www.pwc.dk

itm8 Business Application Management

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2024 til 31. december 2024 i relation til itm8 Business Application Managements drifts- og hosting-ydelser

Februar 2025

pwc

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt itm8 Business Application Managements drifts- og hosting-ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i kunders regnskaber.

itm8 Business Application Management anvender Keepit som underdatabehandlere for backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Keepit varetager for itm8 Business Application Management.

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

itm8 Business Application Management bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af itm8 Business Application Managements drifts- og hosting-ydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2024 til 31. december 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til itm8 Business Application Managements drifts- og hosting-ydelser var udformet og implementeret, herunder redegør for:

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

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

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2024 til 31. december 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

København, den 19. februar 2025
itm8 Business Application Management

Johnny Klostergaard
CEO

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

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

Til: itm8 Business Application Management, itm8 Business Application Management's kunder og deres revisorer.

Omfang

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

itm8 Business Application Management anvender Keepit som underdatabehandlere for backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Keepit varetager for itm8 Business Application Management.

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

itm8 Business Application Managements ansvar

itm8 Business Application Management er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om itm8 Business Application Managements beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

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

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

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

Begrænsninger i kontroller hos en serviceleverandør

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

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

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

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

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

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

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

Aarhus, den 19. februar 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3 itm8 Business Application Managements systembeskrivelse

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for itm8 Business Application Managements kunder og deres revisorer i overensstemmelse med kravene i den danske revisionsstandard ISAE 3402 for erklæringsopgaver om kontroller hos en serviceleverandør. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret i forbindelse med itm8 Business Application Managements leverance af serviceydelser vedrørende drift og hosting.

Beskrivelsen indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at kunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet, i det omfang det kan medføre en risiko for væsentlige fejl i kunders it-drift i perioden fra 1. januar 2024 til 31. december 2024.

3.2 Beskrivelse af itm8 Business Application Managements ydelser

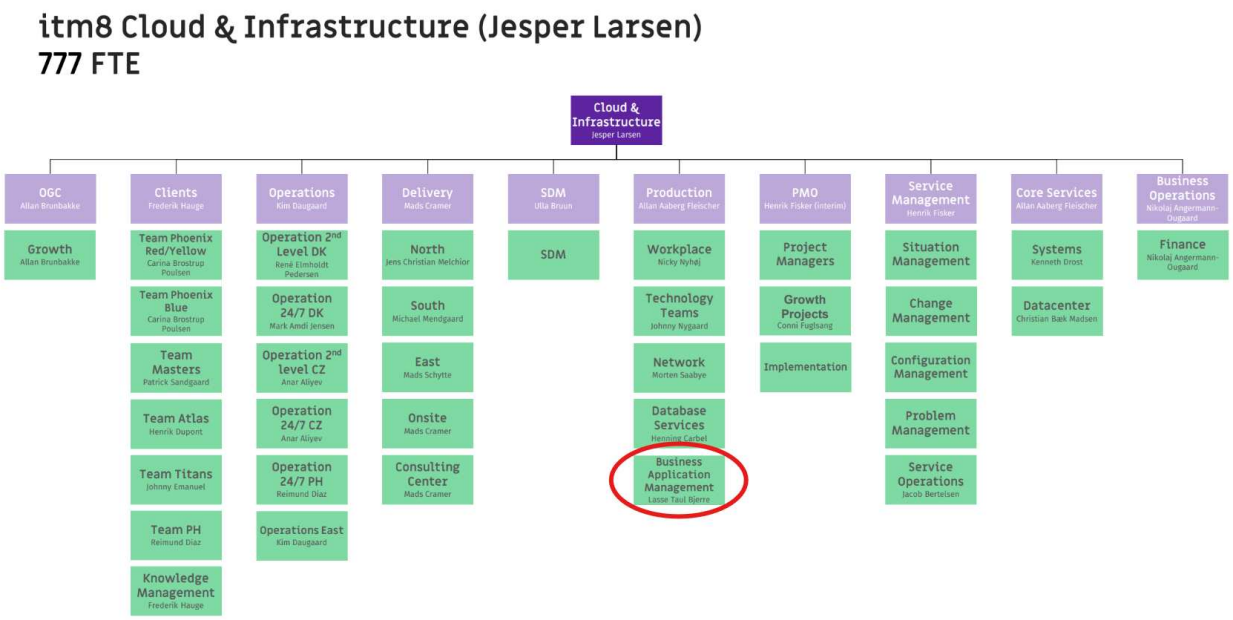
itm8 Business Application Management er en afdeling i koncernen itm8, som indtil 1. januar 2024 var et selvstændigt brand under navnet Miracle 42. itm8 leverer i dag en bred vifte af it-konsulentydelser til en lang række kunder med en samlet omsætning på mere end 2,4 mia. kr. itm8 Business Application Managements kerneydelser er hosting og konsulentvirksomhed inden for Microsoft og Oracle. Vores mangeårige erfaring med at drive store it-løsninger gør os i stand til at garantere meget høj kvalitet, sikkerhed og leverancestabilitet. I afdelingen er vi omkring 25 fastansatte medarbejdere, alle med en solid, teoretisk baggrund og praktisk erfaring inden for bl.a. drift, projektledelse, arkitektur, database og infrastruktur.

itm8 Business Application Management har indarbejdet processer og har fokuseret målrettet på it-drift siden 2011. itm8 Business Application Management forholder sig løbende til opbygning af gode processer inden for projektledelse, procesledelse, teknologiledelse, kompetencestyring samt styring og gennemførelse af it-projekter. itm8 Business Application Management har indarbejdet metoder, værktøjer og processer fra PRINCE2, DS 484/ISO 27001, ISAE 3402 og ITIL®.

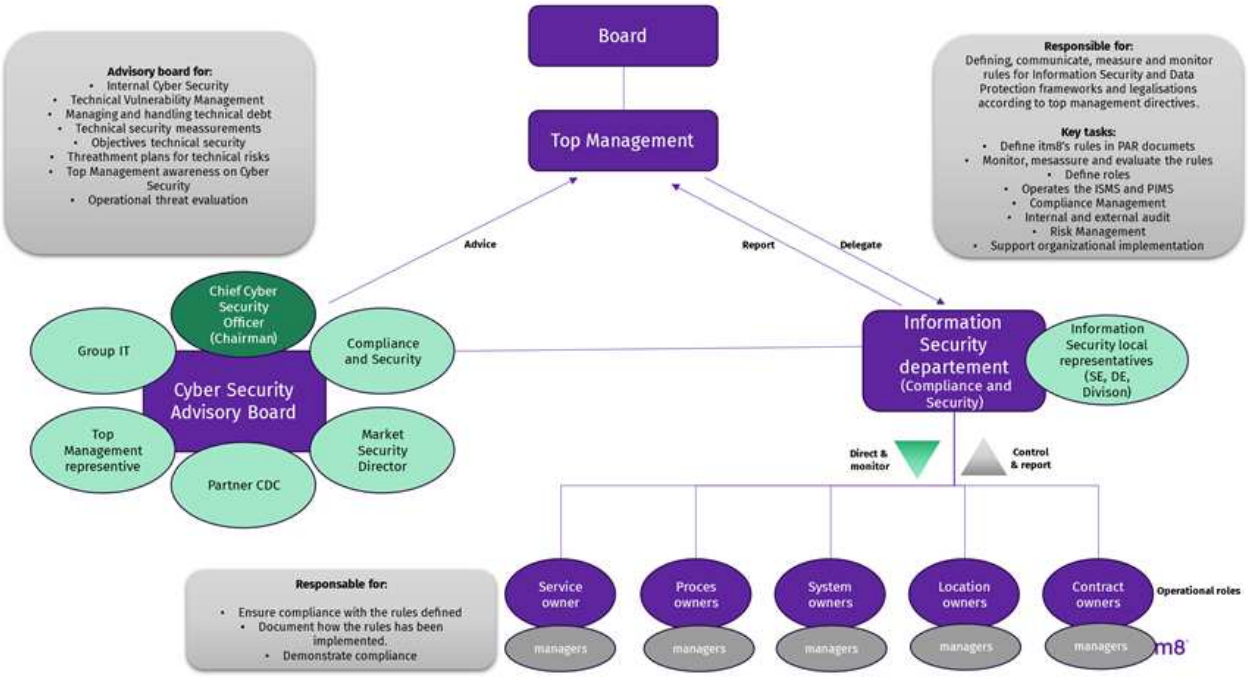
itm8 Business Application Management ser kvalitetsstyring som en løbende vurderingsproces integreret i løsningsvalg, dokumentation, projektledelse og de forskellige processer, der er i forbindelse med vedligehold, drift og support. Den bruges til at kontrollere og sikre kvaliteten af Serviceydelserne og til at sikre, at tidsplaner og budgetter overholdes, og at serviceydelserne implementeres korrekt hos kunden. Kvalitetsstyring skal identificere processuelle svagheder, rette op på de identificerede svagheder og kontinuerligt forbedre dem.

