtyper (sårbarhedsscanninger, penetrationstests, rødt/blåt hold-aktiviteter, konfigurationsgennemgange, kodegennemgange, social engineering-tests, tests af adgangskontroller), hyppighed, omfang og udløsende faktorer (installationer, vedligeholdelse, opgraderinger mm). Testen dokumenteres, og uregelmæssigheder risikoklassificeres, afhjælpes og gentestes, inden de kan lukkes.	Inspiceret, at der er foretaget dokumenterede periodiske tests af væsentlig infrastruktur og væsentlige applikationer i form af fx sårbarhedsscanninger, penetrationstests, rødt/blåt hold-aktiviteter, konfigurationsgennemgange, kodegennemgange, social engineering-tests og tests af adgangskontroller. Inspiceret, at uregelmæssigheder vurderes, klassificeres og afhjælpes.	Ingen afvigelser noteret.

Kontrolmål 7 – Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberhygiejnepraksisser er implementeret i virksomheden, og at medarbejderne gennemfører løbende træning/uddannelse i cybersikkerhed.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.1 (7.A)	Der er implementeret cyberhygiejnepolitikker og -procedurer, som omfatter, men ikke er begrænset til, følgende: • at etablere et minimumssæt af baseline-sikkerhedspolitikker (se "1. Risikoanalyse og sikkerhedspolitik for informationssystemer") • at tage regelmæssige sikkerhedskopier af relevante data, teste de sikkerhedskopierede data (integritetskontroller) og teste procedurer for gendannelse fra backup (se "3. Backup") • at planlægge kapacitet og ressourcer (personale og it) for at undgå potentielle kapacitetsflaskehalse (se "3. Redundans") • at udarbejde en krisestyringsplan for hændelser (se "3. Krisestyring") • at evaluere cybersikkerheden i virksomhedens it-forsyningskæde regelmæssigt (se "4. Forsyningskædesikkerhed") • at etablere risikobaserede serviceaftaler (SLA'er) med leverandører og tjenesteudbydere (se "4. Forsyningskædesikkerhed") • at installere regelmæssigt patches og opdateringer til operativsystemer og applikationer (se "5. Indkøb, udvikling og vedligeholdelse") • at installere og automatisk opdatere anti-malware-software på alle relevante aktiver	Forespurgt om processen for overvågning af cyberhygiejneprogrammet. Inspiceret, at ledelsen har implementeret overvågningskontroller for at sikre efterlevelse af cyberhygiejne, som omfatter, men ikke er begrænset til, følgende: • at etablere et minimumssæt af baseline-sikkerhedspolitikker (se "1. Risikoanalyse og sikkerhedspolitik for informationssystemer") • at tage regelmæssige sikkerhedskopier af relevante data, teste de sikkerhedskopierede data (integritetskontroller) og teste procedurer for gendannelse fra backup (se "3. Backup") • at planlægge kapacitet og ressourcer (personale og it) for at undgå potentielle kapacitetsflaskehalse (se "3. Redundans") • at udarbejde en krisestyringsplan for hændelser (se "3. Krisestyring") • at evaluere cybersikkerheden i virksomhedens it-forsyningskæde regelmæssigt (se "4. Forsyningskædesikkerhed") • at etablere risikobaserede serviceaftaler (SLA'er) med leverandører og tjenesteudbydere (se "4. Forsyningskædesikkerhed") • at installere regelmæssigt patches og opdateringer til operativsystemer og applikationer (se "5. Indkøb, udvikling og vedligeholdelse")	Ingen afvigelser noteret.

