



# itm8 A/S

**Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller for perioden fra 1. januar 2025 til 31. december 2025 i relation til ydelser fra itm8 | Managed Services til kunder**

**Februar 2026**



## Indhold

1. Ledelsens udtalelse.....	3
2. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres design, implementering og operationelle effektivitet .....	5
3. Serviceorganisationens systembeskrivelse .....	8
4. Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf .....	17

# 1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet af itm8 A/S (itm8) til brug for kunder, der har anvendt ydelser fra itm8 | Managed Services, 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 deres regnskaber.

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

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

itm8 bekræfter, at:

- a) Den medfølgende beskrivelse i afsnit 3 giver en hensigtsmæssig præsentation af ydelser fra itm8 | Managed Services, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2025 til 31. december 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
  - (i) Redegør for, hvordan generelle it-kontroller i relation til ydelser fra itm8 | Managed Services var designet 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 designet og implementeret til at nå disse mål
    - Kontroller, som vi med henvisning til ydelser fra itm8 | Managed Services har forudsat ville være implementeret af kunderne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
    - Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
    - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for generelle it-kontroller
  - (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til ydelser fra itm8 | Managed Services foretaget i perioden fra 1. januar 2025 til 31. december 2025
  - (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af generelle it-kontroller i relation til ydelser fra itm8 | Managed Services, der er beskrevet, 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 alle aspekter ved generelle it-kontroller i relation til ydelser fra itm8 | Managed Services, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt designet og implementeret og var operationelt effektive i hele perioden fra 1. januar 2025 til 31. december 2025. 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
- (iii) Kontrollerne var anvendt konsistent som designet og implementeret, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2025 til 31. december 2025.

Herning, 17. februar 2026  
**itm8 A/S**

Frank Bech Jensen  
Head of Compliance and Security

## 2. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres design, implementering og operationelle effektivitet

**Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller for perioden fra 1. januar 2025 til 31. december 2025 i relation til ydelser fra itm8 | Managed Services til kunder**

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

### Omfang

Vi har fået som opgave at afgive erklæring om itm8's beskrivelse i afsnit 3 af generelle it-kontroller i relation til ydelser fra itm8 | Managed Services, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2025 til 31. december 2025 (beskrivelsen), og om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

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

### itm8's ansvar

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

### Revisors uafhængighed og kvalitetsstyring

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

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

### Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om hensigtsmæssigheden af præsentationen af itm8's beskrivelse samt om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som 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 hensigtsmæssigt præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og implementeret og er operationelt effektive.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen af en serviceleverandørs system og om designet, implementeringen og den operationelle effektivitet af kontroller hos en serviceleverandør, omfatter udførelse af handlinger for at opnå bevis for beskrivelsen samt for kontrollerens design, implementering og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er hensigtsmæssigt præsenteret, og at kontrollerne ikke er hensigtsmæssigt designet og implementeret og ikke er operationelt effektive. Vores handlinger har også 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 mål samt relevansen af de kriterier, som itm8 har specificeret og beskrevet i afsnit 1.

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

## Iboende begrænsninger

itm8's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle aspekter ved ydelser fra itm8 | Managed Services, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør eller serviceunderleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser i ydelser fra itm8 | Managed Services. Herudover er fremskrivningen til fremtidige perioder af enhver vurdering af hensigtsmæssigheden af præsentationen af beskrivelsen, eller af konklusioner om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af de kontroller, der er nødvendige for at nå de tilhørende kontrolmål, undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

## Konklusion

På baggrund af kriterierne og de kontrolmål, der er beskrevet i itm8's udtalelse i afsnit 1, er det vores opfattelse:

- a) at beskrivelsen af generelle it-kontroller i relation til ydelser fra itm8 | Managed Services, som designet og implementeret i hele perioden fra 1. januar 2025 til 31. december 2025, i alle væsentlige henseender er hensigtsmæssigt præsenteret
- b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret med henblik på at opnå høj grad af sikkerhed for, at de anførte kontrolmål ville være opnået, hvis de beskrevne kontroller var operationelt effektive i hele perioden fra 1. januar 2025 til 31. december 2025, og hvis kunderne udførte de komplementære kontroller, der er omtalt i afsnit 3
- c) at de testede kontroller i alle væsentlige henseender har fungeret effektivt i hele perioden fra 1. januar 2025 til 31. december 2025. De testede kontroller var de kontroller, som sammen med de komplementære kundekontroller omtalt i afsnit 3, forudsat at de var operationelt effektive, var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået.

## Beskrivelse af test af kontroller

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

## Tiltænkte brugere og formål

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



Vi tillader kun, at itm8 – efter eget skøn – offentliggør denne erklæring i dens fulde længde, herunder beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf. Offentliggørelse må kun ske til kunder, der har anvendt ydelser fra itm8 | Managed Services i hele eller dele af perioden fra 1. januar 2025 til 31. december 2025, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information om kontroller, som kunderne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. PwC påtager sig intet ansvar over for kunderne eller deres revisorer.

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

Aarhus, 17. februar 2026

**PricewaterhouseCoopers**

Statsautoriseret Revisionspartnerselskab

CVR-nr. 33 77 12 31

Jesper Parsberg Madsen  
statsautoriseret revisor  
mne26801

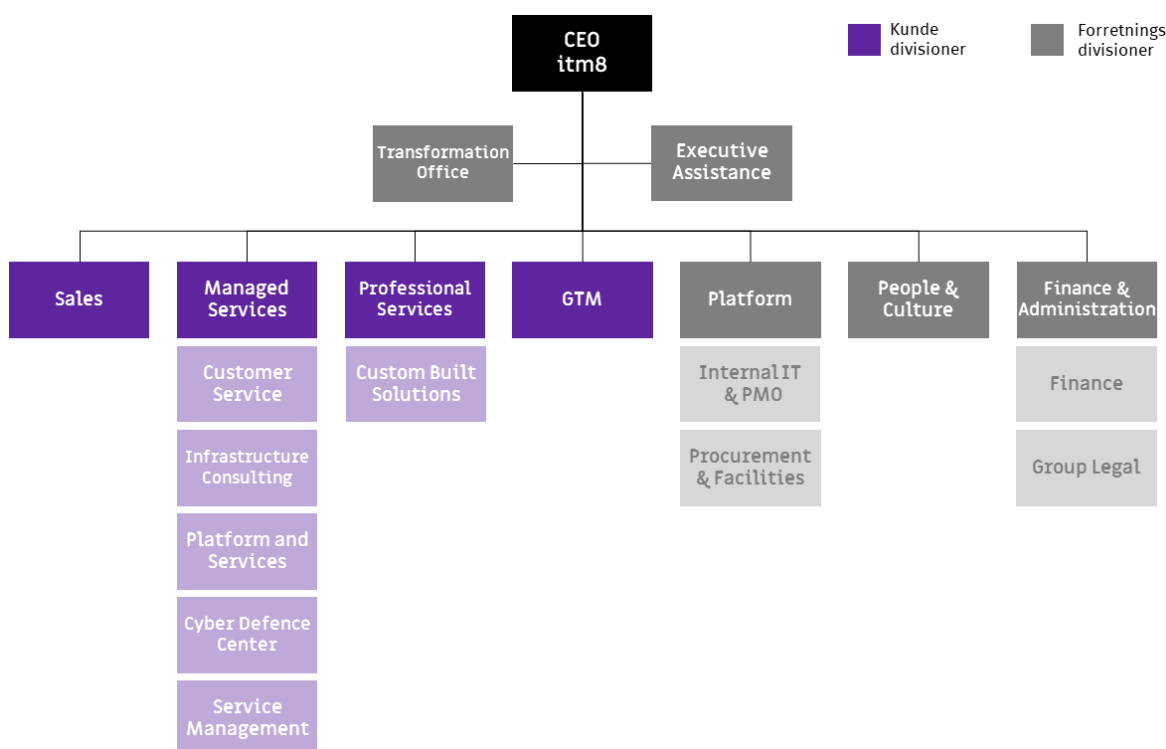
Iraj Bastar  
director

## 3. Serviceorganisationens systembeskrivelse

### 3.1. Beskrivelse af serviceorganisationen

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

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



Omfang af itm8 | Managed Services ISAE 3402 uafhængig revisorerklæring

Denne uafhængige revisionserklæring fokuserer på itm8 Managed Services, som er den centrale del af rapportens omfang. Divisionen tilbyder cloud-løsninger og it-infrastruktur-tjenester, der lever op til itm8's standarder for sikker og kvalitetsorienteret servicelevering. En vigtig del af disse leverancer er elementer fra itm8 Cybersecurity, herunder Cyber Defense Center, der spiller en afgørende rolle med 24/7-overvågning, SIEM-loghåndtering og hændeshåndtering, som alle er kritiske for infrastrukturens sikkerhed.

Derudover inddrages komponenter fra itm8 Professional Services, Custom Built Solutions, der udvikler skræddersyede løsninger som SEPO Send Sikker og Tandlægejournalssystemet TK2. Disse specialiserede løsninger understøtter itm8's forpligtelse til at levere sikre og tilpassede tjenester, der imødekommer kundernes unikke behov.