3.3 itm8 Business Application Managements organisation og sikkerhed

itm8 Business Application Management er en afdeling i koncernen itm8 i forretningsområdet Cloud & Infrastructure, der ledes af Jesper Larsen, Executive Partner med reference til Henrik Kastbjerg, CEO. Afdelingen ledes af Lasse Taul Bjerre, Director, med reference til Allan Aaberg Fleicher, Acquisitions Manager, M&A, og er organiseret som det fremgår af diagrammet. Afdelingen opererer under eget CVR-nummer og tegnes juridisk af Johnny Klostergaard.



itm8 har en fælles sikkerhedsorganisation, som Business Application Management er en del af, og befinder sig på det operationelle niveau i diagrammet herunder.



Direktionen i itm8, som er den øverst ansvarlige for it-sikkerheden, sørger for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelse af den til enhver tid gældende it-sikkerhedspolitik. Denne sikkerhedspolitik fastlægges af Information Security Department. I 2023 - 2024 er den fælles sikkerhedspolitik gradvist blevet indført i hele itm8 og er nu gældende politik for itm8 Business Application Management.

For at understøtte sikkerhedsorganisationens arbejde har itm8 Business Application Management etableret en it-sikkerhedsgruppe, som er ansvarlig for de overordnede målsætninger for implementering af it-sikkerhed i serviceydelserne. Det er direktøren for Operations, som er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollerbart, hvor dette overhovedet er muligt, og være et udtryk for "best practice" inden for

de enkelte kontrolaktiviteter på de serviceområder, som kunderne tilbydes. It-sikkerhedsgruppen består p.t. af følgende medlemmer:

- Lasse Taul Bjerre, IT-sikkerhedsansvarlig – labje@itm8.com
- Kenneth Holm – kenho@itm8.com
- Michael Byø-Boisen – miboi@itm8.com

Gruppen mødes jævnligt for at fastsætte og følge op på målsætninger vedr. it-sikkerheden.

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

3.4 Risikostyring ved itm8 Business Application Management

Risikostyring gennemføres hos itm8 Business Application Management på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der sigter mod interne systemer generelt. Input til denne vurdering indhentes i hele organisationen. Processen faciliteres af ansvarlige og ledere, der udarbejder et udkast til itm8 Business Application Managements ledelse. Efter intern bearbejdning godkendes vurderingen af itm8 Business Application Managements ledelse.

I projektindstillingsfasen udarbejdes der – afhængigt af projektets karakter – dels en sikkerhedsvurdering og dels en vurdering af særlige risici og usikkerheder. Dette sker efter en foruddefineret procedure.

På operationelt projektniveau gennemføres der løbende risikostyring. Der arbejdes efter en fast projektstyringsmodel, hvor ansvaret for projektrelateret risikostyring ligger hos projektlederen, som ofte vælger at inddrage projektdeltagere, eksterne partnere og evt. styregruppemedlemmer i processen.

3.5 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering

itm8 Business Application Managements sikringsforanstaltninger og kontroller følger standarderne fra kontrolrammen ISO 27001:2022.

itm8's it-sikkerhedspolitik, etablerede processer og kontroller omfatter alle de systemer og ydelser, kunderne tilbydes. Det fortsatte arbejde med tilpasning og forbedring af itm8 Business Application Managements sikringsforanstaltninger sker løbende i samarbejde med højt kvalificerede specialister.

På basis af ISO 27001 som kontrolramme er relevante kontrolområder og kontrolaktiviteter implementeret ud fra "best practice" til minimering af risici på de serviceydelser, som leveres af itm8 Business Application Managements hosting-afdeling. Med udgangspunkt i den valgte kontrolmodel indgår følgende kontrolområder i det samlede kontrolmiljø:

- Organisatoriske foranstaltninger
- Personrelaterede foranstaltninger
- Fysisk adgangskontrol
- Tekniske foranstaltninger.

De forskellige kontrolområder er igen delt ind i forskellige sikkerhedsområder som beskrevet nedenfor, hvor der for hvert område er regler og principper der følges.

3.6 Sikkerhedsområder

3.6.1 Forvaltning af aktiver

itm8 Business Application Management har implementeret og vedligeholder forskellige CMDB'er afhængigt af aktivernes art. Dette omfatter databaser på endepunkter, servere, netværksudstyr og andre systemer, som alle har ejere og anden relevant information tildelt.

Der er etableret regler for acceptabel brug af itm8 Business Application Managements aktiver, som er dokumenteret i politik for acceptabel brug. Udleverede aktiver registreres, og aflevering af aktiver er en del af offboarding-proceduren.

Regler for, hvordan aktiver skal beskyttes og håndteres, når de tages ud af sikre områder, er også kommunikeret. Derudover har itm8 Business Application Management politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.

For bortskaffelse eller genbrug af udstyr er der implementeret retningslinjer, der sikrer, at lagringsmedier bortskaffes gennem en certificeret leverandør for at sikre korrekt destruktion.

Endelig har itm8 Business Application Management implementeret forskellige sikkerhedspolitikker for brugerslutpunkter for at sikre, at de er tilstrækkeligt beskyttet. Dette inkluderer blandt andet fjernsletning af harddiske og malwarebeskyttelse.

3.6.2 Sikring af fortsat drift

itm8 Business Application Management har udviklet forretningskontinuitetsplaner for at sikre, at både informationssikkerhed og drift opretholdes på et højt niveau, selv under forstyrrelser. For at sikre, at disse planer er effektive, gennemfører itm8 Business Application Management årlige IKT-beredskabstests. Disse tests sikrer, at planerne fungerer som tiltænkt, og at organisationen følger dem korrekt.

Derudover har itm8 Business Application Management etableret procedurer for månedlig rapportering om driften. Disse rapporter indeholder detaljerede oplysninger om produktionsmiljøoperationer, herunder kapacitetsdata. For at sikre at fremtidige kapacitetskrav opfyldes, overvåges driftsmiljøet og relevante systemparametre automatisk.

Backupprocesser udføres i overensstemmelse med itm8 Business Application Managements bedste praksis eller kundernes specifikke forretningskrav. Backupjobbene overvåges nøje for at sikre deres kontinuerlige drift, og årligt gennemføres en recovery-test for at bekræfte systemernes genoprettelseskapacitet.

Endelig har itm8 Business Application Management etableret redundans i egne informationsbehandlingsfaciliteter. Der kan også leveres redundans til kundesystemer, hvis kunderne har sådanne krav, hvilket yderligere styrker evnen til at opretholde kontinuerlig drift under forskellige scenarier.