Kontrolmål 7 – Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberhygiejnepraksisser er implementeret i virksomheden, og at medarbejderne gennemfører løbende træning/uddannelse i cybersikkerhed.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
	(se "5. Indkøb, udvikling og vedligeholdelse") • at segmentere enhedens netværk efter aktivernes kritikalitet (se "5. Indkøb, udvikling og vedligeholdelse") • at udføre regelmæssige, automatiserede sårbarhedsscanninger på tværs af virksomhedens net- og informationssystemer (se "6. Tekniske test") • at udføre regelmæssig sikkerhedstest (se "6. Tekniske test") • at opbygge en cybersikkerhedskultur og -bevidsthed gennem regelmæssig brugertræning (se "7. Cybersikkerhedstræning") • at kryptere data i hvile og under transport i overensstemmelse med aktivklassifikationsniveauer (se "8. Kryptografi") • at begrænse administrative privilegier (se "9. Adgangskontrol") • at håndhæve stærke adgangskoder (se "9. Adgangskontrol") • at anvende multifaktorgodkendelse (MFA) i overensstemmelse med aktivklassifikationsniveauer (se "9. Adgangskontrol") • at begrænse netværksporte og -tjenester til det strengt nødvendige ift. virksomhedens forretningsmæssige behov (se "9. Adgangskontrol")	• at installere og automatisk opdatere anti-malware-software på alle relevante aktiver (se "5. Indkøb, udvikling og vedligeholdelse") • at segmentere enhedens netværk efter aktivernes kritikalitet (se "5. Indkøb, udvikling og vedligeholdelse") • at udføre regelmæssige, automatiserede sårbarhedsscanninger på tværs af virksomhedens net- og informationssystemer (se "6. Tekniske test") • at udføre regelmæssig sikkerhedstest (se "6. Tekniske test") • at opbygge en cybersikkerhedskultur og -bevidsthed gennem regelmæssig brugertræning (se "7. Cybersikkerhedstræning") • at kryptere data i hvile og under transport i overensstemmelse med aktivklassifikationsniveauer (se "8. Kryptografi") • at begrænse administrative privilegier (se "9. Adgangskontrol") • at håndhæve stærke adgangskoder (se "9. Adgangskontrol") • at anvende multifaktorgodkendelse (MFA) i overensstemmelse med aktivklassifikationsniveauer (se "9. Adgangskontrol") • at begrænse netværksporte og -tjenester til det strengt nødvendige ift. virksomhedens forretningsmæssige behov (se "9. Adgangskontrol")	

Kontrolmål 7 – Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberhygiejnepraksisser er implementeret i virksomheden, og at medarbejderne gennemfører løbende træning/uddannelse i cybersikkerhed.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
	• at vedligeholde en fortegnelse over hardware- og softwareaktiver (se "9. Aktivstyring").	• at vedligeholde en fortegnelse over hardware- og softwareaktiver (se "9. Aktivstyring").	
7.2 (7.B)	Der foreligger formaliserede procedure for træning og uddannelse i bevidsthed om cybersikkerhed, som omfatter, men ikke er begrænset til, følgende: • Roller og enheder, der er omfattet af sikkerhedskurser • Uddannelse af medlemmer af ledelsesorganerne • Videndeling mellem ledelsesmedlemmer og vigtige enheder i virksomhedens organisation.	Inspiceret, om der foreligger en formaliseret procedure for træning og uddannelse i bevidsthed om cybersikkerhed, som inkluderer, men ikke er begrænset til følgende: • Roller og enheder, der er omfattet af sikkerhedskurser • Uddannelse af medlemmer af ledelsesorganerne • Videndeling mellem ledelsesmedlemmer og vigtige enheder i virksomhedens organisation. Inspiceret, at procedurerne godkendes af ledelsen en gang årligt eller i tilfælde af ændringer.	Ingen afvigelser noteret.
7.3 (7.B)	Virksomhedens ledelse modtager løbende uddannelse i bevidsthed om cybersikkerhed, der vedrører risici, som er identificeret i forhold til NIS2, og kontrolrammen.	Forespurgt om processen for træning i bevidsthed af virksomhedens ledelse. Inspiceret, at træning i bevidsthed har været afholdt for virksomhedens ledelse i forhold til risici, som er identificeret i forhold til NIS2, og kontrolrammen.	Ingen afvigelser noteret.
7.4 (7.B)	Virksomhedens medarbejdere modtager løbende træning i bevidsthed om cybersikkerhed, og generel bevidsthed om sikkerhed indgår i obligatoriske kurser.	Forespurgt om processen for træning i bevidsthed om cybersikkerhed af virksomhedens medarbejdere. Inspiceret, at medarbejdernes viden om cybersikkerhed bliver testet løbende. Inspiceret, at der sker opfølgning på manglende gennemførelse af træningen.	Ingen afvigelser noteret.

