www.pwc.dk

itm8 A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2024 til 31. december 2024 i relation til itm8's hosting-ydelser

Februar 2025

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt itm8 A/S' hosting-ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

itm8 A/S anvender Fuzion og InterXion som serviceunderleverandører af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Fuzion og InterXion varetager for itm8 A/S.

itm8 A/S anvender B4Restore og Keepit som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for itm8 A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

itm8 A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af hosting-ydelserne, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2024 til 31. december 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til hosting-ydelserne var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller
   - Relevante kontrolmål og kontroller udformet til at nå disse mål
   - Kontroller, som vi med henvisning til hosting-ydelsernes udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Hvordan andre betydelige begivenheder og forhold end transaktioner behandles
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til hosting-ydelserne foretaget i perioden fra 1. januar 2024 til 31. december 2024

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til hosting-ydelserne, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved generelle it-kontroller i relation til hosting-ydelserne, som den enkelte kunde måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2024 til 31. december 2024. 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, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2024 til 31. december 2024.

Herning, den 3. februar 2025
itm8 A/S

Frank Bech Jensen
Head of Compliance and Security

2 Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2024 til 31. december 2024 i relation til itm8 A/S' hosting-ydelser

Til: itm8 A/S (itm8), itm8's kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om itm8's beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til hosting-ydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2024 til 31. december 2024 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

itm8 A/S anvender Fuzion og InterXion som serviceunderleverandører af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Fuzion og InterXion varetager for itm8.

itm8 anvender B4Restore og Keepit som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for itm8.

Enkelte af de kontrolmål, der er anført i itm8's beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med itm8's kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

itm8's ansvar

itm8 er ansvarlig for udarbejdelsen af beskrivelsen og 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 anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

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 itm8's beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sine hosting-ydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som itm8 har specificeret og beskrevet i ledelsens udtalelse.

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

Begrænsninger i kontroller hos en serviceleverandør

itm8's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved hosting-ydelserne, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en 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. Det er vores opfattelse,

a) at beskrivelsen af de generelle it-kontroller i relation til hosting-ydelserne, således som de var udformet og implementeret i hele perioden fra 1. januar 2024 til 31. december 2024, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2024 til 31. december 2024, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2024 til 31. december 2024.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt itm8's hosting-ydelse, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 3. februar 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

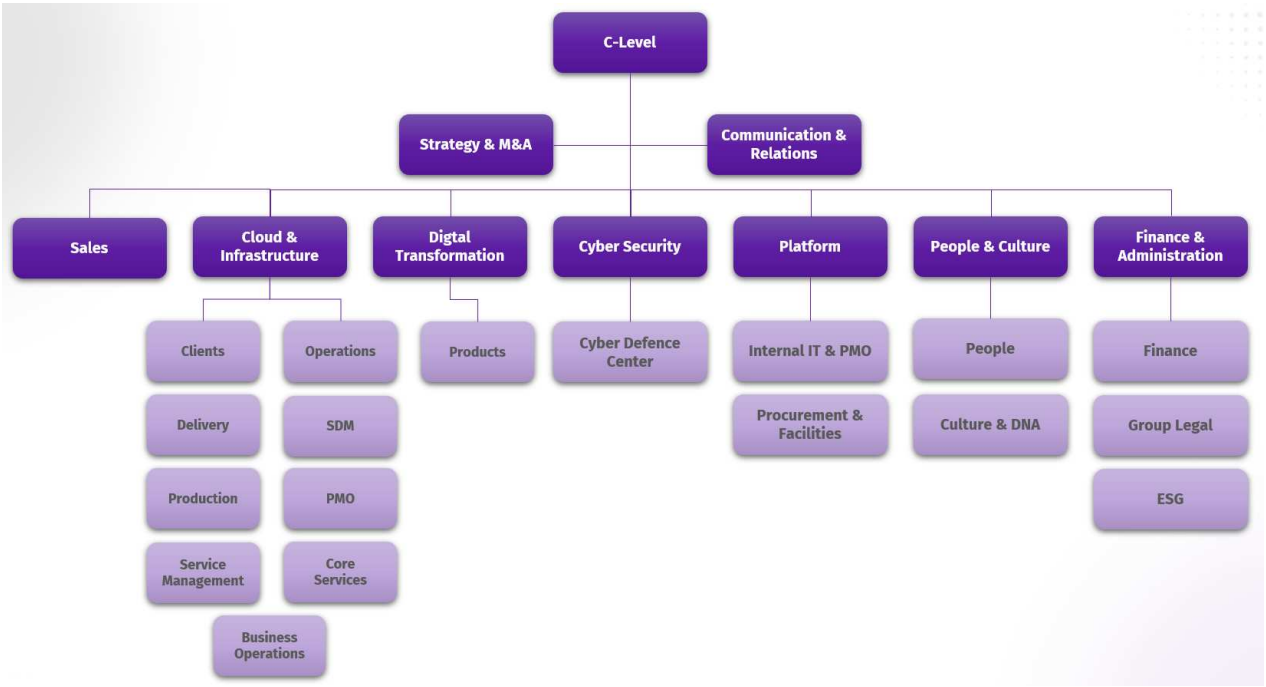
3 Service organisationens systembeskrivelse

Beskrivelse af serviceorganisationen

itm8 A/S har gennemgået en markant udvikling og er blevet en struktureret organisation, der leverer specialiserede it-tjenester og løsninger. Organisationen er opdelt i flere divisioner, hvor kundeorienterede afdelinger 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 kvalitet og compliance til en bred vifte af kunder.

Denne uafhængige revisorerklæring fokuserer på itm8 | Cloud & Infrastructure, som er en central del af erklæringens omfang. Divisionen tilbyder cloud-løsninger og it-infrastrukturtjenester, der lever op til itm8's standarder for sikker og kvalitetsorienteret servicelevering. Rapporten omfatter desuden udvalgte elementer fra itm8 | Cybersecurity, herunder Cyber Defence Center, der spiller en afgørende rolle med 24/7-overvågning, SIEM-loghåndtering og hændelseshåndtering, som alle er kritiske for infrastruktursikkerheden.

Derudover inddrages komponenter fra itm8 | Digital Transformation, særligt Team Products-gruppen, der udvikler skræddersyede løsninger som Send Secure (SEPO) og Tandlægejournal-systemet (TK2). Disse specialiserede løsninger understøtter itm8's forpligtelse til at levere sikre og tilpassede tjenester, der imødekommer kundernes unikke behov.



Omfang af itm8 | Cloud & Infrastructure ISAE 3402 uafhængig revisorerklæring

Kundedivisioner

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

- itm8 | Cloud & Infrastructure
  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.

- itm8 | Cybersecurity
  itm8 | Cybersecurity tilbyder omfattende sikkerhedstjenester, der spænder fra penetrationstests og red teaming til rådgivning om cyberrisici. Divisionen inkluderer et Cyber Defence Center, som leverer løbende SIEM-loghåndtering, sårbarhedsvurderinger og realtids-hændelseshåndtering.

- itm8 | Digital Transformation
  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 Tandlægejournal-systemet (TK2), for at optimere forretningsprocesser.

- itm8 | Application Services
  itm8's Application Services-division accelererer udvikling og vedligeholdelse af applikationer med fokus på sikkerhed og kvalitet. Tjenesterne inkluderer applikationsstyring, databaseadministration, overvågning, performanceoptimering og teknisk support.

Forretningsdivisioner

Som støtte til disse kerneområder leverer itm8's forretningsdivisioner—såsom HR, 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 højkvalitetstjenester, der understøtter kundernes strategiske mål.

Ledelsessystem for informationssikkerhedLedelsessystemet for informationssikkerhed (ISMS) hos itm8 | Cloud & Infrastructure er designet til at opfylde kravene i ISO 27001:2022 og integrere informationssikkerhed i vores organisatoriske processer og kultur.

Organisatorisk kontekst

Vores ISMS er tilpasset itm8's kontekst og tager højde for vores strategiske mål, eksterne og interne udfordringer samt interessenternes behov og forventninger. Gennem interessentanalyser sikrer vi, at vores informationssikkerhedstiltag er på linje med forventningerne fra relevante parter og tilpasset et skiftende risikobillede.

Ledelse

Ledelsens engagement er en hjørnesten i vores ISMS. Topledelsen har defineret og godkendt en omfattende informationssikkerhedspolitik, der fastlægger organisationens sikkerhedsmål og sikrer sammenhæng med de overordnede forretningsmål. Ledelsen arbejder aktivt på at fremme en sikkerhedskultur, allokere tilstrækkelige ressourcer samt tydeligt kommunikere og forankre roller og ansvar i hele organisationen.