#### Kundedivisioner

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

- **itm8 | Managed Services**

Med fokus på cloud-løsninger og it-infrastruktur hjælper denne division kunder med at implementere robuste hosting- og driftsstrategier. Divisionen omsætter kundernes forretningsstrategier til skalerbare cloud- og infrastrukturløsninger gennem platformsevalueringer, design af sikkerhedspolitikker, migrationer, modernisering og 24/7-support.

Managed Services leverer services til kunder inden for servicedesk, drift, applikationsdrift og konsulent-ydelser. Managed Services indeholder desuden Cyber Defense Center, som er en afdeling, der tilbyder omfattende sikkerhedstjenester som bl.a. løbende SIEM-loghåndtering, sårbarhedsvurderinger og realtidshændelseshåndtering via et 24X7 Security Operation Center.

- **itm8 | Professional Services | Custom Built Solutions**

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-plattformen og Tandlægejournalssystemet (TK2), for at optimere forretningsprocesser.

## Forretningsdivisioner

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

Sammen skaber disse divisioner en robust struktur, der gør itm8 i stand til at levere specialiserede højkvalitets-tjenester, der understøtter kundernes strategiske mål.

## 3.2. Informationssikkerhedsledelsessystem

Ledelsessystemet for informationssikkerhed (ISMS) hos itm8 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 interessenterne 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 hjørnesteen i vores ISMS. Topleddelsen har defineret og godkendt en hensigtsmæssig og effektiv informationssikkerhedspolitik, der fastlægger organisationens mål omkring informationssikkerhed 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 risici 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 strenge 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 al drift 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 ISO 27001, nye og ændrede forretningsbehov samt hele tiden imødegå det aktuelle trusselsbillede. Resultaterne bruges til løbende forbedring og sikrer, at vores ISMS forbliver effektivt og opdateret.

**Forbedring:**

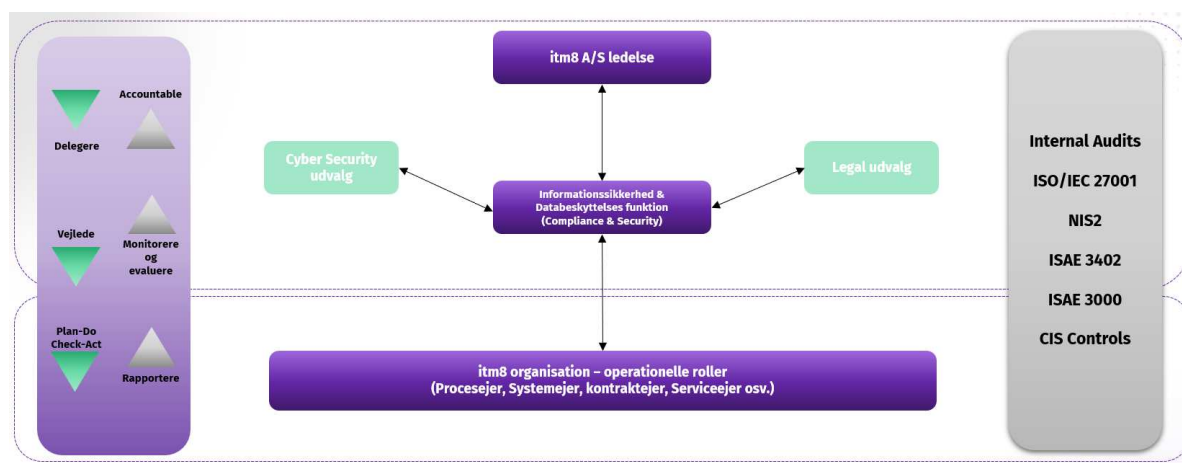
Løbende forbedring er integreret i vores ISMS gennem kvartalsvise møder om kontinuerlig forbedring (CIM) i Compliance & Security-teamet. Disse møder, hvor der føres officielle referater, giver en platform for at diskutere alle aspekter af informationssikkerhed hos itm8. Indsigter fra møderne, interne audit 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.

### 3.3. Informationssikkerhedsstyring

Informationssikkerhedsstyring hos itm8 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 informationssikkerhedsmål og understøttes af 15 emnespecifikke politikker. Disse politikker dækker områder som adgangskontrol, aktivstyring, forretningskontinuitet og hændelsehåndtering 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 Cyber security- og Legal-kommissionerne for at håndtere tekniske og juridiske sikkerhedsaspekter.



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 risikobaseret tilgang til styring af projekter, 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.

### 3.4. Styring af aktiver

itm8 administrerer sine informationer og tilknyttede aktiver i overensstemmelse med ISO/IEC 27001:2022-standarden. Vi opretholder aktivfortegnelser via forskellige databaser, herunder en primær CMDB til CI'er og kundevedtede løsninger samt InTune MDM til administration af brugerenheder. 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 brugerenheder og kundevedtede platforme som servere.

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

### 3.5. Informationsbeskyttelse

Hos itm8 sikrer vi effektiv informationsbeskyttelse i overensstemmelse med ISO/IEC 27001:2022-kontroller. Vi har etableret et klassifikationskema 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 standard-systemdesign 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.

### 3.6. HR-sikkerhed

Human resources-sikkerhed hos itm8 håndteres i overensstemmelse med ISO/IEC 27001:2022 for at sikre, at alt personale er tilstrækkeligt vurderet, uddannet og holdt ansvarlige for deres roller i informationssikkerhed. Vi gennemfører baggrundstjek af medarbejdere ved ansættelse, hvilket inkluderer indhentning af en ren straffeattest for kritisk personale. 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 hemmeligholdsftaler 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.

### 3.7. Security awareness

itm8 arbejder med strukturerede programmer for medarbejdere angående træning og test inden for sikkerhed. Programmerne starter ved ansættelse som en onboarding-forløb, og fortsætter herefter kontinuerligt med fast planlagte træningsmoduler og afprøvning af organisationens modstandsdygtighed mod phishingmail.

Træning består af en kombination af standardsikkerhedstræning og tilpasset træning, som er målrettet itm8's egne retningslinjer og krav.

### 3.8. Fysisk sikkerhed

itm8 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, pinkoder og alarmsystemer og tv-overvågning 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 skriveborde og låste skærme håndhæves, og forventningerne kommunikerer 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 nødgeneratorer 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.

### 3.9. System- og netværkssikkerhed

System- og netværkssikkerhed hos itm8 håndteres i overensstemmelse med ISO/IEC 27001:2022 for at sikre et sikkert driftsmiljø for både interne 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 al drift.

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 segregere miljøer, der er skræddersyet til at beskytte både produktions- og kontornetværk. Netværkstjenester opsættes sikkert, i overensstemmelse med bedste praksis og kundefaletter, 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 i CAB-møder for at sikre, at potentielle virkninger bliver fuldt ud vurderet og afbødet, hvilket opretholder sikkerheden og stabiliteten af vores systemer og netværk.

### 3.10. Applikationssikkerhed

itm8 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.

### 3.11. Sikker konfiguration

Vi har en konfigurationsstyringsproces, der understøttes af en centraliseret CMDB, som bruges til at administrere alle konfigurationsenheder (CI'er) 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.

### 3.12. Identitets- og adgangsstyring

Hos itm8 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 multifaktorautentifikation (MFA), hvor det er kritisk for at øge sikkerheden.

### 3.13. 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 teknologejere for at sikre rettidig identifikation og afhjælpning af sårbarheder.

### 3.14. 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 det oprindelige produktionsmiljø for at sikre deres tilgængelighed, selv under store forstyrrelser.

### 3.15. Sikkerhed i leverandørforhold

Hos itm8 håndterer vi leverandørforhold med stærkt fokus på informationssikkerhed. Vores aftaler med leverandører inkluderer ofte sikkerhedsaddenda, hvor det er muligt og relevant, og vi overvåger aktivt leverandørernes operationer 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.

### 3.16. 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 ejendomsretter (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 anvender erfaringerne, observationer og tilbagemelding fra audit som en del af vores forbedringsproces og sikrer, at disse behandles og adresseres i organisationen.

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.

### 3.17. Håndtering af informationssikkerhedshændelser

Vi håndterer informationssikkerhedshændelser gennem en struktureret proces for hændeshåndtering, 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 hændeshåndtering 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 på vores Continuous Improvement Meetings, der finder sted hver anden måned.

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

Som en del af behandlingen af informationssikkerhedshændelser anvendes lessons-learned for at sikre en læring ud fra hændelsen med henblik på at skabe forbedringer, der kan nedsætte risikoen for, at lignende hændelser opstår.

Som afslutning er det væsentligt at understrege, at arbejdet med compliance og informationssikkerhed er en løbende proces, hvor kontinuerlig forbedring er i centrum. itm8 forpligter sig til systematisk at evaluere og optimere eksisterende procedurer, så de altid lever op til gældende krav og bedste praksis.