3.6.3 Personrelaterede sikkerhedsområder

itm8 Business Application Management screener alle potentielle kandidater, og herunder indhentes rene straffeattester. Medarbejdere skal løbende levere en ren straffeattest hvert tredje år. Ansættelsesvilkår omfatter accept af overholdelse af informationssikkerhedspolitikken.

Sikkerhedstræning udføres løbende, herunder phishing-simuleringer, for at øge medarbejdernes praktiske erfaring. Medarbejdere skal kende informationssikkerhedskrav og politikker. Disciplinære foranstaltninger ved overtrædelser er beskrevet i politikken.

Fortsat informationssikkerhedsansvar kommunikeres ved fratrædelse, og fortrolighedsaftaler indgås ved ansættelse. Nogle medarbejdere kan være underlagt yderligere fortrolighedskrav.

For fjernarbejde er der etableret sikkerhedsforanstaltninger som VPN-forbindelser og virtuelle skriveborde for at sikre, at informationssikkerhedsniveauet opretholdes.

3.6.4 Identifikation og adgangskontrol

itm8 Business Application Management har fastlagt retningslinjer for adgang til både egne systemer og kundesystemer baseret på forretnings- og informationssikkerhedskrav. For at sikre korrekt tildeling af autentifikationsoplysninger er der krav om at benytte password management-systemet "PasswordState" til medarbejderne, som samtidig stiller krav til oprettelse af sikre adgangskoder.

Medarbejdernes privilegerede tekniske rettigheder i både interne og kundevendte systemer gennemgås løbende for at sikre, at de er passende og i overensstemmelse med arbejdsrelaterede behov. Ikke-teknisk privilegerede medarbejdere får de nødvendige rettigheder til at bruge interne systemer, og disse rettigheder justeres ved ansættelse, overdragelse og opsigelse.

Når en medarbejder forlader virksomheden, tilbagekaldes alle adgange. Ved jobskifte tilpasses adgangen, så den matcher de nye opgaver. itm8 Business Application Management har en politik for tildeling og begrænsning af privilegeret adgang, hvor alle brugere med sådanne rettigheder har en dedikeret bruger. Listen over privilegerede brugere revideres kvartalsvist.

Adgangen til systemer og applikationer begrænses til medarbejdere med et arbejdsrelateret behov. Derudover har itm8 Business Application Management implementeret sikre autentificeringsteknologier, herunder multifaktorautentifikation, for at beskytte følsom information

3.6.5 Beskyttelse af informationer og data

itm8 Business Application Management har en dataklassificeringsordning, der fastlægger, hvordan forskellige typer data skal kategoriseres og håndteres baseret på deres klassificering.

For at sikre at information overføres gennem sikre og pålidelige kommunikationskanaler, er der også indført specifikke politikker og procedurer. Disse foranstaltninger er designet til at beskytte data under overførsel og sikre, at de når deres destination uden risiko for at blive kompromitteret. Dette omfatter fx brug af VPN-forbindelser, kryptering og direkte linjer.

Derudover har itm8 Business Application Management identificeret de nødvendige krav til beskyttelse af privatlivets fred og personligt identificerbare oplysninger (PII). Der er implementeret passende kontroller og foranstaltninger for at opfylde disse krav og sikre, at privatlivets fred respekteres.

Endelig er der etableret procedurer for sikker sletning af data. Disse procedurer sikrer, at ingen oplysninger opbevares længere end nødvendigt i henhold til lovgivning eller forretningsbehov, hvilket hjælper med at minimere risikoen for datalækager og overholdelse af lovkrav.

3.6.6 Informationssikkerhedsstyring

itm8 Business Application Management er underlagt informationssikkerhedspolitikken for hele itm8, som er godkendt af topledelsen og delt med alle medarbejdere. Derudover er der udviklet flere specifikke politikker, der støtter hovedpolitikken og er distribueret til relevante medarbejdere.

Disse politikker gennemgås mindst en gang om året eller ved større ændringer for at sikre, at de altid er opdaterede. itm8 Business Application Management har også fastlagt klare roller og ansvar i overensstemmelse med information security management-systemet.

For at sikre en passende adskillelse af opgaver er der defineret politikker, som også revideres årligt eller ved væsentlige ændringer. Dette sikrer, at adskillelsen afspejler informationssikkerhedspolitikken og de nødvendige sikkerhedsniveauer.

Ledelsen hos itm8 Business Application Management er forpligtet til at støtte informationssikkerhedsinitiativer og uddanne medarbejderne i disse tiltag. Endelig er der etableret procedurer for kommunikation med relevante myndigheder i tilfælde af en sikkerhedshændelse.

3.6.7 Fysisk sikkerhed

itm8 Business Application Management har implementeret fysiske sikkerhedsforanstaltninger for at beskytte virksomhedens områder og følsomme oplysninger. Alle kontorer er udstyret med adgangskontrolsystemer, der kræver personlige id-kort og PIN-koder for adgang. Derudover er der etableret adskilte sikkerhedszoner og CCTV-overvågning ved indgange til kontorer, datacentre og andre faciliteter.

For at sikre at arbejdet i sikre områder udføres uden risiko for medarbejdere og informationsaktiver, har itm8 Business Application Management beskrevet specifikke procedurer og retningslinjer. Der er også en politik om ryddet skrivebord og skærm, der forhindrer, at følsomme oplysninger efterlades uden opsyn, og sikrer, at skærme og slutpunkter låses, når de ikke er i brug.

Beskyttelse af kritisk udstyr er en prioritet for itm8 Business Application Management. Der sørges for, at alt udstyr vedligeholdes i overensstemmelse med producentens specifikationer, og der kræves det samme af partnere. Derudover er der etableret beskyttelse af kabler i datacentre for at forhindre uautoriseret adgang og skader.

3.6.8 Konfigurationssikkerhed

itm8 Business Application Management har etableret processer og værktøjer til at håndhæve sikkerhedskonfigurationer for hardware, software, tjenester og netværk, både for nye og eksisterende systemer. Der er udviklet standardskabeloner for sikker konfiguration, som tager højde for nødvendigt beskyttelsesniveau og itm8's informationssikkerhedspolitik. Disse skabeloner revideres periodisk og opdateres ved nye trusler eller software- og hardwareversioner.

Ved oprettelse af skabeloner fokuseres der på at minimere antallet af privilegerede identiteter, deaktivere unødvendige funktioner, synkronisere ure, ændre standardautentifikationsoplysninger og aktivere timeout-faciliteter.

Ændringer og installation af software på operationelle systemer håndteres sikkert af uddannede administratorer med ledelsesgodkendelse. Kun godkendt kode installeres efter omfattende test, og alle opdateringer logges.

itm8 Business Application Management har etableret og implementeret retningslinjer for brugen af kryptografi for at sikre maksimale fordele og minimere risici.

Valget af kryptografiske teknikker og algoritmer er tilpasset beskyttelseskravene for den information, der skal sikres, og sikrer, at de er industristandard og overholder gældende love og regler. Implementeringen følger industristandarder og bedste praksis med kryptografiske nøgler administreret sikkert for at forhindre uautoriseret adgang eller afsløring.

Kryptografi anvendes til at beskytte følsom information under transmission og opbevaring, hvor alle krypterings- og dekrypteringsoperationer udføres sikkert. Kryptografiske nøgler bruges udelukkende til deres tilsigtede formål og beskyttes mod uautoriseret adgang eller afsløring. Nøgler ændres periodisk eller bortskaffes sikkert, når de ikke længere er nødvendige. Alt kryptografisk udstyr og software vedligeholdes og opdateres i henhold til producentens anbefalinger for at adressere kendte sårbarheder.

3.6.9 Leverandørforhold

itm8 Business Application Management har etableret procedurer for at håndtere sikkerhedsrisici ved brugen af leverandørers produkter og tjenester. Dette inkluderer en årlig risikovurdering og revision af leverandører for at sikre, at de fortsat opfylder itm8 Business Application Managements sikkerhedskrav.