Planlægning

Planlægningen af vores ISMS bygger på en struktureret risikostyringsproces og -metodologi understøttet af et dedikeret system. Vi udfører regelmæssige risikovurderinger for at identificere, evaluere og mitigere ri-

sici og sikre, at de håndteres inden for acceptable niveauer. Informationssikkerhedsmål fastsættes, gennemgås periodisk og integreres i virksomhedens overordnede strategiske planlægning for at sikre en proaktiv tilgang til risikostyring.

Support

Vores ISMS understøttes af et dokumenthåndteringssystem (DMS), som sikkert opbevarer al officiel dokumentation og opfylder kvalitetskrav. Derudover vedligeholder vi et omfattende sikkerhedsbevidsthedsprogram, der tilbyder løbende træning og tests for at sikre, at alle medarbejdere forstår deres rolle i at opretholde og forbedre informationssikkerheden. Programmet fokuserer på kompetenceudvikling og øget bevidsthed på tværs af organisationen.

Drift

Vi implementerer og styrer vores processer baseret på ITIL-rammeværket, hvilket sikrer, at alle operationer er i overensstemmelse med bedste praksis og vores definerede informationssikkerhedsmål. Vores operationelle tilgang integrerer sikkerhed i de daglige forretningsaktiviteter, så sikkerhed bliver en naturlig del af organisationen. DMS fungerer som en central platform for alle processer, procedurer og politikker, hvilket sikrer, at driftsaktiviteterne er i overensstemmelse med ISMS.

Præstationsevaluering

For at sikre effektiviteten af vores ISMS overvåger, måler og evaluerer vi regelmæssigt vores informationssikkerhedsprocesser. Dette inkluderer et struktureret internt revisionsprogram, der systematisk gennemgår alle elementer af ISMS over en treårig cyklus. Disse revisioner, kombineret med ledelsesgennemgange og andre præstationsmålinger, giver kritisk indsigt, som hjælper os med at fastholde overensstemmelse med forretningsbehov og nye trusler. Resultaterne bruges til løbende forbedring og sikrer, at vores ISMS forbliver effektivt og opdateret.

Forbedring

Løbende forbedring er integreret i vores ISMS gennem halvårlige møder om kontinuerlig forbedring (CIM) i Compliance & Security-teamet. Disse møder, hvor der føres officielle referater, giver en platform for at diskutere alle aspekter af informationssikkerhed hos itm8. Indsigter fra møderne, interne audits og præstationsevalueringer bruges til at drive forbedringer i vores ISMS. Vi er forpligtede til en cyklus af løbende udvikling for at sikre, at vores ISMS forbliver dynamisk og effektivt i håndteringen af nye trusler og i overensstemmelse med branchens bedste praksis.

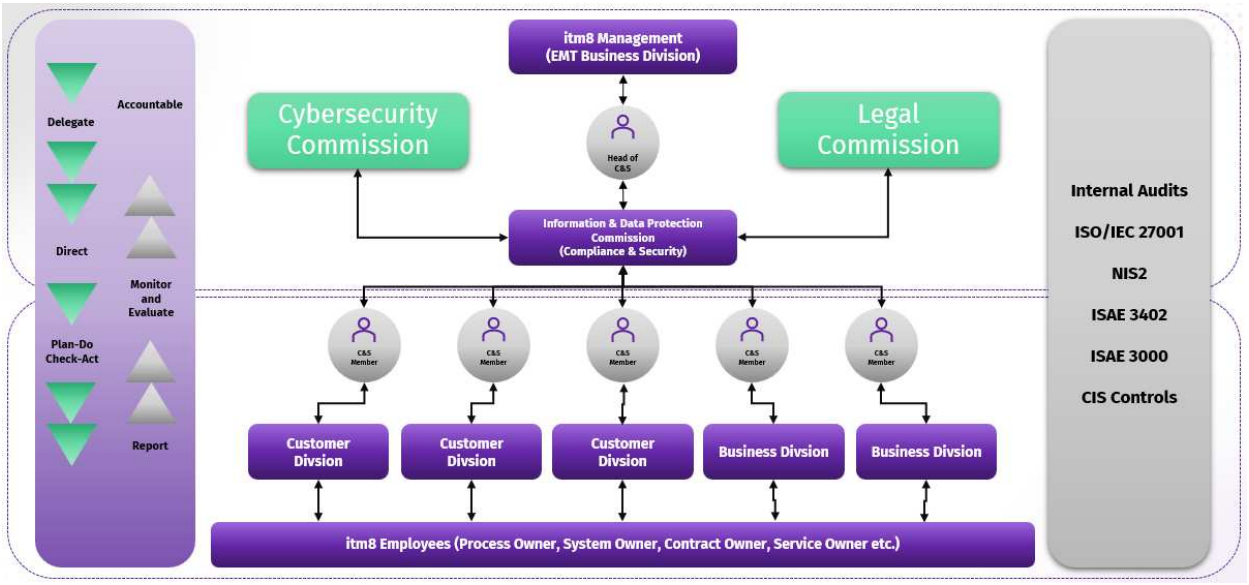
Der har ikke været væsentlige ændringer til procedurer og kontroller i perioden fra 1. januar 2024 til 31. december 2024.

Informationssikkerhedsstyring

Informationssikkerhedsstyring hos itm8 | Cloud & Infrastructure er designet til at sikre, at sikkerhedspraksis er integreret i hele organisationen i overensstemmelse med ISO/IEC 27001:2022. Vores tilgang starter med en informationssikkerhedspolitik, godkendt af topledelsen, der beskriver vores sikkerhedsmål og understøttes af 15 emnespecifikke politikker. Disse politikker dækker områder som adgangskontrol, aktivstyring, forretningskontinuitet og hændelseshåndtering og ejes af Compliance & Security-teamet. Relevante politikker kommunikeres til de berørte interessenter.

Vi har klart definerede roller inden for informationssikkerhed, herunder funktioner som information security manager, systemejer og procesejer, for at sikre, at ansvar er tydeligt tildelt og forstået. Funktionsadskillelse er implementeret i kritiske områder som backup, finans, ændringsstyring og udvikling for at reducere risici forbundet med uautoriseret adgang eller fejl.

Vores struktur for informationssikkerhedsstyring placerer det overordnede ansvar hos topledelsen, som delegerer opgaver til Compliance & Security-teamet. Dette team samarbejder med Cybersecurity- og Legalkommissionerne for at håndtere tekniske og juridiske sikkerhedsaspekter. Medlemmer af Compliance & Security-teamet er tilknyttet specifikke divisioner og arbejder sammen med roller som procesejere, systemejere og serviceejere for at implementere sikkerhedsforanstaltninger på tværs af itm8.



itm8 sikkerhedsstyringsstruktur

Ledelsen spiller en afgørende rolle i at understøtte vores informationssikkerhedsramme, sikre overholdelse af gældende krav og aktivt deltage i styringen af vores ISMS. Vi opretholder en opdateret liste over alle relevante myndigheder og lovgivning med tilknyttede ansvarlige ejere for at sikre compliance og lette kommunikationen med tilsynsmyndigheder. Vores deltagelse i forskellige interessegrupper, såsom sikkerhedsfora og it-netværksgrupper, holder os opdateret om branchetrends og bedste praksis.

Informationssikkerhed er også integreret i vores projektstyringspraksis gennem en risikostyringsproces, der kræver, at projektledere udfører en indledende risikovurdering i starten af et projekt. Dette sikrer, at sikkerhedsovervejelser behandles tidligt i projektets livscyklus, hvilket yderligere forankrer informationssikkerhed i vores organisatoriske processer og kultur.

Styring af aktiver

itm8 | Cloud & Infrastructure administrerer sine informationer og tilknyttede aktiver i overensstemmelse med ISO/IEC 27001:2022-standarderne. Vi opretholder aktivfortegnelser via forskellige databaser, herunder en primær CMDB til CI'er og kundevendte løsninger samt InTune MDM til endpoint-administration. Klare politikker og sikkerhedsguides beskriver acceptabel brug og sikrer, at alle medarbejdere forstår, hvordan aktiver håndteres ansvarligt.

Procedurer for tilbagelevering af aktiver er integreret i vores HR-processer for at sikre sikker tilbagelevering, når medarbejdere forlader virksomheden eller skifter rolle. Vi har etableret retningslinjer for sikring af aktiver uden for virksomheden samt for håndtering af lagermedier på både endpoint-enheder og kundevendte platforme som servere.