Ved aktivt at inddrage erfaringer fra hændeshåndtering, interne og eksterne audit, samt ved at styrke medarbejdernes kompetencer og implementere relevante nøgletal, sikres et robust og fremtidssikret informationssikkerhedsniveau. Fremadrettet vil itm8 fortsætte med at investere i udvikling og forankring af en stærk compliance- og sikkerhedskultur, der kan imødegå nuværende og kommende udfordringer.

### 3.18. Væsentlige ændringer

Der har ikke været væsentlige ændringer til procedurer og kontroller i perioden fra 1. januar 2025 til 31. december 2025.

Kontrolmål og -aktiviteter fremgår detaljeret i afsnit 4.

### 3.19. Komplementære kontroller hos kunderne

#### Forhold, der skal overvejes af kundernes revisorer

##### Leverede serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på itm8's standardvilkår. Kundernes afvigelser fra itm8's 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 itm8's 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 administrator-adgangskode). 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 itm8's 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 operationelle effektivitet 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 den operationelle effektivitet 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.
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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.1	<p><b>Politikker for informationssikkerhed</b>  <i>Informationssikkerhedspolitikker og emnespecifikke politikker skal fastlægges, 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.</i></p> <p>itm8 har udarbejdet og dokumenteret en informationssikkerhedspolitik, der er godkendt af den øverste ledelse og distribueret til alle relevante medarbejdere. Derudover er der udarbejdet flere emnespecifikke politikker, som understøtter informationssikkerhedspolitikken og kommunikeres til alle relevante medarbejdere. Disse politikker gennemgås mindst en gang om året, eller når der sker væsentlige ændringer.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der forefindes en ledelsesgodkendt og ajourført sikkerhedspolitik.</p> <p>Vi har inspiceret, at informationssikkerhedspolitikkerne kommunikeres til medarbejderne og relevante parter og er revideret årligt.</p>	Ingen afvigelser noteret.
5.2	<p><b>Roller og ansvar i forbindelse med informationssikkerhed</b>  <i>Roller og ansvar i forbindelse med informationssikkerhed skal fastlægges og tildeles i overensstemmelse med organisationens behov.</i></p> <p>itm8 har fastlagt klart definerede roller og ansvarsområder, der er i overensstemmelse med kravene i virksomhedens informationssikkerhedsledelsessystem (ISMS). Disse roller er tildelt på baggrund af organisationens behov for at sikre en effektiv ledelse og overvågning af informationssikkerheden på tværs af virksomheden.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at de organisatoriske ansvarsområder er fastlagt og tildelt relevante personer.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.3	<p><b>Funktionsadskillelse</b>  <i>Modstridende funktioner og ansvarsområder skal adskilles.</i></p> <p>itm8 har udarbejdet politikker for funktionsadskillelse, som sikrer, at modstridende ansvarsområder er korrekt adskilt. Disse politikker gennemgås mindst en gang om året, eller når der sker væsentlige ændringer, så de er i overensstemmelse med informationssikkerhedspolitikken, og så det nødvendige niveau af adskillelse opretholdes for at beskytte informationssikkerheden.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos itm8, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.</p>	Ingen afvigelser noteret.
5.4	<p><b>Ledelsens ansvar</b>  <i>Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.</i></p> <p>itm8 kræver, at ledelsen aktivt bakker op om og sætter sig ind i gældende informationssikkerhedsinitiativer. Ledelsen er også ansvarlig for at under vise medarbejderne i disse initiativer for at sikre, at organisationens informationssikkerhedspolitikker og -procedurer overholdes.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at ledelsen er bekendt med virksomhedens informationssikkerhedsinitiativer.</p>	Ingen afvigelser noteret.
5.5	<p><b>Kontakt med myndigheder</b>  <i>Organisationen skal etablere og opretholde kontakt med relevante myndigheder.</i></p> <p>itm8 har udarbejdet kommunikationsprocedurer for underretning af relevante myndigheder i tilfælde af en sikkerhedshændelse.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 har en kommunikationsprocedure for, hvordan der kommunikeres med relevante myndigheder i tilfælde af en sikkerhedshændelse.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.6	<p><b>Kontakt med særlige interessegrupper</b>  <i>Organisationen skal etablere og opretholde kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.</i>                      itm8 deltager i forskellige ekspertgrupper om diverse aspekter af informationssikkerhed for at forbedre grundlaget for informationssikkerhed i itm8 og indsamle viden om sårbarheder og relevante informationssikkerhedsinitiativer.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at itm8 har en kommunikationsprocedure for, hvordan der kommunikeres med relevante specialistgrupper i tilfælde af sikkerhedsbrud.</p>	Ingen afvigelser noteret.
5.7	<p><b>Underretning om trusler</b>  <i>Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretninger om trusler.</i>                      itm8 indsamler trusselsinformation fra forskellige kilder, herunder sårbarhedsrapporter, udvalgte nyhedskilder, leverandører, myndigheder og interessegrupper, for at understøtte risikobaseret beslutningstagning.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.                      Vi har inspiceret, at itm8 indhenter og analyserer information til brug for risikobaseret beslutningstagning.</p>	Ingen afvigelser noteret.
5.8	<p><b>Informationssikkerhed i projektledelsen</b>  <i>Informationssikkerhed skal integreres i projektledelsen.</i>                      itm8 har fastlagt procedurer for risikovurdering som en del af vores projektledelse for at håndtere informationssikkerhedsrisici før og under projektimplementeringen.</p>	<p>Vi har forespurgt om de procedurer og kontrolaktiviteter, der udføres.                      Vi har inspiceret, at der er etableret en politik for informationssikkerhed i projektledelsen.                      Endvidere har vi på stikprøvebasis inspiceret, at informationssikkerhed er indarbejdet i projektledelsen, og at itm8 har udført risikovurderinger som en integreret del af project management-processen.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.9	<p><b>Fortegnelse over informationsaktiver og understøttende aktiver</b></p> <p><i>Der skal udarbejdes og vedligeholdes en fortegnelse over informationsaktiver og understøttende aktiver, herunder ejere.</i></p> <p>itm8 har implementeret og vedligeholder flere konfigurationsstyringsdatabaser (CMDB'er), der er tilpasset arten af de aktiver, der er omfattet. Dette omfatter fortegnelse over brugerenheder, servere, netværksudstyr og databaser, som alle har tildelte ejere og relevante oplysninger knyttet til sig.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af fortegnelsen over aktiver.</p>	Ingen afvigelser noteret.
5.10	<p><b>Accepteret brug af informationsaktiver og understøttende aktiver</b></p> <p><i>Regler for accepteret brug og procedurer til håndtering af informationsaktiver og understøttende aktiver skal identificeres, dokumenteres og implementeres.</i></p> <p>itm8 har fastlagt og implementeret regler for accepteret brug af virksomhedens aktiver, som er dokumenteret i politikken for accepteret brug.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at passende kontroller er på plads for at sikre dokumentation og vedligeholdelse af beholdningen af aktiver, herunder accepteret brug af aktiver.</p>	Ingen afvigelser noteret.
5.11	<p><b>Tilbagelevering af aktiver</b></p> <p><i>Relevante medarbejdere og interessenter skal tilbagelevere alle organisationens aktiver, som de er i besiddelse af, når deres ansættelse, kontrakt eller aftale ændres eller ophører.</i></p> <p>itm8 har fastlagt procedurer for sikker tilbagelevering af aktiver ved ophør eller ændring af ansættelse for at sikre, at følsomme virksomhedsspecifikke oplysninger ikke forlader itm8.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har observeret, at der er etableret en procedure, som sikrer, at virksomhedens aktiver returneres ved medarbejderes fratrædelse.</p> <p>På baggrund af stikprøver af fratrådte medarbejdere observerede vi, at der foreligger dokumentation for bekræftelse af, at alle aktiver er blevet returneret ved fratrædelsen.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.12	<p><b>Klassificering af information</b></p> <p><i>Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.</i></p> <p>itm8 har etableret en dataklassificeringsordning, der omhandler, hvordan forskellige typer data skal klassificeres og håndteres i overensstemmelse med deres klassificering.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at itm8 har etableret en dataklassificeringsordning til klassificering af information.</p>	Ingen afvigelser noteret.
5.13	<p><b>Mærkning af information</b></p> <p><i>Et passende sæt procedurer til mærkning af information skal udarbejdes og implementeres i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.</i></p> <p>itm8 har en politik for mærkning af information i henhold til vores informationsklassifikationssystem.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at der opretholdes et klassifikationsskema, som er gjort tilgængeligt for medarbejdere.</p> <p>Vi har observeret endvidere, at klassifikationsskemaet er blevet gennemgået og godkendt.</p>	Ingen afvigelser noteret.
5.14	<p><b>Overførsel af information</b></p> <p><i>Der skal være fastlagt regler eller procedurer for eller aftaler om overførsel af information for alle former for overførselsfaciliteter i organisationen og mellem organisationen og andre parter.</i></p> <p>itm8 har fastlagt politikker og procedurer for overførsel af information, der sikrer, at information overføres via sikre og pålidelige kommunikationskanaler.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at en passende teknisk sikkerhedsarkitektur er blevet etableret i netværket, samt at der er fastlagt regler for overførsel af information.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.15	<p><b>Adgangsstyring</b></p> <p><i>Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til informationsaktiver og understøttende aktiver baseret på forretningsmæssige og informationssikkerhedsmæssige krav.</i></p> <p>itm8 har implementeret retningslinjer for adgang til egne og kunders systemer baseret på forretningsmæssige og informationssikkerhedsmæssige krav.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har kontrolleret, at retningslinjer for adgangskontrol er implementeret, gennemgået og godkendt.</p>	Ingen afvigelser noteret.
5.16	<p><b>Identitetsstyring</b></p> <p><i>Identiteters samlede livscyklus skal styres.</i></p> <p>itm8 styrer identiteter i deres samlede livscyklus fra registrering til afmelding for at sikre, at identiteter har passende og nødvendig adgang i forhold til deres funktion og intet andet.</p>	<p>Vi har forespurgt om de procedurer/ kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at procedurerne omfatter hele livscyklussen for en identitet.</p>	Ingen afvigelser noteret.
5.17	<p><b>Autentifikationsoplysninger</b></p> <p><i>Tildeling og styring af autentifikationsoplysninger skal ske gennem en styringsproces; herunder skal medarbejdere rådgives om passende håndtering af autentifikationsoplysninger.</i></p> <p>itm8 styrer og udfører tildeling af autentifikationsoplysninger gennem en kontrolleret styringsproces, der ligeledes sikrer, at oplysningerne genereres tilfældigt og er i overensstemmelse med organisationens politik for kompleksitet af autentifikationsoplysninger.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at itm8 har etableret formaliserede procedurer for håndtering af autentifikationsoplysninger, herunder brugernavne, passwords og certifikater.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.18	<p><b>Adgangsrettigheder</b></p> <p><i>Adgangsrettigheder til informationsaktiver og understøttende aktiver skal tilvejebringes, gennemgås, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for adgangsstyring.</i></p> <p>itm8 gennemgår regelmæssigt medarbejdernes privilegerede tekniske rettigheder i både interne og kundevendte systemer for at sikre, at de er passende i forhold til deres arbejdsbetingede behov. Ikke-teknisk privilegerede medarbejdere tildeles de nødvendige rettigheder til at bruge de interne systemer, og disse rettigheder tilpasses ved ændringer i ansættelse, overflytninger og opsigelser. Når en medarbejder forlader itm8, inddrages alle adgangsrettigheder.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen.</p> <p>Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.</p>	<p>Under vores revision har vi konstateret, at de udførte user management-kontroller ikke er registreret fyldestgørende i overensstemmelse med de gældende procedurer. Endvidere forelå der ikke dokumentation for alle gennemførte periodiske reviews af privilegerede brugeradgange for to management-domæner.</p> <p>Vi er informeret om, at kontrollerne er udført, men de er ikke dokumenteret. Vi har ikke i vores stikprøver konstateret afvigelser.</p> <p>Ingen yderligere afvigelser noteret.</p>
5.19	<p><b>Informationssikkerhed i leverandørforhold</b></p> <p><i>Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.</i></p> <p>itm8 har fastlagt procedurer for håndtering af sikkerhedsrisici relateret til leverandørers produkter og -tjenester, herunder årlige risikovurderinger og audit for at sikre, at leverandørerne fortsat opfylder organisationens sikkerhedskrav.</p>	<p>Vi har inspiceret, at der findes en formel og dokumenteret procedure, der sikrer, at nye eller genhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav.</p> <p>Vi har inspiceret, at der udarbejdes risikovurderinger med passende mellemrum på kritiske leverandører.</p> <p>Vi har inspiceret, at itm8 jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav.</p>	<p>Ingen afvigelser noteret.</p>

