Unit IT A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2020 til 31. december 2020 i relation til Unit IT A/S' it-drift og hosting-aktiviteter til kunder

Januar 2021

Indholdsfortegnelse

1 Ledelsens udtalelse

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

Unit IT A/S anvender Front-Safe A/S som serviceunderleverandør for opbevaring af backupdata. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Front-Safe A/S varetager for Unit IT A/S.

Unit IT A/S bekræfter, at:

(a) Den medfølgende beskrivelse i afsnit 2 giver en retvisende beskrivelse af Unit IT A/S' driftsydelser til kunder i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan generelle it-kontroller i relation til driftsydelser 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 driftsydelsers 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 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 driftsydelser, foretaget i perioden fra 1. januar 2020 til 31. december 2020.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til driftsydelser, 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 driftsydelser, 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 2020 til 31. december 2020. 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 2020 til 31. december 2020.

Middelfart, den 7. januar 2021

Mark Frihagen, CEO

2 Unit IT A/S' beskrivelse af generelle it-kontroller for driftsydelser i Danmark

Indledning – kort om Unit IT A/S

Virksomheden udspringer af den **verdensomspændende** USTC-koncern i Middelfart og var indtil 2003 intern it-afdeling for koncernens mange selskaber inden for bl.a. rederi, shipping og bunker-olie.

Unit IT er en sammensmeltning af tre fagligt højt kompetente it-leverandører med hver deres speciale. Du kender os fra tidligere som Outforce, MindZet og it-Craft. I 2018 har vi taget nyt fælles navn for at vise udadtil, at vi nu er én virksomhed med en bred palet af ydelser.

Unit IT A/S rådgiver, designer, servicerer, implementerer og drifter it-løsninger med fokus på følgende:

- Vi er leverandør af dedikerede hostede it-løsninger med 24x7-drift
- Vi er leverandør af it-infrastrukturprojekter
- Vi er kvalitetsbevidste – leverer altid efter "best practice"
- Vi leverer til aftalt tid
- Vi er lette at indgå aftaler med under devisen "Keep It Simple".

Beskrivelse af ydelser

Unit IT A/S' primære ydelser er følgende:

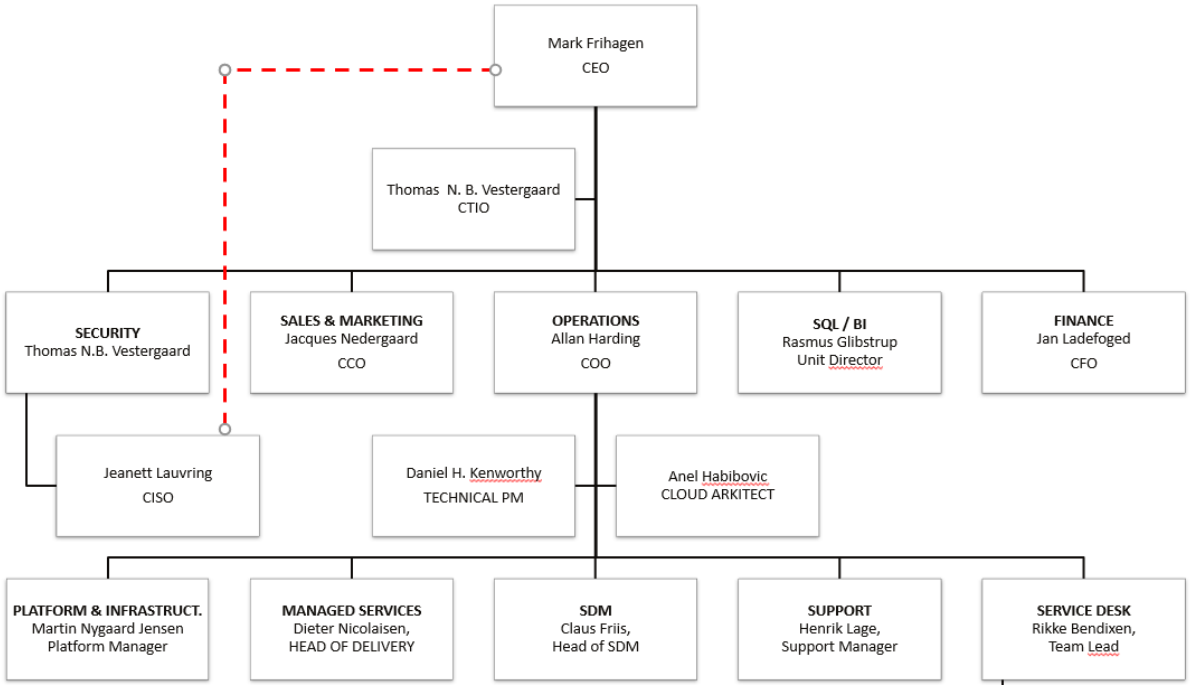
- Levering af private og public cloud-services til og med et Windows-operativsystem
- High performance storage-løsninger
- Kundespecifikke Remote Desktop- og Citrix-løsninger
- MS Exchange og O365
- Helpdesk inkl. klientsupport
- SQL as a service
- Image og remote backup.