Der er procedurer for sikker bortskaffelse og genanvendelse af udstyr, som omfatter både interne og kundevendte aktiver, hvilket sikrer, at alle data slettes korrekt. Brugerens endpoint-enheder administreres centralt og er tilknyttet domænet, hvilket gør det muligt for os at håndhæve sikkerhedskonfigurationer og opretholde kontrol over disse aktiver.

Informationsbeskyttelse

Hos itm8 | Cloud & Infrastructure sikrer vi effektiv informationsbeskyttelse i overensstemmelse med ISO/IEC 27001:2022-kontroller. Vi har etableret et klassifikationsskema beskrevet i vores *Principles & Rules for Information Protection*, som vejleder i klassifikation og mærkning af information baseret på dens følsomhed. Dette sikrer, at al information håndteres korrekt i forhold til sin klassifikation.

For at beskytte data under overførsel har vi udviklet specifikke regler og politikker, herunder sikkerhedsguides, der beskriver sikre metoder til informationsudveksling. Beskyttelse af registre håndteres gennem standardsystemdesign og etablerede procedurer med særligt fokus på privatlivsbeskyttelse og overholdelse af EU's GDPR for personoplysninger (PII).

Vi har klare procedurer for sletning af information for at sikre, at data fjernes sikkert, når det ikke længere er nødvendigt. Datamaskering anvendes ved brug af testdata fra produktionsmiljøer for at opretholde privatliv og sikkerhed, selv under testscenarier.

For at forhindre datalækager har vi implementeret overvågningsaktiviteter, der er designet til at opdage og afhjælpe uautoriseret dataeksponering. Testinformation beskyttes i overensstemmelse med vores fastlagte standarder og relevante aftaler, hvilket sikrer, at det behandles med samme omhu som live-data.

HR-sikkerhed

Human resources-sikkerhed hos itm8 | Cloud & Infrastructure håndteres i overensstemmelse med ISO/IEC 27001:2022 for at sikre, at alt personale er tilstrækkeligt vurderet, uddannet og holdt ansvarlig for deres roller i informationssikkerhed. Vi gennemfører baggrundstjek af medarbejdere ved ansættelse, hvilket inkluderer indhentning af en ren straffeattest, og dette tjek gentages hvert tredje år af ansættelsen for at opretholde et højt niveau af pålidelighed.

Vores ansættelsesvilkår indeholder specifikke klausuler relateret til informationssikkerhed, hvilket sikrer, at alle medarbejdere forstår deres forpligtelser. Vi har et sikkerhedsbevidsthedsprogram, der omfatter regelmæssig træning, kontinuerlige phishing-simuleringer og andre testscenarier for at holde medarbejderne forberedte på sikkerhedstrusler.

For at håndtere brud på informationssikkerheden har vi en disciplinær proces på plads, som anvendes, når det er nødvendigt for at håndhæve vores sikkerhedspolitikker. Efter opsigelse eller ændringer i ansættelsen håndterer vi adgangsrettigheder omhyggeligt, og de tilbagekaldes eller justeres efter behov for at opretholde sikkerheden.

Fortroligheds- og hemmeligholdelsesaftaler er integrerede dele af vores ansættelseskontrakter, med yderligere aftaler for visse roller afhængig af kundens krav. For fjernarbejde har vi etableret specifikke regler og retningslinjer, der er beskrevet i vores sikkerhedsguides, for at sikre, at medarbejderne opretholder sikkerhedsstandarder, når de arbejder uden for kontoret.

Fysisk sikkerhed

itm8 | Cloud & Infrastructure opretholder robuste fysiske sikkerhedsforanstaltninger i overensstemmelse med ISO/IEC 27001:2022 for at beskytte vores aktiver og faciliteter. Fysiske sikkerhedsperimetre er etableret på både kontor- og datacenterlokationer, hvor områder, der kræver beskyttelse, samt de nødvendige sikkerhedsforanstaltninger, defineres. Fysisk adgang til disse lokationer kontrolleres gennem brug af ID-kort, PIN-koder og alarmsystemer ved centrale adgangspunkter.

Kontorer, rum og faciliteter er sikret baseret på deres følsomhed med definerede sikkerhedszoner, der har skræddersyede foranstaltninger for at beskytte mod uautoriseret adgang. Vi implementerer beskyttelse mod fysiske og miljømæssige trusler og tilpasser sikkerhedskontrollerne i forhold til den følsomhed, informationen i et pågældende område har.

Retningslinjer og procedurer for arbejde i sikre områder er på plads for at opretholde et højt sikkerhedsniveau i disse miljøer. En politik om ryddelige borde og skærme håndhæves, og forventningerne kommunikeres gennem vores sikkerhedsguides for at sikre, at følsomme oplysninger ikke efterlades eksponeret.

Udstyr placeres og beskyttes baseret på dets følsomhed og formål med sikre placeringer, der sikrer hardwarens sikkerhed og integritet. Støttefunktioner tilpasses efter behovene for hver lokation; for eksempel er datacentre og andre kritiske steder udstyret med backupgeneratorer og UPS-systemer for at opretholde driften under strømafbrydelser.

Vi sikrer også, at alt udstyr vedligeholdes professionelt i henhold til producentens anbefalinger, så det fungerer effektivt og forbliver sikkert gennem hele dets livscyklus. Kabelinstallationer håndteres sikkert for at forhindre manipulation og uautoriseret adgang, og alle vedligeholdelsesaktiviteter udføres for at opretholde de højeste standarder for operationel sikkerhed.

System- og netværkssikkerhed

System- og netværkssikkerhed hos itm8 | Cloud & Infrastructure håndteres i overensstemmelse med ISO/IEC 27001:2022 for at sikre et sikkert driftsmiljø for både interne systemer og kundesystemer. Vi har etableret dokumenterede driftsprocedurer, der guider håndteringen af forskellige opgaver i vores it-miljøer, hvilket sikrer konsistens og sikkerhed på tværs af alle operationer.

For at beskytte mod malware implementerer og overvåger vi beskyttelsesforanstaltninger på vores interne infrastruktur og udvider disse tjenester til kundemiljøer som aftalt. Brug af privilegerede værktøjsprogrammer er begrænset til en udpeget gruppe af medarbejdere, hvilket sikrer, at kun autoriseret personale har adgang til kritiske funktioner.

Vores netværkssikkerhedsramme omfatter flere forsvarslag såsom DMZ'er, firewalls og segregerede miljøer, der er skræddersyet til at beskytte både produktions- og kontornetværk. Netværkstjenester opsættes sikkert i overensstemmelse med bedste praksis og kundeaftaler og sikrer, at tjenesterne lever op til kontraktuelle og sikkerhedsmæssige krav.

Vi opretholder streng netværkssegregation, hvor produktions- og kontornetværk holdes adskilt, og kundernes netværk segmenteres i henhold til deres specifikke aftaler for at opretholde dataintegritet og sikkerhed. Webfiltreringsforanstaltninger, herunder Safelinks, er på plads for at advare brugere om potentielt skadelige websider, og brud på disse sikkerhedsforanstaltninger udløser notifikationer til vores Cyber Defense Center for øjeblikkelig handling.

Change management er en integreret del af vores tilgang med en struktureret proces, der omfatter risikovurdering af ændringer. Kritiske ændringer gennemgås på CAB-møder for at sikre, at potentielle virkninger bliver fuldt ud vurderet og afbødet, hvilket opretholder sikkerheden og stabiliteten af vores systemer og netværk.

Applikationssikkerhed

itm8 | Cloud & Infrastructure håndterer applikationssikkerhed i overensstemmelse med ISO/IEC 27001:2022-kontroller. Adgang til kildekode er begrænset til de medarbejdere, der har behov for det, hvilket sikrer, at følsom kode beskyttes. Vi har implementeret en sikker udviklingscyklus, der integrerer sikkerhedskrav tilpasset applikationernes kritikalitet.

Sikker systemarkitektur og kodningspraksis følges for at reducere sårbarheder, og sikkerhedstest udføres under udviklings- og acceptstadiet for at validere applikationer, før de overgår til produktion.

For outsourcet udvikling sikrer specifikke retningslinjer, at sikkerhedsstandarder overholdes. Udviklings-, test- og produktionsmiljøer holdes adskilt for at forhindre indblanding og opretholde systemintegriteten.

Sikker konfiguration

Vi har en konfigurationsstyringsproces, der understøttes af en centraliseret CMDB, som bruges til at administrere alle konfigurationsenheder (CIs) for både interne systemer og kundevendte miljøer.

Vores procedure for patch management sikrer, at softwareopdateringer og patches anvendes sikkert og i overensstemmelse med kontraktlige aftaler. Derudover har vi etableret regler for brugen af kryptering til at beskytte data og kommunikation, hvilket sikrer, at de opfylder de krævede sikkerhedsstandarder.