## 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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.20	<p><b>Håndtering af informationssikkerhed i leverandøraftaler</b></p> <p><i>Relevante informationssikkerhedskrav skal fastsættes og aftales med hver enkelt leverandør på baggrund af typen af leverandørforhold.</i></p> <p>itm8 har fastsat sikkerhedskrav til leverandører, som er indeholdt i de kontraktlige aftaler og de generelle vilkår og betingelser for leverandører, der samarbejder med itm8.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at der foreligger en formel og dokumenteret procedure til at sikre, at nye eller genforhandlede applikations- eller serviceleverandørkontrakter valideres i forhold til en liste over definerede informationssikkerhedskrav.</p>	Ingen afvigelser noteret.
5.21	<p><b>Styring af informationssikkerhed i forsyningskæden for informations- og kommunikationsteknologi (IKT)</b></p> <p><i>Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med forsyningskæden for IKT-produkter og -tjenester.</i></p> <p>itm8 har fastlagt procedurer for styring af sikkerhedsrisici forbundet med brugen af en leverandørs produkter og tjenester, som omfatter en årlig risikovurdering og audit af leverandører for at sikre, at leverandøren fortsat lever op til de sikkerhedskrav, itm8 forventer.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at der er etableret en formel og dokumenteret procedure, som sikrer, at nye eller genforhandlede kontrakter vedrørende applikationer eller tjenesteleverandører valideres op imod en fastlagt liste af informationssikkerhedskrav.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.22	<p><b>Overvågning, vurdering og ændringsstyring af leverandørydelser</b></p> <p><i>Organisationen skal regelmæssigt overvåge, vurdere, evaluere og styre ændringer i leverandørens informationssikkerhedspraksis og levering af ydelser.</i></p> <p>itm8 har fastlagt procedurer for håndtering af sikkerhedsrisici forbundet med leverandørers produkter og -tjenester, herunder årlige risikovurderinger og audit for at sikre overholdelse af organisationens sikkerhedskrav. Derudover håndteres eventuelle ændringer i leverandørtjenester, som påvirker kundemiljøer, tjenester eller infrastruktur, gennem itm8's proces for ændringsstyring.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>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.</p> <p>Vi har ved inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt.</p> <p>Vi har ved inspektion af stikprøver påset, at itm8 jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav.</p> <p>Vi har inspiceret, at tredjepartserklæringer for hovedleverandører er modtaget og behandlet af itm8.</p>	Ingen afvigelser noteret.
5.23	<p><b>Informationssikkerhed ved brug af cloud-tjenester</b></p> <p><i>Der skal fastlægges processer for anskaffelse, brug, styring og afslutning af brugen af cloud-tjenester i overensstemmelse med organisationens informationssikkerhedskrav.</i></p> <p>itm8 har fastlagt en strategi for anvendelse af cloud-tjenester, der er i overensstemmelse med organisationens informationssikkerhedskrav og omfatter processer for anskaffelse, styring og afslutning.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er etableret en strategi for brugen af cloud-tjenester.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.24	<p><b>Planlægning og forberedelse af hændelseshåndtering ved sikkerhedshændelser</b></p> <p><i>Organisationen skal planlægge og forberede sig på at håndtere informationssikkerhedshændelser ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedshændelser.</i></p> <p>itm8 har defineret og implementeret en plan for håndtering af informationssikkerhedshændelser, som omfatter en proces for hændelseshåndtering samt klart definerede roller og ansvar i forbindelse med håndtering af hændelser.</p>	<p>Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for håndtering af hændelser.</p> <p>Vi har inspiceret, at roller og ansvar i relation til processen for hændelseshåndtering er blevet kommunikeret til medarbejderne.</p>	Ingen afvigelser noteret.
5.25	<p><b>Vurdering af og beslutning om informationssikkerhedshændelser</b></p> <p><i>Organisationen skal vurdere informationssikkerhedshændelser og beslutte, om de skal kategoriseres som informationssikkerhedshændelser.</i></p> <p>itm8 har fastlagt procedurer for vurdering af informationssikkerhedsepisoder for at afgøre, om sådanne episoder skal klassificeres som sikkerhedshændelser.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at der er implementeret en formel og dokumenteret hændelsehåndteringsproces relateret til informationssikkerhedshændelser og -brud.</p> <p>Vi har inspiceret, at alle hændelser er blevet registreret, at nødvendige handlinger er blevet udført, og at løsningerne er dokumenteret i et hændelsehåndteringssystem samt rapporteret via Compliance &amp; Security.</p>	Ingen afvigelser noteret.
5.26	<p><b>Håndtering af informationssikkerhedshændelser</b></p> <p><i>Informationssikkerhedshændelser skal håndteres i overensstemmelse med de dokumenterede procedurer.</i></p> <p>itm8 har fastlagt procedurer for håndtering af informationssikkerhedshændelser.</p>	<p>Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelsehåndteringsproces.</p> <p>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.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.27	<p><b>Læring fra informationssikkerhedshændelser</b></p> <p><i>Den viden, der opnås i forbindelse med informationssikkerhedshændelser, skal anvendes til at styrke og forbedre informationssikkerhedsforanstaltningerne.</i></p> <p>itm8 har fastlagt procedurer for at lære af informationssikkerhedshændelser, hvilket sikrer, at hændelser løbende gennemgås for at finde muligheder for at forbedre organisationens sikkerhedsniveau.</p>	<p>Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelsehåndteringsproces.</p> <p>Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at sikkerhedshændelser er gennemgået.</p>	Ingen afvigelser noteret.
5.28	<p><b>Indsamling af bevismateriale</b></p> <p><i>Organisationen skal fastlægge og implementere procedurer til identifikation, indsamling, anskaffelse og opbevaring af bevismateriale i forbindelse med informationssikkerhedsepisoder.</i></p> <p>itm8 har fastlagt mekanismer og procedurer for indsamling af bevismateriale i forbindelse med informationssikkerhedsepisoder, så det sikres, at læring opnås på baggrund af korrekt bevismateriale.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at en formel proces for vurdering og analyse af informationssikkerhedshændelser opretholdes.</p> <p>Ud fra en stikprøve på to måneder har vi observeret, at Compliance &amp; Security gennemgår og analyserer hændelser, der er kategoriseret som informationssikkerhedshændelser.</p>	Ingen afvigelser noteret.
5.29	<p><b>Informationssikkerhed under driftsforstyrrelser</b></p> <p><i>Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.</i></p> <p>itm8 har udarbejdet forretningskontinuitetsplaner for at sikre, at organisationen kan opretholde informationssikkerhed og drift på et passende niveau under driftsforstyrrelser.</p>	<p>Vi har inspiceret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, gennemgås og godkendes en gang om året.</p> <p>Vi har inspiceret, at de bagvedliggende procedurer for forretningskontinuitetsplanen er blevet gennemgået og godkendt af relevant personale.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.30	<p><b>IKT-beredskab til understøttelse af forretningskontinuitet</b></p> <p><i>IKT-beredskab skal planlægges, implementeres, vedligeholdes og testes på baggrund af mål for forretningskontinuitet og krav til IKT-kontinuitet.</i></p> <p>itm8 gennemfører årlige IKT-beredskabstests for at sikre, at forretningskontinuitetsplanerne effektivt understøtter de ønskede resultater, og at organisationen efterlever disse planer.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, revideres og godkendes årligt.</p> <p>Vi har inspiceret, at IKT-beredskabstests er blevet gennemgået årligt og godkendt af passende personale.</p>	Ingen afvigelser noteret.
5.31	<p><b>Juridiske, lovmæssige, regulatoriske og kontraktlige krav</b></p> <p><i>Juridiske, lovmæssige, regulatoriske og kontraktlige krav, der er relevante for informationssikkerhed, samt organisationens tilgang til overholdelse af disse krav, skal være identificerede, dokumenterede og opdaterede.</i></p> <p>itm8 har dokumenteret alle de relevante juridiske, lovmæssige, regulatoriske og kontraktlige krav relateret til informationssikkerhed, som organisationen skal overholde. Denne liste opdateres løbende for at sikre nøjagtighed.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at der er etableret en formel politik for overholdelse af gældende lovgivning, som løbende vedligeholdes, revideres og godkendes.</p> <p>Vi har inspiceret, at listen over juridiske, lovmæssige, regulatoriske og kontraktlige krav er dokumenteret, og at listen er blevet gennemgået og godkendt af passende personale.</p>	Ingen afvigelser noteret.
5.32	<p><b>Immaterielle rettigheder</b></p> <p><i>Organisationen skal implementere passende procedurer for at beskytte sine immaterielle rettigheder.</i></p> <p>itm8 har en politik for beskyttelse af immaterielle rettigheder, som omfatter beskyttelse af både internt udviklede immaterielle rettigheder samt leverandørers, konkurrenters og øvrige relevante parter rettigheder.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at der er planlagt formelle møder med henblik på at undersøge relevant lovgivning og regulatoriske krav.</p> <p>Ud fra en stikprøve af møder har vi observeret, at møder vedrørende juridiske forhold er blevet afholdt.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.33	<p><b>Beskyttelse af fortegnelser</b></p> <p><i>Fortegnelser skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse.</i></p> <p>itm8 har fastlagt procedurer til beskyttelse af fortegnelser, fx logoplysninger, mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse. Procedureerne omfatter funktionsadskillelse, så medarbejdere, der har adgang til at slette logdata, ikke har adgang til kundernes og itm8's systemer.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at der opretholdes en dokumenthåndteringsprocedure, som gennemgås og godkendes.</p>	Ingen afvigelser noteret.
5.34	<p><b>Beskyttelse af privatliv og personoplysninger</b></p> <p><i>Organisationen skal identificere og opfylde kravene vedrørende beskyttelse af privatliv og personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav.</i></p> <p>itm8 har identificeret gældende krav vedrørende beskyttelse af privatliv og personoplysninger og har etableret passende kontroller og foranstaltninger til at opfylde disse krav.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at itm8 har fastsat krav til beskyttelse af privatliv og personoplysninger.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.35	<p><b>Uafhængig vurdering af informationssikkerhed</b></p> <p><i>Organisationens metode til styring af informationssikkerhed og implementeringen heraf, herunder personer, processer og teknologier, skal vurderes uafhængigt med planlagte mellemrum, eller når der sker væsentlige ændringer.</i></p> <p>itm8 får regelmæssigt foretaget audit udført af uafhængige eksterne parter, der både dækker overholdelse af standarder for informationssikkerhed og afgivelse af revisionserklæringer.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er planlagt formelle møder med henblik på at identificere og vurdere relevant lovgivning og regulatoriske krav.</p> <p>Vi har endvidere inspiceret, at der udføres intern revision af kontrollerne.</p>	Ingen afvigelser noteret.
5.36	<p><b>Overholdelse af politikker, regler og standarder for informationssikkerhed</b></p> <p><i>Overholdelse af organisationens informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder skal vurderes regelmæssigt.</i></p> <p>itm8 sikrer overholdelse af organisationens informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder, som gennemgås regelmæssigt. Ledelsen understøtter og håndterer opretholdelsen af denne overholdelse.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har observeret, at der er fastlagt formelle møder til gennemgang af politikker, regler, standarder osv.</p> <p>Vi har inspiceret, at der er implementeret procedurer, der sikrer regelmæssig gennemgang af informationssikkerhedspolitikken, de emnespecifikke politikker, regler og standarder af passende personale.</p>	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.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
5.37	<p><b>Dokumenterede driftsprocedurer</b>  <i>Driftsprocedurerne for faciliteter til informationsbehandling skal dokumenteres og stilles til rådighed for de medarbejdere, der har brug for dem.</i></p> <p>itm8 har udarbejdet og dokumenteret driftsprocedurer til understøttelse og styring af driften af de løsninger og tjenester, som organisationen leverer. Dette omfatter en platform for kommunikation samt sikring af, at procedurerne er tilgængelige for de medarbejdere, der har et arbejdsbetinget behov.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er udarbejdet driftsprocedurer, og at disse skal opdateres mindst én gang årligt.</p> <p>Vi har endvidere inspiceret, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.</p>	Ingen afvigelser noteret.