Unit IT A/S har i øjeblikket to datacentre på egen matrikel i Middelfart og co-location i Kolding. Der er ca. 24 km's adskillelse mellem de to datacentre og co-location. Herfra foretages overvågning og drift af ca. 2.500 servere.

Beskrivelsen omfatter drift og overvågning for 1. januar 2020 – 31. december 2020 og er udelukkende til brug for de virksomheder, der anvender Unit IT A/S' it-drift og hosting-aktiviteter, og disse virksomheders revisorer og må ikke anvendes til andre formål.

Risikostyring

Organisatorisk opbygning i Unit IT A/S



Ledelsen har det overordnede ansvar for Unit IT A/S' sikkerhedsarbejde.

Unit IT A/S har som styrende element, at informationssikkerheden er baseret på de reelle risici, som Unit IT A/S er udsat for. Derfor har vi med ISO 27005 som rammeværktøj vurderet risikostyringen som beskrevet nedenfor.

Etablerede forhold i risikostyring er vurderet geografisk, it-mæssigt og politisk med udgangspunkt i en kvalitativ konsekvens- og sandsynlighedsvurdering. Med respekt for at Unit IT A/S' omverden forandres, vil Unit IT A/S kontinuerligt vurdere behovet for tilretning af virksomhedens risikostyring.

	Forebyggende tiltag	**Udbedrende tiltag**
Administrative tiltag	Politikker og vejledning Awareness Change management CAB-board Technical management Compliance-kontroller Leverandørkontrakter Service- og supportaftaler Systemdokumentation	Beredskabsplaner Logning Disaster recovery-procedurer Procedure for major incidents
Fysiske og tekniske tiltag	Firewalls Antivirus Alarmsystemer Testmiljøer Monitorering Intrusion prevention Redundans Brugerstyring Clusters Passwordpolitik	Standbyudstyr Backup/restore Virtualisering Standbysite Server snapshots Intrusion detection Brandslukning Nødstrøm

Unit IT A/S benytter løbende eksterne partnere som Arrow ECS, Lenovo og HP, således at vi sikrer, at vores installation er udført og vedligeholdt efter best practice i forhold til teknik og sikkerhed.

Det er op til kunden at gøre krav på specifikke sikkerhedsrutiner eller tekniske installationer, såfremt best practice i forhold til teknik og sikkerhed jf. Unit IT A/S' standard ikke lever op til dette.

Kontrolmiljø

Unit IT A/S har valgt at bruge ISO 27000-serien som framework for etablering af kontrolmiljøet. Dette betyder, at komponenter fra ISO 27000-serien er gennemset og vurderet i forhold til implementering i virksomheden. Unit IT A/S anser ISO 27000 som værende en væsentlig sikkerhedsstandard i bestræbelserne på at oparbejde og adressere en compliant og konsistent tilgang til kontrolmiljø og it-sikkerhedspolitikkerne i Unit IT A/S.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (regelsæt for styring af informationssikkerhed), og Unit IT A/S har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger:

- Overordnede retningslinjer
- Organisering af informationssikkerhed
- Styring af informationsrelaterede aktiver
- Medarbejdersikkerhed
- Fysisk sikkerhed
- Styring af netværk og drift
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer
- Styring af sikkerhedshændelser
- Beredskabsstyring
- Overensstemmelse med lovbestemte og kontraktlige krav.

Unit IT A/S er opdelt i funktionelle forretningsenheder (se organisationsplan under punktet Risikostyring) og har derigennem gunstige muligheder for at arbejde struktureret med såvel vejledende som normative krav i ISO 27000-serien. Derudover giver den strukturelle opbygning gode betingelser for at tilvejebringe og opretholde et højt serviceniveau over for Unit IT A/S' kunder. Unit IT A/S anser højt serviceniveau og høj kundetilfredshed som værende essentielle i minimering af risici for Unit IT A/S.