Identitets- og adgangsstyring

Hos itm8 | Cloud & Infrastructure overholder vi ISO/IEC 27001:2022-kontroller for at beskytte adgangen til systemer og information. Vi har implementeret en adgangskontrolpolitik og tilhørende procedurer for effektivt at regulere adgangen.

Identitetsstyring håndteres i samarbejde mellem personaleledelse, brugeradministration og HR og dækker hele livscyklussen for brugeridentiteter. Godkendelsespraksis er defineret for både kundevendte og interne miljøer, hvilket sikrer, at sikre metoder er på plads.

Adgangsrettigheder tildeles baseret på jobkrav, og vi begrænser privilegeret adgang til kun nødvendigt personale. Specifikke regler styrer håndteringen af privilegerede konti og godkendelsesoplysninger. Adgang til følsomme oplysninger, herunder kundedata og HR-optegnelser, er begrænset i henhold til foruddefinerede politikker.

Sikker godkendelse håndhæves med anvendelse af multifaktorautentificering (MFA), hvor det er kritisk for at øge sikkerheden.

Trussels- og sårbarhedshåndtering

Trussels- og sårbarhedshåndtering er tilpasset ISO/IEC 27001:2022-kontroller for at beskytte vores systemer og data. Vi håndterer trusselsefterretninger på flere niveauer: strategisk, taktisk og operationelt. Strategiske trusselsefterretninger adresserer bredere samfundsmæssige, geopolitiske og markedsrelaterede trusler, mens taktiske og operationelle trusselsefterretninger fokuserer på tekniske aspekter såsom specifikke sårbarheder, angrebsmønstre og ondsindede enheder.

Vores håndtering af tekniske sårbarheder styres af en defineret procedure, som inkluderer løbende sårbarhedsvurderinger og håndtering i vores eget interne miljø med ansvar tildelt teknologiejere for at sikre rettidig identifikation og afhjælpning af sårbarheder.

Kontinuitet

Kontinuitetsstyring er designet til at sikre løbende drift og modstandsdygtighed. Vores forretningskontinuitetsplaner beskriver kommunikationsstrategier, roller og procedurer for at opretholde forretningsfunktioner under forstyrrelser eller store hændelser.

Kapacitetsstyring håndteres gennem etablerede kriterier og tærskelværdier, med løbende overvågning af platformskapaciteter for at sikre rettidige justeringer og forhindre potentielle problemer.

Vi opretholder omfattende og sikre backupfaciliteter, herunder redundante backupper, der håndteres af en ISO/IEC 27001-certificeret tredjepartsleverandør. Disse backupper opbevares i geolokaliserede faciliteter adskilt fra den oprindelige produktionsmiljø for at sikre deres tilgængelighed, selv under store forstyrrelser.

Sikkerhed i leverandørforhold

Hos itm8 | Cloud & Infrastructure håndterer vi leverandørforhold med stærkt fokus på informationssikkerhed. Vores aftaler med leverandører inkluderer ofte sikkerhedsbilag, hvor det er muligt og relevant, og vi overvåger aktivt leverandørernes aktiviteter for potentielle problemer.

En formel procedure for leverandør-onboarding sikrer, at leverandører kategoriseres og evalueres, inden der indgås aftaler. Vi udfører løbende risikovurderinger for kritiske leverandører for at håndtere potentielle risici effektivt.

Vores Cloud Security-strategi skitserer sikkerhedshensyn for cloud-tjenester, herunder strategier for håndtering af og exit-strategier for cloud-partnerskaber efter behov, hvilket sikrer løbende sikkerhed gennem hele livscyklussen af disse tjenester.

Compliance

Vi sikrer overholdelse af juridiske, lovgivningsmæssige, regulatoriske og kontraktuelle krav ved at opretholde et overblik over gældende forpligtelser og tildele interne ejere for hver krav.

Intellektuelle ejendomsrettigheder (IPR) beskyttes gennem etablerede regler og retningslinjer, der er inkluderet i vores politikker og medarbejderkontrakter, hvilket sikrer korrekt håndtering og beskyttelse af intellektuelle aktiver.

Vi gennemfører løbende uafhængige gennemgange af vores informationssikkerhedspraksis, herunder ISAE 3402- og ISAE 3000-revisioner for hosting-tjenester og databeskyttelse, samt revisioner af kunder og eksterne revisioner i henhold til vores ISO 27001-certificering.

Vi forbliver compliant med relevante politikker, regler og standarder for informationssikkerhed og opdaterer løbende vores praksis for at sikre, at vi følger de relevante rammeværk og at vores foranstaltninger afspejler de gældende compliance krav.

Håndtering af informationssikkerhedshændelser

Vi håndterer informationssikkerhedshændelser gennem en struktureret incident management-proces, der omfatter procedurer for store hændelser og sikkerhedshændelser. Disse procedurer beskriver roller, ansvar og de nødvendige skridt for at vurdere, reagere på og lære af hændelser.

Vi sikrer grundig indsamling af beviser under hændelseshåndtering for at understøtte analyse og levere dokumentation til gennemgang. Informationssikkerhedshændelser rapporteres løbende til den øverste ledelse som en del af vores regelmæssige ledelsesgennemgange, samt gennemgås under vores to-månedlige Continuous Improvement Meetings.

Vores SIEM Log Management-løsning logger og overvåger aktiviteter døgnet rundt, mens tidssynkronisering opretholdes for at sikre præcise tidsstempler for alarmer, hvilket giver et pålideligt overblik over hændelser og it-miljøets drift.

Kontrolmål og -aktiviteter fremgår detaljeret i afsnit 4.

Komplementære kontroller hos kunder

Forhold, der skal overvejes af kundernes revisorer

Leverede serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på itm8s standardvilkår. Kundernes afvigelser fra itm8s standardvilkår er derfor ikke omfattet af denne erklæring.

Kundernes egne revisorer bør derfor vurdere, om denne erklæring kan udvides til at omfatte den specifikke kunde, og afdække eventuelle andre risici, som er relevante for aflæggelsen af kundernes regnskaber. Hvad angår ændringsstyring, er det kun kerneinfrastrukturen, der er omfattet af standardkontrakterne, og eventuel ændringsstyring på kundeløsningerne skal dækkes af en særskilt aftale med itm8.

Brugeradministration

itm8 tildeler adgang og rettigheder i overensstemmelse med kundens anvisninger, når disse er meldt ind til servicedesk. itm8 er ikke ansvarlig for, at disse oplysninger er korrekte, og det er således kundernes ansvar at sikre, at adgangen og rettighederne til systemer og applikationer tildeles hensigtsmæssigt og i overensstemmelse med bedste praksis for funktionsadskillelse.

itm8 tildeler også adgang til tredjepartskonsulenter – primært udviklere, der skal vedligeholde applikationer, der indgår i hosting-aftalen. Dette sker i henhold til instrukser fra itm8s kunder.

Kundernes egne revisorer bør derfor uafhængigt vurdere, om de adgange og rettigheder til applikationer, servere og databaser, der tildeles til kundens egne medarbejdere og til tredjepartskonsulenter, er hensigtsmæssige på baggrund af en vurdering af risikoen for fejlinformationer i regnskabsaflæggelsen.

Som standard anvender itm8 og kundens interne it-medarbejdere en fælles systemadgang (fælles administratoradgangskode). De konti, der benyttes af itm8, er ofte konti med udvidede rettigheder. Som en øget beskyttelse af disse konti tilbyder itm8 en Just-in-Time-løsning. Dette er ikke en del af standardkontrakten med itm8. Just-in-Time er et system til beskyttelse af itm8s administratorkonti. Det sikrer, at brugen af adgang logges og kan spores, at der bruges stærke adgangskoder, og at adgangskoder ændres, hver gang kontoen er blevet brugt. Med Just-in-Time er der ingen, der kender adgangskoden, når itm8 ikke er logget ind. Dette begrænser muligheden for, at en itm8-konto kan bruges af en hacker til lateral bevægelse, og at en medarbejder kan huske en adgangskode, når han ikke længere er ansat i itm8.

Beredskabsplanlægning

De generelle betingelser for hosting hos itm8 fastlægger ikke krav til beredskabsplanlægning og gendannelse af kundernes systemmiljø i tilfælde af en nødsituation.

itm8 sikrer generel backup af kundemiljøerne, men hosting-aftalerne omfatter ikke en garanti for fuld gendannelse af kundernes systemmiljø efter en nødsituation. Kundernes egne revisorer bør derfor uafhængigt vurdere risikoen for manglende beredskabsplanlægning og regelmæssig test heraf i forhold til en risiko for fejlinformation i regnskabsaflæggelsen.