## Kontrolmål 6: Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at personalesikkerhed er implementeret og fungerer effektivt før, under og efter ansættelsen.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.1	<p><b>Screening</b></p> <p><i>Der skal udføres baggrundstjek af alle jobansøgere forud for ansættelse i organisationen og løbende i overensstemmelse med relevante love, forskrifter og etiske regler, og baggrundstjekket skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.</i></p> <p>itm8 gennemfører screening af potentielle kandidater, herunder indhentning af rene straffeattester for alle medarbejdere, der håndterer kundedata. Medarbejdere, der håndterer kundedata, skal kunne fremvise en ren straffeattest under deres ansættelse, og itm8 indhenter denne hvert tredje år.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksperter konsulenter samt hvert tredje ansættelsesår.</p> <p>Vi har inspiceret, at der er indhentet straffeattester inden ansættelsesstart for nyansatte.</p>	Ingen afvigelser noteret.
6.2	<p><b>Ansættelsesvilkår og -betingelser</b></p> <p><i>Ansættelseskontrakterne skal beskrive medarbejdernes og organisationens ansvar for informationssikkerhed.</i></p> <p>itm8 har fastlagt ansættelsesvilkår som en del af ansættelsesaftalen mellem medarbejderen og itm8. Disse vilkår omfatter forventninger om overholdelse af gældende informationssikkerhedsinitiativer.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås.</p>	Ingen afvigelser noteret.