Sikkerhedskravene til leverandører er en del af de kontraktlige aftaler og de generelle forretningsbetingelser for samarbejde med itm8 Business Application Management. Derudover har itm8 Business Application Management udviklet en strategi for brugen af cloud-tjenester, som er i overensstemmelse med informationssikkerhedskravene. Denne strategi dækker brug, styring og udfasning af cloud-tjenester.

3.6.10 System- og netværkssikkerhed

itm8 Business Application Management har etableret dokumenterede driftsprocedurer for at understøtte og styre driften af sine løsninger og services. Disse procedurer er tilgængelige for medarbejdere med et arbejdsrelateret behov via en dedikeret kommunikationsplatform.

For at sikre beskyttelse mod malware har itm8 Business Application Management implementeret antivirussoftware på alle relevante systemer, som overvåges løbende. Derudover fremmes brugerbevidsthed om malware-forsvar gennem sikkerhedsbevidsthedsplatformen, der løbende træner medarbejderne.

itm8 Business Application Management har også indført politikker for at sikre sikker kommunikation og minimere risikoen for datamanipulation. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsrelateret behov, og kommunikationen mellem itm8 Business Application Management og kunder udføres ved hjælp af sikre og gennemprøvede teknologier. Kundenetværk adskilles efter behov, og kunder har ikke adgang til andre kundenetværk.

For at beskytte mod skadeligt indhold har itm8 Business Application Management implementeret webfiltreringsforanstaltninger. Der er også etableret en change management-proces, der sikrer, at alle ændringer i informationssystemer i produktionsmiljøer er underlagt change management-procedurer. Dette sikrer, at ændringer ikke påvirker hinanden unødigt, og at tilbagerulningsplaner er på plads.

3.6.11 Håndtering af trusler og sårbarheder

itm8 Business Application Management har etableret og implementeret procedurer for at sikre passende, rettidig og effektiv indsamling af oplysninger om eksisterende og nye trusler. Formålet er at forebygge skader på virksomheden samt reducere truslers påvirkning. Proceduren omfatter identifikation og udvælgelse af informationskilder, indsamling og behandling af information samt analyse og kommunikation af trusselsoplysninger.

For at forhindre udnyttelse af tekniske sårbarheder har itm8 Business Application Management etableret og implementeret procedurer, der inkluderer roller og ansvar for sårbarhedshåndtering, identifikation af informationsressourcer til sårbarhedsovervågning, krav til leverandører om rapportering og håndtering af sårbarheder, brug af sårbarhedsscanningsværktøjer samt planlagte penetrationstests for at identificere sårbarheder. Patch management-procedurer sikrer, at de nyeste godkendte patches og opdateringer installeres for al autoriseret software.

Kontrolmål og -aktiviteter fremgår detaljeret i afsnit 4.

3.7 Komplementære kontroller hos kunder

Forhold, der skal overvejes af kundernes revisorer

Leverede serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på itm8 Business Application Managements standardvilkår. Kundernes afvigelser fra itm8s standardvilkår er derfor ikke omfattet af denne erklæring.