Overholdelse af relevant lovgivning

itm8 har planlagt procedurer og kontroller, så lovgivningen på de områder, som itm8 er ansvarlig for, overholdes i tilstrækkelig grad. itm8 er ikke ansvarlig for de applikationer, der kører på det hostede udstyr. Derfor omfatter denne erklæring ikke sikring af, at der er etableret tilstrækkelige kontroller i brugerapplikationerne, og at applikationerne overholder bogføringsloven, persondataloven og anden relevant lovgivning.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunder er ikke omfattet af vores testhandlinger.

Vores test af funktionaliteten har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2 Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontrollerne er implementeret og har fungeret i perioden fra 1. januar 2024 til 31. december 2024. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.1	**Politikker for informationssikkerhed** *Informationssikkerhedspolitik og emnespecifikke politikker skal defineres, godkendes af ledelsen, offentliggøres, kommunikeres til og anerkendes af relevante medarbejdere og relevante interessenter og vurderes med planlagte mellemrum, samt hvis der sker væsentlige ændringer.* itm8 | Cloud & Infrastructure har etableret og dokumenteret en informationssikkerhedspolitik, der er godkendt af topledelsen og distribueret til alle medarbejdere. Derudover er flere emnespecifikke politikker udviklet for at støtte informationssikkerhedspolitikken og kommunikeres til alle relevante medarbejdere. Disse politikker gennemgås mindst én gang årligt, eller hver gang der sker væsentlige ændringer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har inspiceret, at informationssikkerhedspolitikkerne kommunikeres til medarbejderne og relevante parter og er revideret årligt.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.2	**Roller og ansvar for informationssikkerhed** *Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov.* itm8 | Cloud & Infrastructure har etableret klart de-finerede roller og ansvar, der er i overensstemmelse med kravene i deres informationssikkerhedsledelsessystem (ISMS). Disse roller er tildelt baseret på organisationens behov for at sikre effektiv ledelse og overvågning af informationssikkerheden på tværs af virksomheden.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer.	Ingen afvigelser noteret.
5.3	**Funktionsadskillelse** *Konfliktende opgaver og konfliktende ansvarsområder skal adskilles.* itm8 | Cloud & Infrastructure har etableret politikker for adskillelse af ansvar, som sikrer, at modstridende opgaver holdes adskilt. Disse politikker gennemgås mindst én gang årligt eller ved væsentlige ændringer for at sikre overensstemmelse med informationssikkerhedspolitikken og opretholde det nødvendige niveau af adskillelse for at beskytte informationssikkerheden.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos itm8, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.4	**Ledelsens ansvar** *Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.* itm8 | Cloud & Infrastructure requires its management team to actively support and familiarize themselves with applicable information security initiatives. Management is also responsible for educating their employees on these initiatives to ensure compliance with the organization's information security policies and procedures.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion påset, at ledelsen er bekendt med informationssikkerhedsinitiativer.	Ingen afvigelser noteret.
5.5	**Kontakt med myndigheder** *Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.* itm8 | Cloud & Infrastructure har etableret kommunikationsprocedurer til at underrette relevante myndigheder i tilfælde af en sikkerhedshændelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har en kommunikationsprocedure for, hvordan der kommunikeres med relevante myndigheder i tilfælde af sikkerhedsbrud.	Ingen afvigelser noteret.
5.7	**Underretning om trusler** *Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretninger om trusler.* itm8 | Cloud & Infrastructure indsamler trusselsinformation fra forskellige kilder, herunder sårbarhedsrapporter, udvalgte nyhedskilder, leverandører, myndigheder og interessegrupper, for at understøtte risikobaseret beslutningstagning.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at itm8 indhenter og analyserer information til brug for risikobaseret beslutningstagning.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.9	**Fortegnelse over information og understøttende aktiver** *Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.* itm8 | Cloud & Infrastructure har implementeret og vedligeholder flere Configuration Management Databaser (CMDB'er), der er tilpasset arten af de aktiver, der er omfattet. Dette inkluderer fortegnelse over endpoints, servere, netværksudstyr og databaser, som alle har tildelte ejere og relevante oplysninger knyttet til sig.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Ingen afvigelser noteret.
5.10	**Acceptabel brug af information og understøttende aktiver** *Regler for acceptabel brug og procedurer til håndtering af information og understøttende aktiver skal identificeres, dokumenteres og implementeres.* itm8 | Cloud & Infrastructure har etableret og implementeret regler for acceptabel brug af virksomhedens aktiver, som er dokumenteret i Politikken for Acceptabel Brug.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at passende kontroller er på plads for at sikre dokumentation og vedligeholdelse af beholdningen af aktiver, herunder acceptabel brug af aktiver.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.12	**Klassifikation af information** *Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.* itm8 | Cloud & Infrastructure har etableret en dataklassificeringsordning, der omhandler, hvordan forskellige typer data skal klassificeres og håndteres i overensstemmelse med deres klassificering.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at itm8 har etableret en dataklassificeringsordning til klassifikation af information.	Ingen afvigelser noteret.
5.14	**Overførsel af information** *Der skal være etableret regler eller procedurer for eller aftaler om overførsel af information for alle former for overførselsfaciliteter i organisationen og mellem organisationen og andre parter.* itm8 | Cloud & Infrastructure har etableret politikker og procedurer for informationsoverførsel, der sikrer, at information overføres via sikre og pålidelige kommunikationskanaler.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at en passende teknisk sikkerhedsarkitektur er blevet etableret i netværket, samt at der er etableret regler for informationsoverførsel.	Ingen afvigelser noteret.
5.15	**Administration af adgang** *Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til information og understøttende aktiver på grundlag af forretnings- og informationssikkerhedskrav.* itm8 | Cloud & Infrastructure har implementeret retningslinjer for adgang til egne og kunders systemer baseret på forretningsmæssige og informationssikkerhedsmæssige krav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har kontrolleret, at retningslinjer for adgangskontrol er implementeret, gennemgået og godkendt.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.18	**Adgangsrettigheder** *Adgangsrettigheder til information og understøttende aktiver bør tilvejebringes, vurderes, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for administration af adgang.* itm8 | Cloud & Infrastructure gennemgår regelmæssigt medarbejderes privilegerede tekniske rettigheder i både interne og kundevendte systemer for at sikre, at de er passende i forhold til arbejdsrelaterede behov. Ikke-tekniske privilegerede medarbejdere tildeles nødvendige rettigheder til brug af interne systemer, som justeres ved ændringer i ansættelse, overflytninger og opsigelser. Når en medarbejder forlader itm8, fjernes alle adgangsrettigheder, og der foretages justeringer ved ændringer i jobfunktioner.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen. Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.	Ingen afvigelser noteret.
5.19	**Informationssikkerhed i leverandørforhold** *Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.* itm8 | Cloud & Infrastructure har etableret procedurer til håndtering af sikkerhedsrisici relateret til leverandørers produkter og tjenester, herunder årlige risikovurderinger og audits for at sikre, at leverandører fortsat opfylder organisationens sikkerhedskrav.	Vi har inspiceret, at der findes en formel og dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved stikprøvevis inspektion påset, at der udarbejdes risikovurderinger med passende mellemrum på kritiske leverandører. Vi har ved inspektion påset, at itm8 jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.20	**Håndtering af informationssikkerhed i leverandøraftaler** *Relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkelt leverandør på grundlag af typen af leverandørforhold.* itm8 | Cloud & Infrastructure har etableret sikkerhedskrav for leverandører, som er inkluderet i de kontraktuelle aftaler og de generelle vilkår og betingelser for samarbejde med itm8.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at en formel og dokumenteret procedure er på plads for at sikre, at nye eller genforhandlede applikations- eller serviceleverandørkontrakter valideres i forhold til en liste over definerede informationssikkerhedskrav.	Ingen afvigelser noteret.
5.22	**Overvågning, vurdering og ændringsstyring af leverandørydelser** *Organisationen skal regelmæssigt overvåge, vurdere, evaluere og styre ændringer i leverandørens informationssikkerhedspraksis og levering af ydelser.* itm8 | Cloud & Infrastructure har etableret procedurer af sikkerhedsrisici forbundet med leverandørers produkter og tjenester, herunder årlige risikovurderinger og audits for at sikre overholdelse af organisationens sikkerhedskrav. Derudover håndteres eventuelle ændringer i leverandørtjenester, som påvirker kundemiljøer, tjenester eller infrastruktur, gennem itm8's change management-proces.	Vi har inspiceret, at der findes en formel, dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt. Vi har ved inspektion af stikprøver påset, at itm8 jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav. Vi har inspiceret, at tredjepartserklæringer for hovedleverandører er modtaget og behandlet af itm8.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.23	**Informationssikkerhed ved brug af cloud-tjenester** *Der skal fastlægges processer for anskaffelse, brug, styring og afslutning af brugen af cloud-tjenester i overensstemmelse med organisationens informationssikkerhedskrav.* itm8 | Cloud & Infrastructure har etableret en strategi for anvendelse af cloudtjenester, der er i overensstemmelse med organisationens informationssikkerhedskrav og omfatter processer for anskaffelse, administration og exit.	Vi har ved inspektion påset, at der er etableret en strategi for brugen af cloud-tjenester.	Ingen afvigelser noteret.
5.24	**Planlægning og forberedelse af incident-håndtering ved sikkerheds-incidents** *Organisationen skal planlægge og forberede sig på at håndtere informationssikkerheds-incidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerheds-incidents.* itm8 | Cloud & Infrastructure har defineret og implementeret en plan for håndtering af informationssikkerhedshændelser, som inkluderer processer for hændelseshåndtering samt klart definerede roller og ansvar i forbindelse med hændelsesrespons.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at den formelle og dokumenterede proces for hændelsesstyring er blevet gennemgået og godkendt. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.26	**Håndtering af informationssikkerheds-hændelser** *Informationssikkerhedshændelser skal håndteres i overensstemmelse med de dokumenterede procedurer.* itm8 | Cloud & Infrastructure har etableret procedurer for håndtering af informationssikkerhedshændelser.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.
5.27	**Læring af informationssikkerhedshændelser** *Den viden, der opnås i forbindelse med informationssikkerheds-incidents, skal anvendes til at styrke og forbedre foranstaltningerne for informationssikkerhed.* itm8 | Cloud & Infrastructure har etableret procedurer for at lære af informationssikkerhedshændelser, hvilket sikrer, at hændelser løbende gennemgås for muligheder for at styrke organisationens sikkerhedsniveau.	Vi har kontrolleret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at sikkerhedshændelser er gennemgået.	Ingen afvigelser noteret.
5.29	**Informationssikkerhed under driftsforstyrrelse** *Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.* itm8 | Cloud & Infrastructure har etableret forretningskontinuitetsplaner for at sikre, at organisationen kan opretholde informationssikkerhed og drift på et passende niveau under forstyrrelser.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at de bagvedliggende procedurer for beredskabsplanen er blevet gennemgået og godkendt af relevant personale.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.30	**IKT-parathed til understøttelse af business continuity** *IKT-parathed skal planlægges, implementeres, vedligeholdelse og testes på grundlag af mål for business continuity og IKT-kontinuitetskrav.* itm8 | Cloud & Infrastructure gennemfører årlige IKT-beredskabstests for at sikre, at forretningskontinuitetsplanerne effektivt understøtter de ønskede resultater, og at organisationen efterlever disse planer.	Vi har kontrolleret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, revideres og godkendes årligt. Vi har inspiceret, at IKT-beredskabstest er blevet gennemgået årligt og godkendt af passende personale.	Ingen afvigelser noteret.
5.31	**Juridiske, lovmæssige, regulatoriske og kontraktlige krav** *Juridiske, lovmæssige, regulatoriske og kontraktlige krav, der er relevante for informationssikkerhed, samt organisationens tilgang til overholdelse af disse krav, skal være identificeret, dokumenteret og opdateret.* itm8 | Cloud & Infrastructure har dokumenteret alle relevante juridiske, lovmæssige, regulatoriske og kontraktuelle krav relateret til informationssikkerhed, som organisationen skal overholde. Denne liste opdateres løbende for at sikre nøjagtighed.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at listen over juridiske, lovmæssige, regulatoriske og kontraktuelle krav er dokumenteret og listen er blevet gennemgået og godkendt af passende personale.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.34	**Privatlivsbeskyttelse og beskyttelse af personoplysninger** *Organisationen skal identificere og opfylde kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav.* itm8 | Cloud & Infrastructure har identificeret gældende krav til beskyttelse af privatliv og personoplysninger (PII) og har etableret passende kontroller og foranstaltninger for at sikre overholdelse af disse krav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at tilstrækkelige kontroller er på plads for at sikre dokumentation og vedligeholdelse af PII.	Ingen afvigelser noteret.
5.36	**Overensstemmelse med politikker, regler og standarder for informationssikkerhed** *Overensstemmelse med organisationens informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder skal vurderes regelmæssigt.* itm8 | Cloud & Infrastructure sikrer overholdelse af sin informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder, som regelmæssigt gennemgås. Ledelsen understøtter og håndterer opretholdelsen af denne compliance.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er implementeret procedurer der sikrer regelmæssig gennemgang af informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder af passende personale.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske foranstaltninger