Kontrolmål 8 – Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

Der foreligger formaliserede procedurer og kontroller til at sikre, at kritiske aktiver beskyttes gennem kryptering.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.1 (8)	Der foreligger en procedure, som indeholder et krav om, at der gøres brug af effektiv kryptering i systemer og hardware, som indeholder eller transmitterer data relateret til NIS2-tjenester.	Forespurgt om processen for anvendelse af kryptering. Inspiceret, at en formaliseret procedure er designet og implementeret for at sikre anvendelse af kryptering i forhold til systemer og hardware eller overførsel af data relateret til NIS2-tjenester. Inspiceret, at proceduren godkendes af ledelsen en gang årligt eller ved ændringer i processen. Inspiceret ved en stikprøve på, at kryptering anvendes på systemer og hardware, der indeholder eller overfører data relateret til NIS2-tjenester.	Ingen afvigelser noteret.
8.2 (8)	Følsomme data, som bruges til at levere NIS2-tjenester, krypteres på slutbrugerenheder.	Forespurgt om processen for anvendelse af kryptering. Inspiceret overvågningsværktøjet (fx administrationskonsollen) for at validere, at kryptering af slutbrugerenhederne er aktiveret. Inspiceret, at afvigelser løbende identificeres og udbedres.	Ingen afvigelser noteret.
8.3 (8)	Der anvendes krypteringsløsninger til at sikre data, når dette er påkrævet, og de godkendes formelt og dokumenteres.	Forespurgt om processen for anvendelse af kryptering. Inspiceret, at den implementerede krypteringsløsning er formelt godkendt og dokumenteret. Inspiceret, at den godkendte krypteringsløsning er implementeret, når dette er påkrævet.	Ingen afvigelser noteret.
8.4 (8)	Stærke kryptografiske kontroller gør brug af ikke-kompromitterede versioner af sikkerhedsprotokoller.	Inspiceret, at der anvendes anerkendte kryptografiske algoritmer og protokoller, og at de er opdateret til nyeste version. Inspiceret, at de anvendte kryptografiske algoritmer ikke indeholder kendte svagheder.	Ingen afvigelser noteret.