## Kontrolmål 6: Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at personalesikkerhed er implementeret og fungerer effektivt før, under og efter ansættelsen.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.3	<p><b>Awareness, uddannelse og træning vedrørende informationssikkerhed</b></p> <p><i>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.</i></p> <p>itm8 gennemfører løbende forskellige awareness-initiativer vedrørende sikkerhed ud fra et årshjul og nye sikkerhedstrusler. Dette omfatter simuleringer af phishingforsøg for at forbedre medarbejdernes praktiske erfaring. Endvidere er alle medarbejdere forpligtet til at sætte sig ind i gældende informationssikkerhedskrav og informationssikkerhedspolitikken.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 afholder årlige awareness-initiativer vedrørende sikkerhed og regelmæssigt gennemfører kampagner om informationssikkerhed.</p> <p>Vi har inspiceret, at medarbejdere er introduceret til informationssikkerhedspolitikken.</p>	Ingen afvigelser noteret.
6.4	<p><b>Sanktioner</b></p> <p><i>Der skal være en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere og andre relevante interessenter, der har overtrådt informationssikkerhedspolitikken.</i></p> <p>itm8 har fastlagt en formel sanktionsproces for overtrædelser af informationssikkerhedspolitikkerne, som er indarbejdet i alle medarbejderkontrakter.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er etableret en formaliseret procedure, som beskriver den disciplinære proces.</p>	Ingen afvigelser noteret.

## Kontrolmål 6: Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at personalesikkerhed er implementeret og fungerer effektivt før, under og efter ansættelsen.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.5	<p><b>Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold</b></p> <p><i>Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.</i></p> <p>itm8 kommunikerer informationssikkerhedsansvar, som forbliver i kraft efter ophør eller ændring af ansættelsesforhold. Dette omfatter indhentning af skriftlig bekræftelse på, at den opsagte medarbejder forstår sin fortsatte forpligtelse.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der indhentes en skriftlig bekræftelse på, at opsagte medarbejdere forstår deres fortsatte forpligtelse i forbindelse med fratrædelse.</p>	Ingen afvigelser noteret.
6.6	<p><b>Fortroligheds- eller hemmeligholdelsesaftaler</b></p> <p><i>Fortroligheds- eller hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejderne og andre interessenter.</i></p> <p>itm8 indgår fortrolighedsaftaler med sine medarbejdere som en del af de indledende kontraktlige ansættelsesaftaler. Derudover kan nogle medarbejdere under deres ansættelse være underlagt yderligere fortroligheds- eller hemmeligholdelsesaftaler, hvis kunderne kræver det.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der underskrives en hemmeligholdelsesaftale i forbindelse med nyansættelser.</p>	Ingen afvigelser noteret.

## Kontrolmål 6: Personalerelaterede foranstaltninger

Procedurer og kontroller sikrer, at personalesikkerhed er implementeret og fungerer effektivt før, under og efter ansættelsen.

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
6.7	<p><b>Distancearbejde</b></p> <p><i>Der skal være implementerede sikkerhedstiltag, når medarbejdere arbejder på distancen, for at beskytte information, der er adgang til, og som behandles eller lagres uden for organisationens lokaltiteter.</i></p> <p>itm8 har fastlagt og implementeret sikkerhedsforanstaltninger for medarbejdere, der arbejder på distancen, for at sikre, at informationssikkerhedsniveauet svarer til, når medarbejderne arbejder fra kontoret. Dette omfatter blandt andet oprettelse af VPN-forbindelser.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er implementeret passende sikkerhedsforanstaltninger for medarbejdere, der arbejder på distancen.</p> <p>Vi har inspiceret, at adgang for medarbejdere, der arbejder på distancen, oprettes gennem VPN-forbindelser.</p>	Ingen afvigelser noteret.
6.8	<p><b>Indrapportering af informationssikkerhedshændelser</b></p> <p><i>Organisationen skal sørge for, at medarbejderne kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt via passende kanaler.</i></p> <p>itm8 har gjort det muligt for medarbejderne at indrapportere observerede eller formodede informationssikkerhedshændelser. Proceduren for denne indrapportering er kommunikeret til og gjort tilgængelig for alle medarbejdere.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at processen for hændelsehåndtering er blevet kommunikeret til og gjort tilgængelig for medarbejderne.</p>	Ingen afvigelser noteret.

## Kontrolmål 7: Fysiske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.1	<p><b>Fysisk områdesikring</b>  <i>Der skal defineres og anvendes områdesikring for at beskytte områder, der indeholder information og understøttende aktiver.</i>                      itm8 har etableret fysisk områdesikring for at beskytte områder, der indeholder information og aktiver, og kontroller er tilpasset områdets relevans og følsomhed.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har observeret, at itm8 har etableret passende fysisk områdesikring.                      Vi har endvidere inspiceret, at itm8 har implementeret passende adgangskontroller til beskyttelse af de fysiske faciliteter.</p>	Ingen afvigelser noteret.
7.2	<p><b>Fysisk adgangskontrol</b>  <i>Sikre områder skal beskyttes ved hjælp af passende adgangskontrol og adgangspunkter.</i>                      itm8 har etableret fysisk adgangskontrol til sikre områder, herunder ID-kort, og konstant tilsyn med godkendte og clearede medarbejdere.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har inspiceret, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes.                      Vi har inspiceret, at itm8 har etableret passende adgangskontrol for at beskytte de fysiske faciliteter.</p>	Ingen afvigelser noteret.
7.3	<p><b>Sikring af kontorer, lokaler og faciliteter</b>  <i>Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.</i>                      itm8 har implementeret fysisk sikkerhed på sine kontorer, herunder adgangspunkter, der kan passeres vha. personlige ID-kort og pinkoder, adskilte sikkerhedszoner og CCTV-overvågning.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har inspiceret, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes.                      Vi har inspiceret, at itm8 har etableret passende adgangskontrol for at beskytte de fysiske faciliteter.</p>	Ingen afvigelser noteret.
7.4	<p><b>Fysisk sikkerhedsovervågning</b>  <i>Lokaliteterne skal overvåges løbende for uautoriseret fysisk adgang.</i>                      itm8 har etableret CCTV i alle datacentre samt i udvalgte kontorbygninger på baggrund af en risikovurdering.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har inspiceret, at CCTV-overvågning er etableret ved indgange til kontorer, datacentre og øvrige faciliteter, hvor følsomme oplysninger behandles, og at dette er baseret på en risikovurdering.</p>	Ingen afvigelser noteret.

## Kontrolmål 7: Fysiske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.5	<p><b>Beskyttelse mod fysiske og miljømæssige trusler</b></p> <p><i>Der skal tilrettelægges og implementeres beskyttelse mod fysiske og miljømæssige trusler som fx naturkatastrofer og andre tilsigtede eller utilsigtede fysiske trusler mod infrastrukturen.</i></p> <p>itm8 har implementeret foranstaltninger i sikre områder for at beskytte mod fysiske og miljømæssige trusler.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har observeret, at itm8 har designet og implementeret foranstaltninger til beskyttelse af sikre områder mod fysiske og miljømæssige trusler.</p> <p>Vi har inspiceret, at passende fysiske og miljømæssige beskyttelsesforanstaltninger er etableret for at beskytte infrastrukturen.</p>	Ingen afvigelser noteret.
7.6	<p><b>Arbejde i sikre områder</b></p> <p><i>Der skal tilrettelægges og implementeres sikkerhedsforanstaltninger for arbejde i sikre områder.</i></p> <p>itm8 har fastlagt procedurer og retningslinjer for arbejde i sikre områder for at sikre, at arbejdet udføres uden at bringe medarbejdere eller informationsaktiver i fare.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at relevante sikkerhedsforanstaltninger er etableret for at sikre medarbejdere samt informationsaktiver.</p>	Ingen afvigelser noteret.
7.7	<p><b>Ryddeligt skrivebord og låst skærm</b></p> <p><i>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.</i></p> <p>itm8 har fastlagt 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.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 har implementeret en politik om ryddet skrivebord og låst skærm.</p>	Ingen afvigelser noteret.

## Kontrolmål 7: Fysiske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.8	<p><b>Placering og beskyttelse af udstyr</b>  <i>Udstyret skal placeres på et sikkert og beskyttet sted.</i>                      itm8 har en politik, der skal sikre beskyttelse af kritisk udstyr.</p>	<p>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 inspiceret, at itm8 har indhentet revisionserklæring fra en underleverandør for at sikre, at tilsvarende krav overholdes, på områder hvor der er sket outsourcing.</p>	Ingen afvigelser noteret.
7.9	<p><b>Sikring af aktiver uden for organisationens områder</b>  <i>Aktiver uden for organisationens område skal beskyttes.</i>                      itm8 har fastsat og kommunikeret regler for, hvordan aktiver skal beskyttes og håndteres, når de fjernes fra området.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at itm8 har fastsat retningslinjer, der sikrer, at det skal godkendes, når udstyr, information eller software fjernes fra organisationens område.</p>	Ingen afvigelser noteret.
7.10	<p><b>Lagringsmedier</b>  <i>Lagermedier skal styres i hele deres livscyklus i forbindelse med anskaffelse, brug, transport og bortskaffelse i overensstemmelse med organisationens klassifikationssystem og krav til håndtering.</i>                      itm8 har fastlagt og implementeret politikker og procedurer for håndtering af lagringsmedier gennem hele deres livscyklus.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at itm8 har fastlagt og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.</p>	Ingen afvigelser noteret.