Unit IT A/S ledes i dag af CEO Mark Frihagen, som referer til USTC-koncernen. Unit IT A/S har i øjeblikket ca. 70 medarbejdere ansat.

Operations-organisationen har i øjeblikket ca. 37 ansatte og består af følgende teams:

- Managed Services. Den primære funktion for dette team er at sikre stabil drift, maksimal oppetid og håndtere planlagte servicevinduer af de managed services, som leveres til virksomhedens kunder.

- Platform & Infrastruktur. Håndterer overvågning af servere, netværk, storage samt WAN-forbindelse, herunder VPN- og layer 2-forbindelser til kunder, samt servicevinduer på infrastrukturen i datacentre. Yderligere varetager teamet installation og tilpasning af Windows OS, Exchange og Citrix.

  Teamet er desuden ansvarlig for implementeringen af nye kunder, herunder styring af tidsplan.

  Teamet har også eksterne opgaver hos onsite-kunder uden for datacentrene. Licensrapportering håndteres ligeledes af teamet.

- Support-teamet. Den primære funktion for dette team er at levere brugersupport til de hostede løsninger, herunder også support af pc'er og MAC, samt at afhjælpe almindelige spørgsmål fra kunder.

  Support-teamet kører i toholdsskift, så det er fysisk bemandet fra kl. 6-21. Alle medarbejdere kan supportere på dansk og engelsk. Unit IT A/S leverer first level brugersupport til mere end 5.000 brugere.

- Service Desk er kontaktpunktet mellem kunder og vores medarbejdere. Formålet er at sikre, at kunden altid mødes med passende og rettidig hjælp i alle typer af henvendelser.

  Service Desk visiterer og koordinerer henvendelser om fx it-nedbrud, forespørgsler på nye opgaver, ændringer i kunders it-miljø og mindre projekter.

  Service Desks ansvar er kort fortalt at sikre, at de rette eksperter og specialister løser netop den givne opgave, og at det sker inden for den aftalte tidsramme og økonomi.

  Service Desk er designet til at håndtere flow for incidents (fx it-nedbrud), Service Requests (forespørgsel eller ny opgave) og Change Requests (ændring i it-miljø) og varetager Vendor Management.

  Service Desk-telefonen er åbne 24/7 for henvendelser om kritiske hændelser, der kræver her-og-nu-assistance.

- Service Delivery Management sikrer, at de i kontrakten aftalte ydelser leveres rettidigt og i den aftalte kvalitet.

  Service Delivery Management varetager al afrapportering af driftsydelser samt målinger på KPI og SLA og afholder driftsstatus- og styregruppemøder med repræsentanter fra både kunde og leverandør.

  Service Delivery Management er ligeledes eskalationspunkt, i tilfælde af at der opstår tvister, og fungerer som Situation Manager i kritiske incidents døgnet rundt.

  Service Delivery Management fungerer, hvor kunden ønsker det, som trusted advisor for kunden og som koordinator mellem kunde og tredjepartsleverandører.

Herudover er der en organisation til håndtering af Salg & Marketing, SQL/BI, Finans og Innovation. (Se ovenstående organisationsdiagram).

Organisering af informationssikkerhed

Unit IT A/S har med udgangspunkt i ISO 27001 kvalitativt vurderet, hvilke sikkerhedsforanstaltninger og kontrolprocedurer som Unit IT A/S tager eller vil tage i anvendelse. Vi er opmærksomme på det forhold, at dette vigtige arbejde er en dynamisk proces, og tager hensyn til dette i virksomhedens daglige virke samt i det eksisterende og kommende strategiarbejde.

Unit IT A/S har strategisk tilvalgt at tilbyde kunderne høj oppetid og tilgængelighed. Dette fordrer et kontinuerligt fokus på forhold, der fastholder og forbedrer driftssikkerheden i Unit IT A/S.

Unit IT A/S er fokuseret på et lavt men væsentligt antal kunder og har formuleret tydeligt i den eksisterende 3-årige strategi at være mere for disse og større kunder.

Unit IT A/S har formuleret mål og handlinger i den nuværende strategi, som har til formål at adressere udefrakommende faktorer, som kan udgøre en risiko for informationssikkerheden.

På de indre linjer har vi formuleret en informationssikkerhedspolitik, som er forankret i virksomhedens personalehåndbog. Personalehåndbogen er lettilgængelig for alle medarbejdere på virksomhedens intranet, og alle medarbejdere tilgår vilkår og rammer ved ansættelse i Unit IT A/S.