Kontrolmål 8 – Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

Der foreligger formaliserede procedurer og kontroller til at sikre, at kritiske aktiver beskyttes gennem kryptering.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.5 (8)	Kryptografiske nøgler styres effektivt i overensstemmelse med dokumenterede standarder og procedurer, og de beskyttes mod uautoriseret adgang og destruktion.	Forespurgt om processen for håndtering af kryptografiske nøgler. Inspiceret, at de kryptografiske nøgler er beskyttet mod modificering, tab eller uautoriseret adgang/offentliggørelse. Inspiceret, at enheder, der bruges til at generere, opbevare eller arkivere nøgler, er fysisk beskyttet gennem brug af tilstrækkelige adgangskontroller.	Ingen afvigelser noteret.
8.6 (8)	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme data via internettet og med e-mail.	Forespurgt om processen for anvendelse af kryptering ved overførsel af fortrolige/følsomme data via internet eller e-mail. Inspiceret, at kryptering er anvendt i tilfælde af overførsel af fortrolige og følsomme data via internet og mail.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.1 (9.A)	Der er implementeret en ledelsesgodkendt procedure, der sikrer, at medarbejdere og – hvor relevant – leverandører/tjenesteudbydere er bekendt med og efterlever deres ansvar for sikkerheden i net- og informationssystemer, i overensstemmelse med enhedens informationssikkerhedspolitik. Proceduren gennemgås og opdateres med planlagte mellemrum.	Inspiceret, at der er udarbejdet en ledelsesgodkendt procedure, der sikrer, at medarbejdere og – hvor relevant – leverandører/tjenesteudbydere er bekendt med og efterlever deres ansvar for sikkerheden i net- og informationssystemer, i overensstemmelse med enhedens informationssikkerhedspolitik. Inspiceret, at proceduren gennemgås og opdateres med planlagte mellemrum.	Ingen afvigelser noteret.
9.2 (9.A)	Virksomheden har implementeret og kommunikeret ansættelsesregler (disciplinære regler), der gælder i tilfælde af overtrædelser af politikker og procedurer vedrørende sikkerheden i net- og informationssystemer.	Inspiceret, at virksomheden har implementeret og kommunikeret ansættelsesregler (disciplinære regler), der gælder i tilfælde af overtrædelser af politikker og procedurer vedrørende sikkerheden i net- og informationssystemer.	Ingen afvigelser noteret.
9.3 (9.A)	Der udføres en screening af virksomhedens medarbejdere som en del af ansættelsesprocessen. Screeningen omfatter i relevant omfang: • Referencer fra tidligere arbejdsgivere • Straffeattest • Eksamensbeviser.	Inspiceret den formaliserede procedure for screening af nye medarbejdere som en del af ansættelsesprocessen. Inspiceret ved en stikprøve på nye medarbejdere, at screeningen i relevant omfang har omfattet: • Referencer fra tidligere arbejdsgivere • Straffeattest • Eksamensbeviser.	Ingen afvigelser noteret.
9.4 (9.A)	Ved ansættelse underskriver medarbejderen en ansættelseskontrakt samt en fortrolighedsaftale, hvor forpligtelser i relation til sikkerhedsansvar er anført. Forpligtelsen vil fortsat gælde ved fratrædelse eller opsigelse.	Inspiceret den formelle procedure for indhentelse af fortrolighedsaftaler. Inspiceret ved en stikprøve på nye medarbejdere, at de har underskrevet en ansættelseskontrakt samt en fortrolighedsaftale, som også er gældende efter ved fratrædelse eller opsigelse.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.5 (9.B)	Der foreligger formaliserede procedurer for administration af adgange, herunder oprettelse, vedligeholdelse og fjernelse af adgangsrettigheder. Herudover indeholder proceduren krav om funktionsadskillelse på relevante områder.	Inspiceret, at der foreligger en formel procedure for adgangshåndtering, herunder tildeling, vedligeholdelse og fjernelse af adgangsrettigheder, samt funktionsadskillelse på relevante områder.	Ingen afvigelser noteret.
9.6 (9.B)	Der foreligger en formel procedure, der sikrer, at tildeling af adgangsrettigheder sker på baggrund af et arbejdsbetinget behov efter princippet om mindst mulig adgang.	Inspiceret, at der foreligger en formel procedure for tildeling af adgangsrettigheder, samt at de tildeles på baggrund af et arbejdsbetinget behov og efter princippet om mindst mulig adgang. Inspiceret ved en stikprøve på nye medarbejdere og tildelinger af nye adgangsrettigheder, at: • tildelingen af rettighederne er godkendt i henhold til proceduren • der er et arbejdsbetinget behov for adgangsrettighederne • rettighederne er tildelt efter princippet om mindst mulig adgang • de tildelte rettigheder er i overensstemmelse med de godkendte adgange.	Ingen afvigelser noteret.