## Kontrolmål 7: Fysiske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.11	<p><b>Forsyningssikkerhed</b>  <i>Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.</i>                      itm8 sikrer, at alt udstyr vedligeholdes i henhold til producentens specifikationer. Desuden sikrer itm8, at virksomhedens samarbejdspartnere gør det samme.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret itm8's egne datacenterfaciliteter for at bekræfte, at passende understøttende udstyr forefindes, og at dette udstyr vedligeholdes i henhold til de angivne vedligeholdelsesprocedurer.                      Vi har endvidere inspiceret, at itm8 har indhentet revisionserklæring fra en underleverandør for at sikre, at tilsvarende krav er opfyldt på områder, der er outsourcet.</p>	Ingen afvigelser noteret.
7.12	<p><b>Sikring af kabler</b>  <i>Kabler til strøm, data eller understøttende informationstjenester skal beskyttes mod aflytning, forstyrrelse og beskadigelse.</i>                      itm8 sikrer, at kabler til strøm, data eller understøttende informationstjeneste, beskyttes i henhold til deres følsomhed og beskyttes i henhold til producentens anbefalinger.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har observeret, at itm8 har implementeret foranstaltninger til beskyttelse af kabler, der forsyner med strøm, data og understøttende informationstjenester, i overensstemmelse med deres følsomhed og producenternes anbefalinger.                      Vi har inspiceret, at der er implementeret beskyttelse af kabelføring i relevante datacentre, og at itm8 indhenter og gennemgår revisionserklæringer fra samarbejdspartnere, der driver itm8's datacentre, for at sikre opfyldelse af kravene.</p>	Ingen afvigelser noteret.
7.13	<p><b>Vedligeholdelse af udstyr</b>  <i>Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.</i>                      itm8 sikrer, at alt udstyr vedligeholdes i henhold til producentens specifikationer.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at de relevante sikkerhedsforanstaltninger er implementeret for at sikre, at udstyr vedligeholdes korrekt.</p>	Ingen afvigelser noteret.

## Kontrolmål 7: Fysiske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
7.14	<p><b>Sikker bortskaffelse eller genbrug af udstyr</b>  <i>Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.</i></p> <p>itm8 har fastsat retningslinjer for bortskaffelse eller genbrug af udstyr, der sikrer, at lagringsmedier destrueres sikkert af certificerede leverandører, eller at alle databærende komponenter slettes sikkert, før udstyr returneres i henhold til garanti- eller serviceaftaler (fx Nutanix uden NRDK).</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 har implementeret procedurer for sikker bortskaffelse eller genbrug af udstyr.</p> <p>Vi har inspiceret, at bortskaffelse eller genbrug af udstyr sker igennem en certificeret leverandør.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.1	<p><b>Brugerenheder</b></p> <p><i>Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, skal beskyttes.</i></p> <p>itm8 har fastlagt sikkerhedspolitikker for brugerenheder, herunder funktioner til fjernsletning, beskyttelse mod malware og andre sikkerhedsforanstaltninger for at sikre tilstrækkelig beskyttelse.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 har fastlagt en politik for anvendelse og beskyttelse af brugerenheder, samt at itm8 har implementeret passende kontroller for beskyttelse af brugerenheder, herunder fjernsletning, malwarebeskyttelse og øvrige sikkerhedsforanstaltninger.</p>	Ingen afvigelser noteret.
8.2	<p><b>Privilegerede adgangsrettigheder</b></p> <p><i>Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.</i></p> <p>itm8 har en politik for tildeling og begrænsning af privilegeret adgang. Brugere med privilegeret adgang har særlige konti til dette formål, og listen over privilegerede brugeres adgang revideres hvert kvartal.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at itm8 har tilrettelagt formaliserede procedurer for brugeradministration.</p> <p>Vi har inspiceret, at der for privilegerede adgangsrettigheder, der tildeles medarbejdere, foreligger en begrundelse for det ønskede adgangsniveau og en godkendelse fra nærmeste chef.</p> <p>Vi har endvidere inspiceret, at privilegerede adgangsrettigheder revideres hvert kvartal.</p>	Ingen afvigelser noteret.
8.3	<p><b>Begrænset adgang til information</b></p> <p><i>Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.</i></p> <p>itm8 begrænser adgangen til systemer og applikationer og sikrer, at kun medarbejdere med et arbejdsbetinget behov har de nødvendige tilladelser.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er fastlagt en politik for begrænsning af adgang til systemer og applikationer til medarbejdere, der har et arbejdsbetinget behov.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.5	<p><b>Sikker autentifikation</b></p> <p><i>Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.</i></p> <p>itm8 har etableret sikre autentifikationsteknologier til følsomme oplysninger information, herunder multifaktorautentifikation (MFA).</p>	<p>Vi har inspiceret, at der er implementeret en formel politik for adgangsstyring, der fastlægger til-ladte tekniske autentifikationsløsninger.</p> <p>Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt.</p> <p>Vi har inspiceret, at adgang til kundemiljøet er sikret ved brug af multifaktorautentifikation.</p>	Ingen afvigelser noteret.
8.6	<p><b>Kapacitetsstyring</b></p> <p><i>Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.</i></p> <p>itm8 har procedurer for månedlig rapportering om driften, herunder kapaciteten i produktionsmiljøet. Automatisk overvågning af driftsmiljøet og relevante systemparametre sikrer, at fremtidige kapacitetskrav opfyldes.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der hver måned sendes rapporter til kunden vedrørende driften i produktionsmiljøerne hos itm8.</p> <p>Vi har ligeledes inspiceret, at kapaciteten på produktionssystemerne hos itm8 overvåges, så fremtidige krav til kapaciteten overholdes.</p>	Ingen afvigelser noteret.
8.7	<p><b>Beskyttelse mod malware</b></p> <p><i>Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.</i></p> <p>itm8 har implementeret procedurer for at sikre, at antivirussoftware er i drift på alle relevante systemer, og at der er løbende overvågning. Brugers bevidsthed understøttes af itm8's platform til sikkerhedsbevidsthed, som giver medarbejderne viden om malwareforsvar.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er installeret antivirussoftware på alle systemer, og at denne overvåges.</p> <p>Vi har endvidere inspiceret, at der er etableret initiativer til bevidsthed om beskyttelse mod malware til medarbejdere.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.8	<p><b>Styring af tekniske sårbarheder</b></p> <p><i>Der skal indhentes oplysninger om tekniske sårbarheder ved brug af informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og passende foranstaltninger skal træffes.</i></p> <p>itm8 har en procedure til løbende at vurdere indberettede sårbarheder, evaluere deres kritikalitet ved hjælp af flere kilder og træffe passende foranstaltninger i forhold til de tjenester, der leveres.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der rettidigt indhentes informationer om tekniske sårbarheder i informationssystemer, at de evalueres, samt at der iværksættes passende foranstaltninger til at håndtere den tilhørende risiko.</p> <p>Vi har ligeledes inspiceret, at kritiske sårbarheder kommunikerer til samtlige relevante interessenter.</p>	Ingen afvigelser noteret.
8.9	<p><b>Konfigurationsstyring</b></p> <p><i>Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.</i></p> <p>itm8 har fastlagt processer og procedurer for konfigurationsstyring for at sikre, at ændringer i konfigurationselementer håndteres og dokumenteres korrekt.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at ressourcer overvåges og tilpasses i overensstemmelse med gældende procedurer for konfigurationsstyring.</p>	Ingen afvigelser noteret.
8.10	<p><b>Sletning af information</b></p> <p>Information, der er lagret i informationssystemer, på enheder eller på andre lagringsmedier, skal slettes, når der ikke længere er brug for den.</p> <p>itm8 har fastlagt procedurer for sletning af oplysninger for at sikre, at ingen data opbevares længere end krævet af lovgivningsmæssige eller forretningsmæssige krav.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at sletning af oplysninger sker i overensstemmelse med itm8's procedurer herfor.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.11	<p><b>Datamaskering</b></p> <p><i>Datamaskering skal anvendes i overensstemmelse med organisationens emnespecifikke politik for administration af adgang og andre relaterede emnespecifikke politikker og forretningskrav under hensyntagen til gældende lovgivning.</i></p> <p>itm8 har fastlagt procedurer for brug af datamaskering, når følsomme data bruges til test- eller udviklingsformål eller generelt skal fjernes fra beskyttede produktionsmiljøer.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Ved inspektion observerede vi, at itm8 har implementeret procedurer for intern kopiering af kundedata til udviklings- og testformål.</p>	Ingen afvigelser noteret.
8.12	<p><b>Forebyggelse af datalækage</b></p> <p><i>Der skal iværksættes tiltag til at forebygge datalækage i systemer, netværk og andre enheder, der behandler, lagrer eller transmitterer følsom information.</i></p> <p>itm8 har etableret systemer til forebyggelse af datalækage, der overvåger systemer, netværk og enheder for mulig datalækage.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.</p> <p>Vi har inspiceret, at firewallregler er implementeret for at begrænse serveres adgang til internettet.</p> <p>Vi har inspiceret, at diskryptering er implementeret på brugerenheder, og at disse enheder overvåges med henblik på potentiel datalækage.</p> <p>Vi har inspiceret, at kryptering er implementeret for følsomme data, der lagres på servere.</p>	Ingen afvigelser noteret.
8.13	<p><b>Backup af information</b></p> <p><i>Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.</i></p> <p>itm8 udfører backup i overensstemmelse med itm8's bedste praksis eller kundernes forretningskrav. Backupjobbene overvåges for at sikre kontinuerlig drift, og en årlig gendannelsestest igangsættes af itm8.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer serviceydelser, hvor backup er relevant.</p> <p>Vi har inspiceret, at der er foretaget en fuld gendannelsestest af it-miljøerne.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.14	<p><b>Redundans i faciliteter til informationsbehandling</b></p> <p><i>Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.</i></p> <p>itm8 har redundans i sine egne informationsbehandlingsfaciliteter og kan levere yderligere redundans for at opfylde kundernes krav.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er etableret redundans på itm8's informationsbehandlingsfaciliteter samt på kundemiljøer i overensstemmelse med gældende kundekontrakter.</p>	Ingen afvigelser noteret.
8.15	<p><b>Logning</b></p> <p><i>Logge, der registrerer aktiviteter, undtagelser, fejl og andre relevante hændelser, skal udarbejdes, opbevares, beskyttes og analyseres.</i></p> <p>itm8 udfører central og intelligent logning (SIEM) på sine egne systemer og for kunder efter behov. Der registreres logfiler for forskellige systemer på forskellige sikkerhedsniveauer. Logfiler kan ikke ændres.</p> <p>Al adgang til kundesystemer logges i systemet til styring af aktiver, opbevares sikkert og sættes op til at revidere ethvert forsøg på at ændre oplysningerne.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at logning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret.</p> <p>Vi har inspiceret, at adgang til kundedata bliver logget.</p> <p>Vi har endvidere inspiceret, at der er implementeret tilstrækkelig funktionsadskillelse i logsystemerne.</p>	Ingen afvigelser noteret.
8.16	<p><b>Overvågning af aktiviteter</b></p> <p><i>Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerhedshændelser.</i></p> <p>itm8 har implementeret et overvågningssystem, der sikrer, at kundesystemerne er i drift, og hvor der er alarmer i tilfælde af unormal adfærd. Systemet overvåges 24/7.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at et overvågningssystem er implementeret, samt at dette overvåges 24/7.</p>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.17	<p><b>Synkronisering af ure</b>  <i>Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.</i>                      itm8 har synkroniseret alle relevante informationsbehandlingssystemer ud fra en enkelt referencetidskilde.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at itm8 har fastsat en referencetidskilde til synkronisering af ure i alle relevante informationsbehandlingssystemer.</p>	Ingen afvigelser noteret.
8.18	<p><b>Brug af privilegerede understøttende programmer</b>  <i>Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.</i>                      itm8 har fastsat politikker for brugen af privilegerede understøttende programmer for at sikre, at disse ikke anvendes, medmindre der er et strengt arbejdsbetinget behov for dem.</p>	<p>Vi har forespurgt om de procedurer og kontrolaktiviteter, der udføres.                      Det er observeret, at adgang til servere sker via anvendelse af jump-hosts.                      Det er endvidere observeret, at hjælpeprogrammer (utility programs) kun kan tilgås af et begrænset antal godkendte brugere med et arbejdsbetinget behov.</p>	Ingen afvigelser noteret.
8.19	<p><b>Softwareinstallation på driftssystemer</b>  <i>Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallation på driftssystemer.</i>                      itm8 har fastsat en række standardbeskrivelser for softwareinstallation. Disse standarder håndhæves på kundesystemer for at sikre en sikker håndtering.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, at softwareinstallation på driftssystemer håndteres hensigtsmæssigt og i overensstemmelse med gældende procedurer.</p>	<p>Under vores gennemgang af en af de udvalgte kunders servermiljø, er det konstateret, at én ud af tre reviderede MSSQL-servere for den pågældende kunde ikke har været patchet tilstrækkeligt.</p> <p>Ingen yderligere afvigelser noteret.</p>