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

Brugeradministration

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

Beredskabsplanlægning

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

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

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

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

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

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

4.2 Testhandlinger

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

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

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.1	**Politikker for informationssikkerhed** *Informationssikkerhedspolitik og emnespecifikke politikker skal defineres, godkendes af ledelsen, offentliggøres, kommunikeres til og anerkendes af relevante medarbejdere og relevante interessenter og vurderes med planlagte mellemrum samt hvis der sker væsentlige ændringer.* itm8 Business Application Management har defineret og dokumenteret en informationssikkerhedspolitik, som godkendes af topledelsen og distribueres til alle medarbejdere. itm8 Business Application Management har defineret og dokumenteret flere emnespecifikke politikker, som understøtter informationssikkerhedspolitikken og distribueres til alle relevante medarbejdere. Informationssikkerhedspolitikken og emnespecifikke politikker revideres mindst årligt, eller hvis der sker væsentlige ændringer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har inspiceret, at informationssikkerhedspolitikkerne kommunikeres til medarbejderne og relevante parter og er revideret årligt.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.2	**Roller og ansvar for informationssikkerhed** *Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov.* itm8 Business Application Management har etableret og defineret roller og ansvar med overensstemmelse med sit information security management-system.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer.	Ingen afvigelser noteret.
5.3	**Adskillelse af opgaver** *Modstridende pligter og modstridende ansvarsområder skal adskilles.* itm8 Business Application Management har defineret politikker for adskillelse af opgaver, som revideres mindst årligt, eller hvis der sker væsentlige ændringer, for at sikre at niveauet af adskillelse afspejler informationssikkerhedspolitikken og det nødvendige niveau af adskillelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøver inspiceret, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos itm8 Business Application Management, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Ingen afvigelser noteret.
5.4	**Ledelsens ansvar** *Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.* itm8 Business Application Managementkræver, at ledelsen sætter sig ind i og støtter gældende informationssikkerhedsinitiativer og uddanner sine medarbejdere i disse tiltag.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at ledelsen er bekendt med informationssikkerhedsinitiativer.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.5	**Kontakt til myndigheder** *Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.* itm8 Business Application Management har etableret og implementeret kommunikationsprocedurer for, hvordan man kommunikerer med relevante myndigheder i tilfælde af en sikkerhedshændelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har en kommunikationsprocedure for, hvordan der kommunikeres med relevante myndigheder i tilfælde af sikkerhedsbrud.	Ingen afvigelser noteret.
5.7	**Underretning om trusler** *Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretninger om trusler.* itm8 Business Application Managementproducerer trusselsefterretninger fra forskellige kilder, herunder sårbarhedsrapporter, udvalgte nyhedskilder, leverandører, myndigheder og særlige interessegrupper til brug for risikobaseret beslutningstagning.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at itm8 Business Application Management indhenter og analyserer information til brug for risikobaseret beslutningstagning.	Ingen afvigelser noteret.
5.9	**Fortegnelse over information og understøttende aktiver** *Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.* itm8 Business Application Management har implementeret og vedligeholder forskellige CMDB'er afhængigt af arten af aktiverne i omfang. Dette omfatter databaser på endepunkter, servere, netværksudstyr, databaser osv., som alle har ejere og anden relevant information tildelt.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.10	**Acceptabel brug af information og understøttende aktiver** *Regler for acceptabel brug og procedurer til håndtering af information og understøttende aktiver bør identificeres, dokumenteres og implementeres.* itm8 Business Application Management har etableret og implementeret regler om acceptabel brug af itm8 Business Application Management' aktiver dokumenteret i vores Politik for acceptabel brug.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at passende kontroller er på plads for at sikre dokumentation og vedligeholdelse af beholdningen af aktiver, herunder acceptabel brug af aktiver.	Ingen afvigelser noteret.
5.11	**Returnering af aktiver** *Medarbejdere og andre interessenter skal aflevere alle de af organisationens aktiver, de har i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører eller ændrer karakter.* itm8 Business Application Management registrerer udleverede aktiver og har aflevering af aktiver som en del af proceduren for offboarding.	Vi har observeret, at en procedure er på plads for at sikre, at aktiver returneres ved opsigelse. Vi har ved stikprøve inspiceret, at der ved op-sagte medarbejdere er dokumentation for, at alle aktiver er returneret ved opsigelse.	Ingen afvigelser noteret.
5.12	**Klassifikation af oplysninger** *Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.* itm8 Business Application Management har etableret en dataklassificeringsordning, der omhandler, hvordan forskellige typer data skal klassificeres og håndteres i henhold til deres klassificering.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at itm8 Business Application Management har etableret en dataklassificeringsordning til klassifikation af information.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.14	**Overførsel af information** *Der skal være etableret regler eller procedurer for eller aftaler om overførsel af information for alle former for overførselsfaciliteter i organisationen og mellem organisationen og andre parter.* itm8 Business Application Management har etableret politikker og procedurer for informationsoverførsel for at sikre, at information rejser gennem sikre og pålidelige kommunikationskanaler.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøver inspiceret, at en passende teknisk sikkerhedsarkitektur er blevet etableret i netværket, samt at der er etableret regler for informationsoverførsel.	Ingen afvigelser noteret.
5.15	**Administration af adgang** *Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til information og understøttende aktiver på grundlag af forretnings- og informationssikkerhedskrav.* itm8 Business Application Management har implementeret generelle retningslinjer for adgang til egne og kundesystemer baseret på forretnings- og informationssikkerhedskrav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at retningslinjer for adgangskontrol er implementeret, gennemgået og godkendt.	Ingen afvigelser noteret.
5.17	**Autentifikationsoplysninger** *Tildeling og styring af autentifikationsoplysninger skal ske i form af en ledelsesproces, herunder rådgivning af medarbejdere om passende håndtering af autentifikationsoplysninger.* itm8 Business Application Management har retningslinjer for tildeling af autentifikationsoplysninger og stiller et password management-system til rådighed for medarbejder i form af programmet PasswordState. Der er desuden vejledning i oprettelse af sikre adgangskoder.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at proceduren sikrer at autentifikationsoplysninger håndteres på sikker vis.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.18	**Adgangsrettigheder** *Adgangsrettigheder til information og understøttende aktiver bør tilvejebringes, vurderes, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for administration af adgang.* itm8 Business Application Managementgennemgår løbende medarbejderens privilegerede tekniske rettigheder i både interne og kundevendte systemer for at sikre, at rettigheden er passende og i overensstemmelse med medarbejderens arbejdsrelaterede behov. Ikke-teknisk privilegerede medarbejdere tildeles de nødvendige rettigheder til at bruge interne systemer. Disse standardrettigheder tilføjes og fjernes i forbindelse med ansættelse, overdragelse og opsigelse hos itm8 Business Application Management. Når en medarbejder forlader itm8 Business Application Management, tilbagekaldes alle adgange. Hvis en medarbejder skifter jobfunktion, tilpasses adgangen, så den afspejler den nye opgave.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspiceret, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen. Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.19	**Informationssikkerhed i leverandørforhold** *Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.* itm8 Business Application Management har etableret procedurer for styring af sikkerhedsrisici forbundet med brugen af en leverandørs produkter og tjenester, som omfatter en årlig risikovurdering og revision af leverandører for at sikre, at leverandøren fortsat lever op til de sikkerhedskrav, itm8 Business Application Management forventer.	Vi har inspiceret, at der findes en formel og dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved stikprøver inspiceret, at der udarbejdes risikovurderinger med passende mellemrum på kritiske leverandører. Vi har inspiceret, at itm8 Business Application Management jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav.	Ingen afvigelser noteret.
5.20	**Håndtering af informationssikkerhed i leverandøraftaler** *Relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkelt leverandør på grundlag af typen af leveranceforhold.* itm8 Business Application Management har fastlagt sikkerhedskrav til leverandører, som behandles som en del af den kontraktlige aftale med leverandørerne og de almindelige forretningsbetingelser for leverandører, der samarbejder med itm8 Business Application Management.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at en formel og dokumenteret procedure er på plads for at sikre, at nye eller genforhandlede applikations- eller serviceleverandørkontrakter valideres i forhold til en liste over definerede informationssikkerhedskrav.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.23	**Informationssikkerhed ved brug af cloud-tjenester** *Der skal fastlægges processer for anskaffelse, brug, styring og afslutning af brugen af cloud-tjenester i overensstemmelse med organisationens informationssikkerhedskrav.* itm8 Business Application Management har fastlagt en strategi for brugen af cloud-tjenester i overensstemmelse med itm8 Business Application Management krav til informationssikkerhed, herunder brug, styring og udtræden af cloud-tjenester.	Vi har inspiceret, at der er etableret en strategi for brugen af cloud-tjenester.	Ingen afvigelser noteret.