9.7 (9.B)	Tildelingen af adgangskoder (hemmelig autentifikationsinformation) til brugere styres gennem en formel proces for administration af adgangskoder.	Inspiceret, at der foreligger en formaliseret adgangskodepolitik. Inspiceret, at opsætningen af adgangskoder er i overensstemmelse med adgangskodepolitikken.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.8 (9.B)	Der foreligger en formel procedure, der sikrer, at adgangsrettigheder fjernes rettidigt i forbindelse med fratrædelse eller ændring af jobfunktion.	Inspiceret, at der foreligger en formel procedure for rettidig fjernelse af adgangsrettigheder ved fratrædelse eller ved ændring af jobfunktion. Inspiceret ved en stikprøve på fratrådte medarbejdere, at deres adgangsrettigheder er fjernet rettidigt. Inspiceret ved en stikprøve på medarbejdere med ændret jobfunktion, at deres adgangsrettigheder er tilpasset rettidigt.	Ingen afvigelser noteret.
9.9 (9.B)	Der foreligger en formel procedure, der sikrer, at adgangsrettigheder gennemgås regelmæssigt.	Inspiceret, at der foreligger en formaliseret procedure for periodisk gennemgang af brugerrettigheder. Inspiceret, at de tildelte brugerrettigheder er blevet gennemgået i overensstemmelse med politikken.	Ingen afvigelser noteret.
9.10 (9.B)	Der foreligger en formel procedure, der sikrer, at systembrugere og adgang til applikationsfunktioner begrænses i overensstemmelse med adgangskontrolpolitikken.	Inspiceret, at der foreligger en formaliseret procedure for systembrugere og deres adgang til applikationsfunktioner. Inspiceret ved en stikprøve på systembrugere, at deres adgang er begrænset i henhold til adgangskontrolpolitikken. Inspiceret ved en stikprøve på brugere med adgang til applikationsfunktionerne, at deres adgang er begrænset i henhold til adgangskontrolpolitikken.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.11 (9.B)	Tildelingen og brugen af privilegerede adgangsrettigheder begrænses og overvåges. Dette omfatter også brugen af understøttende programmer.	Inspiceret, at en formaliseret politik for brug og overvågning af privilegerede adgange er udarbejdet og implementeret. Inspiceret, at brugen af privilegerede adgangsrettigheder er begrænset til personer med et arbejdsbetinget behov. Inspiceret overvågningen af brugen af privilegerede adgangsrettigheder.	Ingen afvigelser noteret.
9.12 (9.B)	Der foreligger procedurer, der angiver sikker afvikling af tjenesteudbydere (fx deaktivering af adgange, IKT-systemer og sletning af tilknyttede data).	Forespurgt om processen for afslutning af kontrakter med NIS2-relaterede leverandører. Inspiceret, at der foreligger en formaliseret procedure, der sikrer nedlukning/fjernelse af NIS2-relevante aktiver og tjenester på sikker vis. Inspiceret ved en stikprøve, at aktiver og/eller tjenester er afviklet på sikker vis.	Ingen afvigelser noteret.
9.13 (9.B)	Der foreligger formaliserede procedurer, der sikrer, at der er implementeret passende fysisk områdesikring af datacentre.	Inspiceret, at en formaliseret procedure for fysisk områdesikring af datacentre er udarbejdet og implementeret. Inspiceret den fysiske områdesikring af datacentre.	Ingen afvigelser noteret.
9.14 (9.B)	Adgang til datacentre er begrænset til medarbejdere med et vigtigt forretningsmæssigt behov herfor, og adgang til datacentre logges.	Inspiceret listen over medarbejdere, der har fysisk adgang til datacentrene. Forespurgt til medarbejdernes forretningsmæssige behov for fysisk adgang til datacentrene. Inspiceret, at fysisk adgang til datacentrene logges, og at adgang er begrænset til medarbejdere med et vigtigt forretningsmæssigt behov.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.15 (9.B)	Virksomheden har implementeret kontroller for at minimere risikoen for potentielle miljømæssige trusler i form af eksempelvis brand, sprængstoffer, røg, vand, støv, kemisk påvirkning, interferens i strømforsyning, interferens i kommunikation samt elektromagnetisk stråling.	Inspiceret, at en formaliseret procedure for at minimere risikoen for fysiske og miljømæssige trusler er udarbejdet og implementeret. Inspiceret, at datacentrene er udstyret med: • indbrudsalarm • brand- og røgalarm • alarm ved opstigende vand • UPS og nødstrømsanlæg • brandslukningsudstyr. Inspiceret, at udstyret er underlagt årligt eftersyn.	Ingen afvigelser noteret.
9.16 (9.C)	Virksomheden har etableret en formaliseret proces med henblik på at oprette og vedligeholde en oversigt over alle relevante systemer og processer i relation til levering af NIS2-tjenester. Følgende kriterier er taget i betragtning ved identificeringen af omfanget af en NIS2-tjeneste: • Elektronisk kommunikationsnetværk • Enhver enhed eller gruppe af forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data • Digitale data, som lagres, behandles, fremfindes eller overføres af elementer anført i punktet ovenfor med henblik på driften, brugen, beskyttelsen og vedligeholdelsen heraf. Processen vurderes regelmæssigt.	Forespurgt om processen for at oprette og vedligeholde en oversigt over relevante systemer i relation til levering af NIS2-tjenester. Inspiceret, at procedurerne til at oprette og vedligeholde en oversigt over relevante systemer i relation til NIS2-tjenester er formaliserede. Inspiceret, at oversigten over NIS2-relevante systemer og processer er i overensstemmelse med gældende aftaler.	Ingen afvigelser noteret.