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.20	<p><b>Netværkssikkerhed</b>  <i>Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.</i>                      itm8 har implementeret flere politikker for at sikre, at kommunikationen er sikker, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsbetinget behov. Kommunikationen mellem itm8 og kundesites foregår ved hjælp af anerkendte og gennemprøvede sikre teknologier.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder:</p> <ul style="list-style-type: none"> <li>• om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra itm8's eget miljø</li> <li>• om fjernadgang er tildelt ved brug af tofaktor-godkendelse</li> <li>• om ændringer i netværksmiljøet i vores stikprøve er sket på kontrolleret vis i overensstemmelse med reglerne for ændringsstyring.</li> </ul>	Ingen afvigelser noteret.
8.21	<p><b>Sikring af netværkstjenester</b>  <i>Sikkerhedsmekanismer, serviceniveauer og servicekrav til netværkstjenester skal identificeres, implementeres og overvåges.</i>                      itm8 har identificeret sikkerhedsmekanismer, serviceniveauer og servicekrav for den netværkstjeneste, vi leverer og bruger, og som overvåges løbende.</p>	<p>Vi har forespurgt ledelsen om de udførte procedurer og kontrolaktiviteter.                      Vi har inspiceret, at der er etableret en hensigtsmæssig sikkerhedsarkitektur i netværket.</p>	Ingen afvigelser noteret.
8.22	<p><b>Segmentering af netværk</b>  <i>Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.</i>                      itm8 adskiller kundenetværk i et eller flere netværk alt efter behovet for adskillelse, hvilket sikrer, at kunderne ikke kan få adgang til andre kundenetværk.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.                      Vi har inspiceret den tekniske sikkerhedsarkitektur, og om der jf. retningslinjerne er etableret et passende sikkerhedsniveau, herunder:</p> <ul style="list-style-type: none"> <li>• om sikre zoner og kundemiljøer er adskilt fra itm8's eget miljø</li> <li>• om adgang til netværket er opdelt i relevante brugergrupper baseret på et arbejdsbetinget behov.</li> </ul>	Ingen afvigelser noteret.

## Kontrolmål 8: Tekniske foranstaltninger

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

No.	itm8's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
8.23	<p><b>Webfiltrering</b></p> <p><i>Adgang til eksterne websteder skal styres for at reducere eksponeringen for skadeligt indhold.</i></p> <p>itm8 har truffet foranstaltninger til webfiltrering for at beskytte mod og reducere eksponeringen for skadeligt indhold.</p>	<p>Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har inspiceret, at der er implementeret webfiltreringsforanstaltninger.</p>	Ingen afvigelser noteret.
8.24	<p><b>Brug af kryptografi</b></p> <p>Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.</p> <p>itm8 har fastsat politikker for brug af kryptografi, herunder regler for brug, valg af kryptografisk teknik, implementering, vedligeholdelse og bortskaffelse.</p>	<p>Vi har forespurgt om de udførte procedurer/kontrolaktiviteter.</p> <p>Vi har inspiceret, at der er fastsat en passende brug af kryptografi og administration af krypteringsnøgler.</p>	Ingen afvigelser noteret.
8.32	<p><b>Ændringsstyring</b></p> <p><i>Ændringer af informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.</i></p> <p>itm8 har fastlagt og implementeret en procedure for ændringsstyring for at sikre, at alle ændringer til informationssystemer i produktionsmiljøer håndteres korrekt, så unødvendige konflikter undgås, og det sikres, at der er etableret nødplaner.</p>	<p>Vi har inspiceret, at procedurerne for ændringsstyring er hensigtsmæssige, og at der er etableret et passende ændringsstyringssystem understøttet af en teknisk infrastruktur.</p> <p>Vi har inspiceret, at der er implementeret en formel procedure for ændringsstyring i organisationen.</p> <p>Endvidere har vi på stikprøvebasis inspiceret, at proceduren for ændringsstyring følges i praksis.</p>	<p>Under vores revision har vi konstateret, at det eksisterende proceduregrundlag for change management ikke har været fuldt dækkende på tværs af hele Managed Services, da der i perioden har været anvendt forskellige ITSM-systemer.</p> <p>Ingen yderligere afvigelser noteret.</p>

# PENNEO

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: 4ecd2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c  
IP: 193.169.xxx.xxx  
2026-02-17 12:35:44 UTC



## Jesper Parsberg Madsen

PRICEWATERHOUSECOOPERS STATS AUTORISERET  
REVISIONSPARTNERSELSKAB CVR: 33771231  
Statsautoriseret revisor

Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e  
IP: 87.49.xxx.xxx  
2026-02-17 12:55:00 UTC



## Iraj Bastar

PRICEWATERHOUSECOOPERS STATS AUTORISERET  
REVISIONSPARTNERSELSKAB CVR: 33771231

### PwC-medunderskriver

Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96  
IP: 208.127.xxx.xxx  
2026-02-17 13:05:11 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

### Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.