Procedurer og kontroller sikrer, at ledelsesretning og støtte til informationssikkerhed blev leveret i overensstemmelse med forretningskrav og relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementering og drift af informationssikkerhed i organisationen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.37	**Dokumenterede driftsprocedurer** *Driftsprocedurer for informationsbehandlingsfaciliteter bør dokumenteres og gøres tilgængelige for medarbejdere, der har brug for dem.* itm8 | Cloud & Infrastructure has established and documented operating procedures to support and manage the operation of solutions and services pro-vided by the organization. This includes a platform for communication and ensuring availability of these procedures to employees with a work-related need.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret driftsprocedurer, og at disse skal opdateres mindst én gang årligt. Vi har kontrolleret, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at menneskelig ressourcesikkerhed er implementeret og effektiv før, under og efter ansættelsen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.1	**Screening** *Der skal udføres verifikation af alle jobansøgeres baggrund. Verifikationen bør foretages, inden de tiltræder i organisationen og løbende, under hensyntagen til love, forskrifter og etiske regler og skal vurderes i forhold til organisationens krav, klassifikationen af den information, der skal gives adgang til, og de relevante risici.* itm8 | Cloud & Infrastructure gennemfører screening af potentielle kandidater, herunder indhentning af straffeattester for alle medarbejdere. Medarbejdere skal løbende levere en ren straffeattest under deres ansættelse, hvilket itm8 indhenter hvert tredje år.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksterne konsulenter samt hvert tredje ansættelsesår. Vi har ved stikprøvevis inspektion påset, at der er erhvervet straffeattester inden ansættelsesstart for nyansatte.	Ingen afvigelser noteret.
6.2	**Ansættelsesvilkår og -betingelser** *Ansættelseskontrakterne skal beskrive medarbejdernes og organisationens ansvar for informationssikkerhed.* itm8 | Cloud & Infrastructure har fastlagt ansættelsesvilkår som en del af ansættelsesaftalen mellem medarbejderen og itm8. Disse vilkår omfatter forventninger om overholdelse af gældende informationssikkerhedsinitiativer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at menneskelig ressourcesikkerhed er implementeret og effektiv før, under og efter ansættelsen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.3	**Awareness, uddannelse og træning vedrørende informationssikkerhed** *Organisationens medarbejdere og relevante interessenter skal modtage passende awareness, uddannelse og træning vedrørende informationssikkerhed samt regelmæssige opdateringer om organisationens informationssikkerhedspolitik, emnespecifikke politikker og procedurer, hvor det er relevant for deres jobfunktion.* itm8 | Cloud & Infrastructure gennemfører kontinuerlige sikkerhedsbevidsthedsinitiativer baseret på en årlig plan og opkommende sikkerhedstrusler. Dette omfatter simuleringer af phishingforsøg og andre brudscenarier for at styrke medarbejderes praktiske erfaring. Desuden kræves det, at alle medarbejdere sætter sig ind i gældende informations-sikkerhedskrav og Informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås, samt at medarbejderne jævnligt skal gennemføre obligatoriske undervisningsforløb for at sikre, at virksomhedens sikkerhedskrav overholdes. Vi har inspiceret, at medarbejdere er introduceret til informationssikkerhedspolitikken.	Ingen afvigelser noteret.
6.5	**Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold** *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.* itm8 | Cloud & Infrastructure kommunikerer informationssikkerhedsansvar, der forbliver i kraft efter ophør eller ændring af ansættelse. Dette omfatter at underrette medarbejdere om deres fortsatte tavshedspligt efter deres ophør.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes en skriftlig bekræftelse på, at opsagte medarbejdere forstår deres forsatte forpligtelse i forbindelse med fratrædelse.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at menneskelig ressourcesikkerhed er implementeret og effektiv før, under og efter ansættelsen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.6	**Hemmeligholdelses- og fortrolighedsaftaler** *Hemmeligholdelses- og fortrolighedsaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejdere og andre interessenter.* itm8 | Cloud & Infrastructure etablerer fortrolighedsaftaler med sine medarbejdere som en del af de indledende, kontraktlige ansættelsesaftaler. Desuden kan nogle medarbejdere under deres ansættelse være underlagt yderligere fortrolighed eller tavshedspligt, hvis kunderne kræver det.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes fortrolighedsaftaler i forbindelse med nyansættelser.	Ingen afvigelser noteret.
6.7	**Distancearbejde** *Der skal være implementerede sikkerhedstiltag, når medarbejdere arbejder på afstand, for at beskytte information, der er adgang til, og som behandles eller lagres uden for organisationens lokaliteter.* itm8 | Cloud & Infrastructure har etableret og implementeret sikkerhedsforanstaltninger for medar-bejdere, der arbejder eksternt, for at sikre, at sikkerhedsniveauet er sammenligneligt med, når medarbejdere arbejder fra kontoret. Dette omfatter blandt andet oprettelse af VPN-forbindelser og sikring af, at alt følsomt arbejde udføres på virtuelle arbejdsstationer.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er implementeret passende sikkerhedsforanstaltninger for personale, der arbejder eksternt.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at menneskelig ressourcesikkerhed er implementeret og effektiv før, under og efter ansættelsen