Kontrolmål 9 – Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
9.17 (9.C)	Virksomheden fører en fortegnelse over NIS2-relevante aktiver, som klassificeres ud fra vigtigheden for kunden, følsomheden og behovet for fortrolighed.	Inspiceret, at en formaliseret procedure for klassifikation af informationer og data er udarbejdet og implementeret. Inspiceret, at fortegnelsen over informationsaktiver og andre relaterede aktiver inkluderer en klassifikation baseret på vigtighed for kunden, følsomheden og behovet for fortrolighed.	Ingen afvigelser noteret.
9.18 (9.C)	Der foreligger formaliserede procedurer, der sikrer, at medier alene bortskaffes af kvalificerede medarbejdere, og at medarbejderne har underskrevet en tavshedserklæring.	Inspiceret, at en formaliseret procedure for sikker bortskaffelse af medier er udarbejdet og implementeret. Forespurgt til bortskaffelse af medier, og om dette er udført af kvalificerede medarbejdere, der har underskrevet tavshedserklæringer.	Ingen afvigelser noteret.

Kontrolmål 10 – Brugen af multifaktorautentifikation eller løbende autentifikationsløsninger, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer i virksomheden, hvor det måtte være relevant

Der foreligger formaliserede procedurer og kontroller for at sikre en stærk autentifikationsproces til administration af adgang til kritiske aktiver samt sikret nødkommunikation.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
10.1 (10.A)	Der foreligger formaliserede procedurer, som fastlægger krav til brugen af multifaktorautentifikation eller alternativt løbende autentifikationsløsninger til kommunikationssystemerne i virksomheden.	Inspiceret, at en formaliseret procedure, som fastlægger krav til anvendelse af multifaktorautentifikation eller alternativt løbende autentifikationsløsninger til kommunikationssystemerne i virksomheden, er udarbejdet og implementeret. Inspiceret, at proceduren er ledelses godkendt årligt eller ved ændringer i processen.	Ingen afvigelser noteret.
10.2 (10.A)	Netværk og informationssystemer, der er forbundet med høj risiko, tilgås som minimum ved at anvende tofaktorautentifikation, eksempelvis når man tilgår: • aktiver ved fjernadgang • administrative systemer • følsomme oplysninger og fortrolig data • systemer, som har høj værdi for virksomheden, eller hvor kompromittering er forbundet med store konsekvenser.	Forespurgt om processen for anvendelse af tofaktorautentifikation i organisationen. Inspiceret, at adgang til netværk og informationssystemer, der er forbundet med høj risiko, som minimum opnås med tofaktorautentifikation.	Ingen afvigelser noteret.
10.3 (10.B)	Der er implementeret sikre primære og sekundære kommunikationsmekanismer til at understøtte fortsat kommunikation og rapportering under en sikkerhedshændelse.	Inspiceret, at sikre primære og sekundære kommunikationsmekanismer er implementeret for at understøtte fortsat kommunikation og rapportering under en sikkerhedshændelse. Inspiceret, at brug af sekundær kommunikationskanal er testet minimum én gang årligt.	Ingen afvigelser noteret.

Kontrolmål 10 – Brugen af multifaktorautentifikation eller løbende autentifikationsløsninger, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer i virksomheden, hvor det måtte være relevant

Der foreligger formaliserede procedurer og kontroller for at sikre en stærk autentifikationsproces til administration af adgang til kritiske aktiver samt sikret nødkommunikation.

Nr.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
10.4 (10.B)	Der gennemføres årlig test af sekundære kommunikationskanaler.	Forespurgt om processen for test af sekundære kommunikationskanaler. Inspiceret, at test af sekundære kommunikationskanaler bliver gennemført årligt. Yderligere inspiceret, at resultatet af testen bliver evalueret, samt at mitigerende handlinger bliver planlagt og igangsat.	Ingen afvigelser noteret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Frank Bech Jensen
Kunde
Serienummer: 4ecdf2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c
IP: 93.165.xxx.xxx
2026-07-08 08:56:11 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-07-08 09:04:59 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 208.127.xxx.xxx
2026-07-08 09:06:32 UTC