5.24	**Planlægning og forberedelse af incident-håndtering ved sikkerhedsincidents** *Organisationen skal planlægge og forberede sig på at håndtere informationssikkerhedsincidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedsincidents.* itm8 Business Application Management har defineret, etableret og implementeret en plan for håndtering af informationssikkerhedshændelser, som omfatter en proces for hændelseshåndtering og roller og ansvar relateret til hændelsesrespons.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at den formelle og dokumenterede proces for hændelsesstyring er blevet gennemgået og godkendt. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.25	**Vurdering af og beslutning om informationssikkerhedshændelser** *Organisationen skal vurdere informationssikkerhedshændelser og beslutte, om de skal kategoriseres som informationssikkerhedsincidents.* itm8 Business Application Management' sikkerhedsudvalg vurderer det seneste kvartals hændelser og kategoriserer på baggrund af vurderingen. Desuden kan sikkerhedsudvalget mødes med kort varsel hvis dette kræves.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.
5.26	**Håndtering af informationssikkerhedsincidents** *Informationssikkerhedsincidents skal håndteres i overensstemmelse med de dokumenterede procedurer.* itm8 Business Application Management har etableret procedurer for at reagere på informationssikkerhedshændelser.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.27	**Læring af informationssikkerhedsincidents** *Den viden, der opnås i forbindelse med informationssikkerhedsincidents, bør anvendes til at styrke og forbedre informationssikkerhedsforanstaltninger.* itm8 Business Application Management har etableret procedurer for at lære af informationssikkerhedshændelser, hvor sikkerhedshændelser løbende gennemgås for læringsmuligheder og forbedring af itm8 Business Application Management' sikkerhedsposition.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at sikkerhedshændelser er gennemgået.	Ingen afvigelser noteret.
5.28	**Indsamling af bevismateriale** *Organisationen skal definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af bevismateriale i relation til informationssikkerhedshændelser.* itm8 Business Application Management har etableret procedurer for indsamling af bevismateriale i forbindelse med sikkerhedshændelser og gemmer dokumentationen i ITSM-systemet.	Vi har foretaget forespørgsler hos ledelsen om de udførte procedurer/kontrolaktiviteter. Vi har observeret, at der opretholdes en formel proces for vurdering og analyse af informationssikkerhedshændelser.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.29	**Informationssikkerhed under driftsforstyrrelse** *Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.* itm8 Business Application Management har etableret forretningskontinuitetsplaner for at sikre, at itm8 Business Application Management kan opretholde informationssikkerhed og drift på et passende niveau under driftsforstyrrelser.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at de bagvedliggende procedurer for beredskabsplanen er blevet gennemgået og godkendt af relevant personale.	Ingen afvigelser noteret.
5.30	**IKT-parathed til understøttelse af forretningskontinuitet** *IKT-beredskab bør planlægges, implementeres vedligeholdelse og testes på grundlag af mål for forretningskontinuitet og IKT-kontinuitetskrav.* itm8 Business Application Management udfører årligt IKT-beredskabstest for at sikre, at forretningskontinuitetsplaner kan understøtte det tilsigtede og passende resultat, og at organisationen handler i henhold til forretningskontinuitetsplaner.	Vi har inspiceret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, revideres og godkendes årligt. Vi har inspiceret, at IKT-beredskabstest er blevet gennemgået årligt og godkendt af passende personale.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.34	**Privatlivsbeskyttelse og beskyttelse af personoplysninger** *Organisationen skal identificere og opfylde kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav.* itm8 Business Application Management har identificeret gældende krav vedrørende bevarelse af privatlivets fred og beskyttelse af PII og etableret passende kontroller og foranstaltninger til at opfylde disse krav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at tilstrækkelige kontroller er på plads for at sikre dokumentation og vedligeholdelse af PII.	Ingen afvigelser noteret.
5.37	**Dokumenterede driftsprocedurer** *Driftsprocedurer for informationsbehandlingsfaciliteter bør dokumenteres og gøres tilgængelige for medarbejdere, der har brug for dem.* itm8 Business Application Management har etableret tilstrækkelige og dokumenterede driftsprocedurer til at understøtte og styre driften af løsninger og services leveret af itm8 Business Application Management. Dette omfatter etablering af en platform for kommunikation og tilgængelighed af disse driftsprocedurer til medarbejdere med et arbejdsrelateret behov for dem.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret driftsprocedurer, og at disse skal opdateres mindst én gang årligt. Vi har inspiceret, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.1	**Screening** *Der skal udføres verifikation af alle jobansøgeres baggrund. Verifikationen bør foretages, inden de tiltræder i organisationen og løbende under hensyntagen til love, forskrifter og etiske regler, og bør vurderes i forhold til organisationens krav, klassifikationen af den information, der skal gives adgang til, og de relevante risici.* itm8 Business Application Management udfører screening af sine potentielle kandidater, hvilket omfatter indhentning af rene straffeattester på alle medarbejdere ansat i itm8 Business Application Management. Alle medarbejdere er forpligtet til løbende at levere en ren straffeattest under deres ansættelse, hvor en sådan straffeattest indhentes af itm8 Business Application Management hvert tredje ansættelsesår.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksterne konsulenter samt hvert tredje ansættelsesår. Vi har ved stikprøver inspiceret, at der er erhvervet straffeattester inden ansættelsesstart for nyansatte.	Ingen afvigelser noteret.
6.2	**Ansættelsesvilkår – og betingelser** *Ansættelseskontrakterne skal beskrive medarbejderes og organisationens ansvar for informationssikkerhed.* itm8 Business Application Management har fastsat ansættelsesvilkår som en del af ansættelsesaftalen mellem en medarbejder og itm8 Business Application Management. Disse omfatter forventninger om overholdelse af gældende informationssikkerhedsinitiativer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.3	**Awareness, uddannelse og træning vedrørende informationssikkerhed** *Organisationens medarbejdere og relevante interessenter skal modtage passende awareness, uddannelse og træning vedrørende informationssikkerhed samt regelmæssige opdateringer om organisationens informationssikkerhedspolitik, emnespecifikke politikker og procedurer, hvor det er relevant for deres jobfunktion.* itm8 Business Application Management udfører løbende forskellige sikkerhedsbevidsthedsinitiativer baseret på et årligt hjul og ad-hoc-trendende sikkerhedstrusler i verden. itm8 Business Application Management udfører simuleringer af phishing-forsøg og andre brudforsøg for at øge medarbejdernes praktiske erfaring med faktiske brudforsøg. Endvidere er alle medarbejdere forpligtet til at sætte sig ind i gældende informationssikkerhedskrav og informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås, samt at medarbejderne jævnligt skal gennemføre obligatoriske undervisningsforløb for at sikre, at virksomhedens sikkerhedskrav overholdes. Vi har inspiceret, at medarbejdere er introduceret til informationssikkerhedspolitikken.	Ingen afvigelser noteret.
6.4	**Sanktioner** *Der skal formaliseres og kommunikeres en sanktionsproces, så der iværksættes handlinger mod medarbejdere og andre relevante interessenter, som har overtrådt informationssikkerhedspolitikken.* itm8 Application Service har i informationssikkerhedspolitikken nedskrevet, hvilke disciplinære foranstaltninger der kan sættes i værk ved overtrædelse af informationssikkerhedspolitikken.	Vi har foretaget forespørgsler hos ledelsen om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er en formaliseret procedure på plads, som beskriver den disciplinære proces.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.5	**Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold** *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.* itm8 Business Application Management kommunikerer informationssikkerhedsansvar, som forbliver gyldigt efter opsigelse eller ændring af ansættelsesforhold. Dette omfatter indhentning af skriftlig bekræftelse på, at den opsagte medarbejder forstår sine fortsatte forpligtelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes en skriftlig bekræftelse på, at opsagte medarbejdere forstår deres forsatte forpligtelse i forbindelse med fratrædelse.	Ingen afvigelser noteret.
6.6	**Hemmeligholdelse- og fortrolighedsaftaler** *Hemmeligholdelses- og fortrolighedsaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejdere og andre interessenter.* itm8 Business Application Management etablerer fortrolighedsaftaler med sine medarbejdere som en del af de indledende, kontraktlige ansættelsesaftaler. Desuden kan nogle medarbejdere under deres ansættelse være underlagt yderligere fortrolighed eller tavshedspligt, hvis kunderne kræver det.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes fortrolighedsaftaler i forbindelse med nyansættelser.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.7	**Distancearbejde** *Der skal være implementerede sikkerhedstiltag, når medarbejdere arbejder på afstand, for at beskytte information, der er adgang til, og som behandles eller lagres uden for organisationens lokaliteter.* itm8 Business Application Management har etableret og implementeret sikkerhedsforanstaltninger for personale, der arbejder eksternt, for at sikre, at informationssikkerhedsniveauet svarer tilstrækkeligt til, når medarbejdere arbejder fra kontorerne. Dette inkluderer blandt andet etablering af VPN-forbindelser og sikring af, at alt følsomt arbejde udføres på virtuelle skriveborde.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er implementeret passende sikkerhedsforanstaltninger for personale, der arbejder eksternt.	Ingen afvigelser noteret.
6.8	**Indrapportering af informationssikkerhedshændelser** *Organisationen skal sørge for, at medarbejdere kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt via passende kanaler.* itm8 Business Application Management har etableret og tilvejebringer en mekanisme for personale til at rapportere observerede eller formodede informationssikkerhedshændelser. Proceduren for at bruge mekanismen kommunikeres til og gøres tilgængelig for alle medarbejdere.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysisk adgangskontrol