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.8	**Indrapportering af informationssikkerhedshændelser** *Organisationen skal sørge for, at medarbejdere kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt via passende kanaler.* itm8 | Cloud & Infrastructure har etableret en mekanisme for medarbejdere til at rapportere observerede eller formodede informationssikkerheds hændelser. Proceduren for at anvende denne mekanisme er kommunikeret og gjort tilgængelig for alle medarbejdere.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Procedurer og kontroller sikrer, at fysisk sikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.2	**Fysisk adgangskontrol** *Sikrede områder skal beskyttes ved hjælp af passende adgangsforanstaltninger og adgangspunkter.* itm8 | Cloud & Infrastructure har etableret fysiske adgangskontroller for sikre områder, herunder id-kort, besøgsregistrering og konstant tilsyn med godkendte og bevilgede medarbejdere.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at itm8 har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.3	**Sikring af kontorer, lokaler og faciliteter** *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.* itm8 | Cloud & Infrastructure har implementeret fysisk sikkerhed i sine kontorer, herunder adgangspunkter tilgængelige via personlige ID-kort og PIN-koder, adskilte sikkerhedszoner og CCTV-overvågning.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at itm8 har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.4	**Fysisk sikkerhedsovervågning** *Lokaliteter skal overvåges løbende for uautoriseret fysisk adgang.* itm8 | Cloud & Infrastructure har etableret CCTV ved indgange til både kontorer og datacentre samt andre faciliteter, der behandler følsom information.	Vi har inspiceret, at CCTV er etableret ved alle indgange til både kontorer, datacentre og andre faciliteter, der behandler følsomme oplysninger.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Procedurer og kontroller sikrer, at fysisk sikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.6	**Arbejde i sikrede områder** *Sikkerhedsforhold for arbejde i sikrede områder skal tilrettelægges og implementeres.* itm8 | Cloud & Infrastructure har etableret procedurer og retningslinjer for arbejde i sikre områder for at sikre, at arbejdet udføres uden at bringe medarbejdere eller informationsejendomme i fare.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at relevante sikkerhedsforhold er etableret for at sikre medarbejdere samt informationsaktiver.	Ingen afvigelser noteret.
7.7	**Ryddeligt skrivebord og låst skærm** *Regler om at holde skriveborde ryddet for papir og bærbare lagringsmedier og om at holde skærme låst på informationsbehandlingsfaciliteter skal defineres og håndhæves på behørig vis.* itm8 | Cloud & Infrastructure har etableret en politik om ryddet skrivebord og låst skærm, der sikrer, at følsomme oplysninger ikke efterlades uden opsyn på kontoret, og at skærme og øvrige mobile enheder låses, når de efterlades uden opsyn.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har implementeret en politik om ryddet skrivebord og låst skærm.	Ingen afvigelser noteret.
7.8	**Placering og beskyttelse af udstyr** *Udstyr skal placeres på et sikkert og beskyttet sted.* itm8 | Cloud & Infrastructure har en politik for at sikre beskyttelse af kritisk udstyr.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har fastlagt retningslinjer for sikring mod brand, vand og varme. Vi har desuden ved inspektion påset, at itm8 har indhentet revisionserklæring fra en underleverandør for at sikre, at tilsvarende krav overholdes, på områder hvor der er sket outsourcing.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Procedurer og kontroller sikrer, at fysisk sikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.9	**Sikring af aktiver uden for organisationens områder** *Aktiver uden for organisationens lokationer skal beskyttes.* itm8 | Cloud & Infrastructure har etableret og kommunikeret regler for, hvordan aktiver skal beskyttes og håndteres, når de fjernes fra området.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret regler, der sikrer, at aktiver er beskyttet og håndteres korrekt, når de fjernes fra organisationens områder, samt at dette er godkendt.	Ingen afvigelser noteret.
7.10	**Lagringsmedier** *Lagringsmedier skal styres i hele deres livscyklus i forbindelse med anskaffelse, brug, transport og bortskaffelse i overensstemmelse med organisationens klassifikationssystem og krav til håndtering.* itm8 | Cloud & Infrastructure har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Ingen afvigelser noteret.
7.11	**Forsyningssikkerhed** *Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.* itm8 | Cloud & Infrastructure sikrer, at al udstyr vedligeholdes i overensstemmelse med producentens specifikationer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret en fuldt redundant infrastruktur med særskilt backup.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Procedurer og kontroller sikrer, at fysisk sikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.13	**Vedligeholdelse af udstyr** *Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.* itm8 | Cloud & Infrastructure sikrer, at al udstyr vedligeholdes i overensstemmelse med producentens specifikationer for at sikre tilgængelighed, integritet og fortrolighed. Derudover sikrer itm8, at dets partnere også overholder disse standarder.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret retningslinjer for, hvordan udstyr vedligeholdes korrekt.	Ingen afvigelser noteret.
7.14	**Sikker bortskaffelse eller genbrug af udstyr** *Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software slettes eller overskrives på forsvarlig vis inden bortskaffelse eller genbrug.* itm8 | Cloud & Infrastructure har implementeret retningslinjer for bortskaffelse eller genbrug af udstyr, hvilket sikrer, at lagermedier destrueres sikkert gennem certificerede leverandører.	Vi har inspiceret, at itm8 har implementeret procedurer for sikker bortskaffelse eller genbrug af udstyr. Vi har inspiceret at bortskaffelse eller genbrug af udstyr sker igennem en certificeret leverandør.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.1	**Brugerenheder** *Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, bør beskyttes.* itm8 | Cloud & Infrastructure har implementeret forskellige sikkerhedspolitikker for enheder, der anvendes af brugerne, for at sikre, at de er tilstrækkeligt beskyttet. Dette inkluderer blandt andet fjernsletning af harddiske, malwarebeskyttelse osv.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har implementeret en politik for brugerenheder.	Ingen afvigelser noteret.
8.2	**Privilegerede adgangsrettigheder** *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* itm8 har en politik for tildeling og begrænsning af privilegerede adgange. Brugere med privilegeret adgang har dedikerede konti til dette formål, og privilegeret brugertilgangsliste auditeres kvartalsvis.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har tilrettelagt formaliserede procedurer for brugeradministration og rettighedsstyring, og at disse også gælder for brugere med privilegerede rettigheder. Vi har inspiceret, at der for autorisationer, der tildeles medarbejdere, foreligger en begrundelse for det ønskede adgangsniveau og en godkendelse fra nærmeste chef. Vi har inspiceret, at privilegerede adgangsrettigheder er revideret på kvartalsbasis.	Ingen afvigelser noteret.
8.3	**Begrænset adgang til information** *Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.* itm8 | Cloud & Infrastructure begrænser adgangen til systemer og applikationer og sikrer, at kun medarbejdere med et arbejdsrelateret behov har de nødvendige tilladelser.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret en politik for begrænsning af adgange til systemer og applikationer til medarbejdere, der har et arbejdsbetinget behov.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.5	**Sikker autentifikation** *Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.* itm8 har etableret sikre autentifikationsteknologier til følsomme oplysninger, herunder multifaktorautentifikation (MFA).	Vi har inspiceret, at der er implementeret en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt. Vi har inspiceret, at de omfattede applikationer og systemer håndhæver sikre logonprocedurer.	Ingen afvigelser noteret.
8.6	**Kapacitetsstyring** *Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.* itm8 | Cloud & Infrastructure har en procedure for månedlig rapportering om driften, herunder kapaciteten i produktionsmiljøet. Automatisk overvågning af driftsmiljøet og relevante system parameter sikrer, at fremtidige kapacitetskrav opfyldes.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der hver måned sendes rapporter til kunden vedrørende driften i produktionsmiljøerne hos itm8. Vi har ligeledes påset, at kapaciteten overvåges på produktionssystemerne hos itm8, så fremtidige krav til kapaciteten overholdes.	Ingen afvigelser noteret.