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.2	**Fysisk adgangskontrol** *Sikrede områder bør beskyttes ved hjælp af passende adgangsforanstaltninger og adgangspunkter.* itm8 Business Application Management har etableret fysiske adgangskontroller til sikring af områder, som omfatter identifikationskort, registrering af besøg og konstant tilsyn med godkendte og fratrådte medarbejdere.	Vi har inspiceret, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at itm8 Business Application Management har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.3	**Sikring af kontorer, lokaler og faciliteter** *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.* itm8 Business Application Management har implementeret fysisk sikkerhed på vores kontorer, som omfatter fysiske adgangspunkter, der er tilgængelige via personlige id-kort og personlige PIN-koder, adskilte sikkerhedszoner og CCTV.	Vi har inspiceret, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at itm8 Business Application Management har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.4	**Fysisk sikkerhedsovervågning** *Lokaliteter skal overvåges løbende for uautoriseret fysisk adgang.* itm8 Business Application Management har etableret CCTV ved indgange til både kontorer, datacentre og andre faciliteter, hvor der behandles følsomme oplysninger.	Vi har inspiceret, at CCTV er etableret ved alle indgange til både kontorer, datacentre og andre faciliteter, hvor der behandles følsomme oplysninger.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysisk adgangskontrol

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.5	**Beskyttelse mod fysiske og miljømæssige trusler** *Beskyttelse mod fysiske og miljømæssige trusler, fx naturkatastrofer og andre tilsigtede eller utilsigtede fysiske trusler mod infrastrukturen, skal tilrettelægges og implementeres.* itm8 Business Application Management har beskrevet fysiske og miljømæssige trusler mod egne datacentre og taget passende forholdsregler til at imødegå disse.	Vi har forespurgt om de procedu-rer/kontrolaktiviteter, der udføres. Vi har inspiceret tilstedeværelsen af brandbekæmpelses-systemer i serverrum.	Ingen afvigelser noteret.
7.6	**Arbejde i sikrede områder** *Sikkerhedsforhold for arbejde i sikrede områder skal tilrettelægges og implementeres.* itm8 Business Application Management har etableret procedurer og retningslinjer for arbejde i sikre områder for at sikre, at udførelse af arbejde ikke bringer medarbejdere og informationsaktiver i fare.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at relevante sikkerhedsforhold er etableret for at sikre medarbejdere samt informationsaktiver.	Ingen afvigelser noteret.
7.7	**Ryddeligt skrivebord og låst skærm** *Regler om at holde skriveborde ryddet for papir og bærbare lagringsmedier og om at holde skærme låst på informationsbehandlingsfaciliteter skal defineres og håndhæves på behørig vis.* itm8 Business Application Management har etableret en politik om ryddet skrivebord og låst skærm, der sikrer, at følsomme oplysninger ikke efterlades uden opsyn på kontoret, og at skærme og slutpunkter låses, når de efterlades uden opsyn.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har implementeret en politik om ryddet skrivebord og låst skærm.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysisk adgangskontrol

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.8	**Placering og beskyttelse af udstyr** *Udstyr skal placeres på et sikkert og beskyttet sted.* itm8 Business Application Management har en politik for at sikre beskyttelse af kritisk udstyr.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har fastlagt retningslinjer for sikring mod brand, vand og varme. Vi har desuden inspiceret, at itm8 Business Application Management har indhentet revisionserklæring fra en underleverandør for at sikre, at tilsvarende krav overholdes, på områder hvor der er sket outsourcing.	Ingen afvigelser noteret.
7.9	**Sikring af aktiver uden for organisationens områder** *Aktiver uden for organisationens lokationer skal beskyttes.* itm8 Business Application Management har etableret og kommunikeret regler for, hvordan aktiver skal beskyttes og håndteres, når de fjernes fra organisationens område.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret regler, der sikrer, at aktiver er beskyttet og håndteres korrekt, når de fjernes fra organisationens områder, samt at dette er godkendt.	Ingen afvigelser noteret.
7.10	**Lagringsmedier** *Lagringsmedier skal styres i hele deres livscyklus i forbindelse med anskaffelse, brug, transport og bortskaffelse i overensstemmelse med organisationens klassifikationssystem og krav til håndtering.* itm8 Business Application Management har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysisk adgangskontrol

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.11	**Forsyningssikkerhed** *Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.* itm8 Business Application Management sikrer, at alt udstyr, der ejes af itm8 Business Application Management, vedligeholdes efter producentens specifikation. Ydermere sikrer itm8 Business Application Management, at dets partnere gør det samme.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret en fuldt redundant infrastruktur med særskilt backup.	Ingen afvigelser noteret.
7.12	**Sikring af kabler** *Kabler, som bærer strøm, data eller understøtter informationstjenester, skal beskyttes mod aflytning, forstyrrelse og beskadigelse.* itm8 Business Application Management har etableret beskyttelse af kabler i egne datacentre.	Vi har forespurgt om de procedu-rer/kontrolaktiviteter, der udføres. Vi har inspiceret, at Der er implementeret passende kontroller for at beskytte fysisk faciliteter og kablingsikkerhed. Vi har inspiceret sikring af kabler til datakommunikation og elforsyning.	Ingen afvigelser noteret.
7.13	**Vedligeholdelse af udstyr** *Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.* itm8 Business Application Management sørger for at vedligeholde udstyr som specificeret af producenten.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret retningslinjer for, hvordan udstyr vedligeholdes korrekt.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysisk adgangskontrol

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.14	**Sikker bortskaffelse eller genbrug af udstyr** *Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software slettes eller overskrives på forsvarlig vis inden bortskaffelse eller genbrug.* itm8 Business Application Management har implementeret retningslinjer for bortskaffelse eller genbrug af udstyr, der sikrer, at hvis lagringsmedier bortskaffes, sker det gennem en certificeret leverandør for at sikre dets ødelæggelse.	Vi har inspiceret, at itm8 Business Application Management har implementeret procedurer for sikker bortskaffelse eller genbrug af udstyr. Vi har inspiceret, at bortskaffelse eller genbrug af udstyr sker igennem en certificeret leverandør.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.1	**Brugerenheder** *Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, bør beskyttes.* itm8 Business Application Management har implementeret forskellige sikkerhedspolitikker for sine brugerslutpunkter for at sikre, at de er tilstrækkeligt beskyttet. Dette inkluderer blandt andet fjernsletning af harddiske, malwarebeskyttelse osv.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har implementeret en politik for brugerenheder.	Ingen afvigelser noteret.
8.2	**Privilegerede adgangsrettigheder** *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* itm8 Business Application Management har en politik for tildeling og begrænsning af brugere med privilegeret adgang. Alle brugere med privilegeret adgang har en dedikeret bruger til den privilegerede adgang. Listen over privilegerede brugere revideres på kvartalsbasis.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har tilrettelagt formaliserede procedurer for brugeradministration og rettighedsstyring, og at disse også gælder for brugere med privilegerede rettigheder. Vi har inspiceret, at der for autorisationer, der tildeles medarbejdere, foreligger en begrundelse for det ønskede adgangsniveau og en godkendelse fra nærmeste chef. Vi har inspiceret, at privilegerede adgangsrettigheder er revideret på kvartalsbasis.	Vi har noteret at to konti på to backupservere har "password never expires" aktiveret. Vi er informeret om, at begge konti er nu tilpasset den gældende passwordpolitik. Ingen yderligere afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.3	**Begrænset adgang til information** *Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.* itm8 Business Application Management har en politik om at begrænse adgangen til systemer og applikationer til medarbejdere, der har et arbejdsrelateret behov.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret en politik for begrænsning af adgange til systemer og applikationer til medarbejdere, der har et arbejdsbetinget behov.	Ingen afvigelser noteret.
8.5	**Sikker autentifikation** *Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.* itm8 Business Application Management har etableret sikre autentifikationsteknologier til følsom information, som blandt andet inkluderer multifaktorautentifikation.	Vi har inspiceret, at der er implementeret en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt. Vi har inspiceret, at de omfattede applikationer og systemer håndhæver sikre logonprocedurer.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.6	**Kapacitetsstyring** *Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.* itm8 Business Application Management har procedurer for månedlig rapportering om driften. Disse rapporter indeholder oplysninger om drift af produktionsmiljøet, herunder oplysninger om kapacitet. Der er etableret automatisk overvågning af driftsmiljøet og relevante systemparametre, herunder kapacitet, for at sikre, at fremtidige kapacitetskrav opfyldes.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der hver måned sendes rapporter til kunden vedrørende driften i produktionsmiljøerne hos itm8 Business Application Management. Vi har inspiceret, at kapaciteten overvåges på produktionssystemerne hos itm8 Business Application Management, så fremtidige krav til kapaciteten overholdes.	Ingen afvigelser noteret.
8.7	**Beskyttelse mod malware** *Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.* itm8 Business Application Management har implementeret procedurer for at sikre fungerende antivirussoftware på alle gældende systemer. Antivirussoftwaren overvåges. Beskyttelse mod malware understøttes med brugerbevidsthed gennem itm8 Business Application Management' platform til sikkerhedsbevidsthed, der giver viden om malware-forsvar til medarbejderne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøver inspiceret, at medarbejdernes pc'er hos itm8 Business Application Management er beskyttet med antivirussoftware – og at denne er opdateret. Vi har inspiceret, at itm8 Business Application Management har etableret initiativer til brugerbevidsthed om beskyttelse mod malware til medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.8	**Håndtering af tekniske sårbarheder** *Der skal indhentes oplysninger om tekniske sårbarheder ved brug af informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og passende foranstaltninger skal træffes.* itm8 Business Application Management har en procedure til løbende at vurdere sårbarheder, der indberettes, og vurdere deres kritikalitet mod flere kilder i forbindelse med de tjenester, som itm8 Business Application Management leverer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøver inspiceret, at der løbende indhentes informationer om tekniske sårbarheder, samt at der træffes passende foranstaltninger til at håndtere eventuelle risici. Vi harinspiceret, at kritiske sårbarheder kommunikeres til samtlige relevante interessenter.	Ingen afvigelser noteret.
8.9	**Konfigurationsstyring** *Konfigurationer, herunder sikkerhedskonfigurationer, af hardware, software, tjenester og netværk bør etableres, dokumenteres, implementeres, overvåges og vurderes.* itm8 Business Application Management har etableret processer og procedurer for konfigurationsstyring for at sikre, at ændringer af konfigurationer håndteres og dokumenteres korrekt.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret procedurer for konfigurationsstyring, samt at konfigurationer håndteres i overensstemmelse med gældende procedurer.	Ingen afvigelser noteret.
8.10	**Sletning af information** *Information lagret i informationssystemer, enheder eller i andre lagringsmedier skal slettes, når der ikke længere er brug for den.* itm8 Business Application Management har etableret procedurer for sletning af oplysninger for at sikre, at ingen data opbevares længere end krævet af lovmæssige eller forretningsmæssige krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at sletning af oplysninger sker i overensstemmelse med itm8 Business Application Managements procedurer herfor.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.13	**Backup af information** *Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.* itm8 Business Application Management udfører backup i overensstemmelse med itm8 Business Application Management' bedste praksis eller kundernes forretningskrav. Backupjobbene overvåges for at sikre deres kontinuerlige drift. Årligt igangsættes en recovery-test af udvalgte dele af itm8 Business Application Management.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer serviceydelser, hvor backup er relevant. Vi har inspiceret, at der er foretaget en fuld gendannelsestest af it-miljøerne.	Ingen afvigelser noteret.
8.14	**Redundans i faciliteter til informationsbehandling** *Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.* itm8 Business Application Management har redundans i egne informationsbehandlingsfaciliteter og har mulighed for at levere redundans, hvis kunden har dette krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der etableret redundans på itm8 Business Application Managements informationsbehandlingsfaciliteter samt på kundemiljøer i overensstemmelse med gældende kundekontrakter.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.15	**Logning** *Logge, der optegner aktiviteter, undtagelser, fejl og andre relevante hændelser, skal udarbejdes, opbevares, beskyttes og analyseres.* itm8 Business Application Management udfører Security Information and Event Management (SIEM) på sine egne systemer, og på kundens systemer, hvis kunden har disse krav. itm8 Business Application Management registrerer logfiler for forskellige systemer på forskellige sikkerhedsniveauer. I SIEM-systemet er der fuld funktionsadskillelse. Medarbejdere, der har adgang til at slette logdata, har ingen adgang til kundesystemer og itm8 Business Application Managements systemer. Al adgang til kundesystemer logges i systemet. Adgangsloggen opbevares efter kundens retningslinjer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at hændelseslogning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret. Vi har inspiceret, at adgang til kundedata bliver logget og opbevares sikkert. Vi har inspiceret, at itm8 Business Application Management har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov, og at der er implementeret tilstrækkelig funktionsadskillelse i adgange til logdata.	Ingen afvigelser noteret.
8.16	**Overvågning af aktiviteter** *Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerhedsincidents.* itm8 Business Application Management har implementeret et overvågningssystem, der sikrer, at kundernes systemer kører, og at der advares om eventuel unormal adfærd gennem overvågningssystemet. Systemet overvåges 24/7.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at et overvågningssystem er implementeret, samt at dette er overvåget 24/7.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.17	**Synkronisering af ure** *Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.* itm8 Business Application Management har synkroniseret alle relevante informationsbehandlingssystemer til en enkelt referencetidskilde.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har etableret en referencetidskilde for tidssynkronisering af alle relevante informationsbehandlingssystemer.	Ingen afvigelser noteret.
8.19	**Softwareinstallation i test- og produktionssystemer** *Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallationer i test og -produktionssystemer.* itm8 Business Application Management har defineret et sæt standardimplementeringsbeskrivelser. Disse systemer er tilladt på kundesystemer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøver inspiceret, at softwareinstallationer håndteres hensigtsmæssigt og i overensstemmelse med gældende procedurer.	Vi har noteret at enkelte server ikke er patchet med nyeste opdateringer. Vi er informeret om, at serveren er blevet patchet efterfølgende. Vi har noteret at 2 Domain Controller ikke har været opdateret/patched jf. godkendte procedure. Vi har noteret at disse to servere ikke har haft indflydelse på Business Application Managements kunder. Vi har modtaget dokumentation efterfølgende på at begge servere er opdateret med de seneste opdateringer. Ingen yderligere afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.20	**Netværkssikkerhed** *Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.* itm8 Business Application Management har implementeret flere politikker for at sikre en sikker kommunikation, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsrelateret behov. Kommunikation mellem itm8 Business Application Management og kundesteder udføres af valide og gennemprøvede, sikre teknologier.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder: • om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra itm8 Business Application Managements eget miljø • om fjernadgang er tildelt ved brug af tofaktorgodkendelse • om ændringer i netværksmiljøet i vores stikprøve er sket på kontrolleret vis i overensstemmelse med reglerne for ændringsstyring.	Ingen afvigelser noteret.
8.22	**Segmentering af netværk** *Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.* itm8 Business Application Management adskiller kundenetværk i et eller flere netværk afhængigt af behovet for adskillelse. Kunder har ikke adgang til andre kundenetværk.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har testet den tekniske sikkerhedsarkitektur og ved stikprøvever inspiceret, om der jf. retningslinjerne er etableret et passende sikkerhedsniveau, herunder: • om sikre zoner og kundemiljøer er adskilt fra itm8 Business Application Managements eget miljø • om adgang til netværket er opdelt i relevante brugergrupper baseret på et arbejdsbetinget behov.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.23	**Webfiltrering** *Adgang til eksterne websteder skal styres for at reducere eksponeringen for skadeligt indhold.* itm8 Business Application Management har implementeret webfiltreringsforanstaltninger, som omfatter beskyttelse og reduktion af eksponering for skadeligt indhold.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret webfiltreringsforanstaltninger.	Ingen afvigelser noteret.
8.24	**Brug af kryptografi** *Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.* itm8 Business Application Management har etableret politikker for brug af kryptografi, som omfatter regler for brug, valg af kryptografisk teknik, implementering, vedligeholdelse og bortskaffelse.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret en passende brug af sikker kryptografi og nøglehåndtering.	Ingen afvigelser noteret.
8.31	**Adskillelse af udviklings-, test og produktionsmiljøer** *Udviklings-, test- og produktionsmiljøer skal adskilles og sikres.* itm8 Business Application Management stiller adskilte miljøer til rådighed for Kunder efter nærmere aftale.	Vi har inspiceret, at der er implementeret tekniske foranstaltninger i change management processen, der understøtter adskillelse i miljøer. Vi har inspiceret, at der er implementeret et tilstrækkelig change management system.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.32	**Ændringsstyring** *Ændringer til informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.* itm8 Business Application Management har etableret og implementeret en change management-proces, der sikrer, at alle ændringer af informationssystemer i produktionsmiljøer er underlagt change management, som sikrer, at ændringer ikke unødigt påvirker hinanden, og at fallback-planer er på plads.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at itm8 Business Application Management har udarbejdet procedurer for årlig gennemgang og opdatering af: • Hændelsesstyring • Problemstyring • Ændringsstyring • Styring af versioner og programrettelser • Brugeradministration.	Ingen afvigelser noteret.

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

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

Johnny Bjørndahl Klostergaard
Kunde
Serienummer: a6bd3c0b-fe9e-4706-af41-2230e38f8634
IP: 95.138.xxx.xxx
2025-02-19 11:45:56 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 83.136.xxx.xxx
2025-02-19 11:53:27 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 208.127.xxx.xxx
2025-02-19 12:47:29 UTC