8.7	**Beskyttelse mod malware** *Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.* itm8 | Cloud & Infrastructure har implementeret en procedure for at sikre, at antivirussoftware er operationelt på alle relevante systemer, med kontinuerlig overvågning på plads. Brugerbevidsthed støttes gennem itm8's awareness-platform, som giver medarbejderne viden om malwarebeskyttelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at medarbejdernes pc'er hos itm8 er beskyttet med antivirussoftware – og at denne er opdateret. Vi har inspiceret, at itm8 har etableret initiativer til brugerbevidsthed om beskyttelse mod malware til medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.8	**Styring af tekniske sårbarheder** *Der skal indhentes oplysninger om tekniske sårbarheder ved brug af informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende tiltag.* itm8 | Cloud & Infrastructure har en procedure for kontinuerligt at vurdere rapporterede sårbarheder, evaluere deres kritikalitet ved hjælp af flere kilder, og Træffe passende foranstaltninger i forhold til de tjenester, der leveres.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der løbende indhentes informationer om tekniske sårbarheder, samt at der træffes passende foranstaltninger til at håndtere eventuelle risici. Vi har ligeledes ved inspektion påset, at kritiske sårbarheder kommunikeres til samtlige relevante interessenter.	Ingen afvigelser noteret.
8.9	**Konfigurationsstyring** *Konfigurationer, herunder sikkerhedskonfigurationer, af hardware, software, tjenester og netværk bør etableres, dokumenteres, implementeres, overvåges og vurderes.* itm8 | Cloud & Infrastructure har etableret processer og procedurer for konfigurationsstyring for at sikre, at ændringer til hardware, software, tjenester og netværk håndteres og dokumenteres korrekt.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret procedurer for konfigurationsstyring, samt at konfigurationer håndteres i overensstemmelse med gældende procedurer.	Ingen afvigelser noteret.
8.10	**Sletning af information** *Information lagret i informationssystemer, enheder eller i andre lagringsmedier skal slettes, når der ikke længere er brug for den.* itm8 | Cloud & Infrastructure har etableret procedurer for sletning af information for at sikre, at ingen data opbevares længere end krævet af lovmæssige eller forretningsmæssige krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at sletning af oplysninger sker i overensstemmelse med itm8's procedurer herfor.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.13	**Backup af information** *Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.* itm8 | Cloud & Infrastructure udfører backup i overensstemmelse med itm8's bedste praksis eller kundernes forretningskrav. Backupopgaverne overvåges for at sikre kontinuerlig drift, og en "restore test" initieres løbende i løbet af året af itm8.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer serviceydelser, hvor backup er relevant. Vi har inspiceret, at der er foretaget en fuld gendannelsestest af it-miljøerne.	Ingen afvigelser noteret.
8.14	**Redundans i faciliteter til informationsbehandling** *Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.* itm8 | Cloud & Infrastructure har redundans i sine egne informationsbehandlingsfaciliteter og kan tilbyde yderligere redundans for at opfylde kundernes krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der etableret redundans på itm8's informationsbehandlingsfaciliteter samt på kundemiljøer i overensstemmelse med gældende kundekontrakter.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.15	**Logning** *Logge, der optegner aktiviteter, undtagelser, fejl og andre relevante hændelser, skal udarbejdes, opbevares, beskyttes og analyseres.* itm8 | Cloud & Infrastructure udfører "Security Information and Event Management" (SIEM) på sine egne systemer og for kunder som krævet. Logfiler optages for forskellige systemer på forskellige sikkerhedsniveauer med fuld adskillelse af roller i SIEM-systemet. Medarbejdere, der kan slette logdata, har ikke adgang til kundernes eller itm8's systemer. Al adgang til kundesystemer logges i vores CMDB, opbevares sikkert og opsættes til at revidere enhver ændring af informationen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at hændelseslogning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret. Vi har inspiceret, at adgang til kundedata bliver logget og opbevares sikkert. Vi har inspiceret, at itm8 har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov, og at der er implementeret tilstrækkelig funktionsadskillelse i adgange til logdata.	Ingen afvigelser noteret.
8.16	**Overvågning af aktiviteter** *Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerheds-incidents.* itm8 | Cloud & Infrastructure har implementeret et monitoreringssystem, der sikrer, at kundesystemer er operationelle, med alarmer for enhver unormal adfærd. Systemet overvåges 24/7.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at et overvågningssystem er implementeret, samt at dette er overvåget 24/7.	Ingen afvigelser noteret.
8.17	**Synkronisering af ure** *Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.* itm8 | Cloud & Infrastructure har synkroniseret alle relevante informationsbehandlingssystemer til en enkelt referencetidskilde.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har etableret en referencetidskilde for tidssynkronisering af alle relevante informationsbehandlingssystemer.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.19	**Softwareinstallation i test- og produktionssystemer:** At sikre integriteten af test- og produktionssystemer og forhindre udnyttelse af tekniske sårbarheder *Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallationer i test- og produktionssystemer.* itm8 | Cloud & Infrastructure har defineret en række standardimplementeringsbeskrivelser for softwareinstallationer. Disse standarder håndhæves på kundesystemer for at sikre sikker styring.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at softwareinstallationer håndteres hensigtsmæssigt og i overensstemmelse med gældende procedurer.	Vi har noteret at 2 Domain Controller ikke har været opdateret/patched jf. godkendte procedure. Vi har modtaget dokumentation efterfølgende at begge servere er opdateret med de seneste opdateringer. Ingen yderligere afvigelser noteret.
8.20	**Netværkssikkerhed** *Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.* itm8 | Cloud & Infrastructure har implementeret flere politikker for at sikre en sikker kommunikation, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsrelateret behov. Kommunikation mellem itm8 og kundesteder udføres af valide og gennemprøvede, sikre teknologier.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder: • om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra itm8's eget miljø • om fjernadgang er tildelt ved brug af tofaktorgodkendelse • om ændringer i netværksmiljøet i vores stikprøve er sket på kontrolleret vis i overensstemmelse med reglerne for ændringsstyring.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.22	**Segmentering af netværk** *Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.* itm8 | Cloud & Infrastructure adskiller kundenetværk i ét eller flere netværk baseret på behovet for adskillelse, hvilket sikrer, at kunder ikke kan få adgang til andre kundenetværk.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået den tekniske sikkerhedsarkitektur og ved stikprøvevis inspektion undersøgt, om der jf. retningslinjerne er etableret et passende sikkerhedsniveau, herunder: • om sikre zoner og kundemiljøer er adskilt fra itm8's eget miljø • om adgang til netværket er opdelt i relevante brugergrupper baseret på et arbejdsbetinget behov.	Ingen afvigelser noteret.
8.23	**Webfiltrering** *Adgang til eksterne websteder skal styres for at reducere eksponeringen for skadeligt indhold.* itm8 | Cloud & Infrastructure har implementeret webfiltreringsforanstaltninger for at beskytte mod og reducere eksponering for ondsindet indhold.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret webfiltreringsforanstaltninger.	Ingen afvigelser noteret.
8.24	**Brug af kryptografi** *Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.* itm8 | Cloud & Infrastructure har etableret politikker for brug af kryptografi, herunder regler for brug, valg af kryptografiske teknikker, implementering, vedligeholdelse og bortskaffelse.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret en passende brug af sikker kryptografi og nøglehåndtering.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og er effektiv

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.32	**Ændringsstyring** *Ændringer af informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.* itm8 | Cloud & Infrastructure har etableret og implementeret en change management-proces for at sikre, at alle ændringer til informationssystemer i produktionsmiljøer håndteres korrekt, undgår unødvendige konflikter og sikrer, at der er tilstrækkelige fallback-planer på plads.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 har udarbejdet procedurer for årlig gennemgang og opdatering af: • Hændelsesstyring • Problemstyring • Ændringsstyring • Styring af versioner og programrettelser • Brugeradministration.	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
2025-02-03 20:06:04 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-03 20:19:00 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 83.136.xxx.xxx
2025-02-03 20:20:08 UTC