Unit IT A/S benytter et centralt logsystem med overbyggende sikkerhedsfunktionalitet og ekstern trussels-information til at opsamle log fra væsentlige administrative systemer for senere opdagelse af unormal adfærd.

I Unit IT A/S foretages den interne administrative sikkerhedsfunktion af CISO. Ansvaret for den tekniske sikkerhed er placeret i Security. Funktionen sikrer implementering og ajourføring af sikkerheds- og kvalitetsprocedurer, forestår den primære kontakt til revisorer/auditorer, sikrer udførelse af egenkontroller, sikrer løbede vedligeholdelse af risikovurderingen samt sikrer, at der findes en beredskabsplan og at denne bliver løbende ajourført.

Den enkelte medarbejder har til stadighed pligt til at følge den faglige udvikling inden for sit område samt holde sit uddannelsesniveau ajour. Medarbejderen er berettiget og forpligtet til relevant videreuddannelse, som aftales med nærmeste overordnede. Unit IT A/S afholder alle omkostninger til denne uddannelse. To gange årligt følges i MUS-samtaler op på uddannelse – for enkelte medarbejdere er der lavet en plan for et år ad gangen. Dette står i referatet fra MUS-samtalerne, hvor andre personlige forhold også er beskrevet.

Unit IT A/S' generelle politikker og forretningsgange er beskrevet i dokumentet "Generelle forretningsgange og driftsrutiner".

Ansvaret for sikkerhedspolitik, beredskabsplaner, driftsrutiner og beskrivelse af forretningsgang ligger hos ledelsen. Det er ledelsen, der kommunikerer eksternt med fx pressen. Ansvaret for formidling af forretningsgang og interne rutiner ligger hos ledelsen. Ved opdatering/rettelser er det ledelsens ansvar at formidle og forankre disse.

Styring af informationsrelaterede aktiver

Vi har kontrakter på aftalte ydelser for alle vores kunder. Særlige forhold er beskrevet heri, som de var ved aftaleindgåelse. Ændringer hertil er beskrevet i bilag til kontrakt og vedlagt kundens godkendelse implementeret i Unit IT A/S' administrative og operationelle systemer.

Medarbejdersikkerhed

Ledelsen i Unit IT A/S vil sikre, at alle medarbejdere er bekendt med deres roller og ansvar, og at alle er kvalificerede og egnede til at udføre deres rolle.

Alle medarbejdere skal leve op til den rolle, som er tilegnet dem, samt følge vores procedure. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres for herigennem at passe særligt godt på vores kunders data og udstyr og dermed vores eksistensgrundlag.

Vi har en procedure og tjekliste for ansættelse af medarbejdere og etablering af samarbejde med ledere, hvor vi sikrer, at vi ansætter den rigtige kandidat ift. baggrund og kompetence.

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, samt personalehåndbogen, hvor forhold omkring alle sider af ansættelsen, herunder ophør, er angivet.

Fysisk sikkerhed

Adgangskontrol, eksterne

Alle besøgende skal indskrives i logbogen, der findes i receptionen. Ud over dette skal alle besøgende bære synligt gæstekort.

Adgangskontrol til datacentre

Unit IT A/S råder over to driftscentre, som foruden at være beskyttet af et normalt alarmsystem, der sidder i huset, også har et ekstra alarmsystem, som kun dækker driftscentrene. Der skal indtastes en 4-cifret kode for at slå alarmsystemet fra og til. Koden er personlig for den enkelte medarbejder, og Operations varetager og vedligeholder disse.

Foruden en kode benyttes der 3D-ansigtsscanner til kontrol i datacenter 1 og datacenter 2, dvs. begge centre har foruden en kode også fysisk adgangskontrol.

Begge datacentre kan tilgås af autoriseret personale 24/7-365. Begge datacentre er overvåget med video, og det er begge kølegrave også.

Datacenteret i Kolding er styret af Global Connect, og Unit IT A/S' medarbejdere har adgangskort for at tilgå datacenteret i Kolding. Har kortet ikke været brugt i 3 måneder, bliver det automatisk spærret og skal genåbnes.

Styring af netværk og drift

Overordnet beskrivelse af datacentre

I Unit IT A/S' datacenter 1 og datacenter 2 sker den primære datadrift. Datacenter 1 og datacenter 2 er placeret på samme matrikel, men er to separate datacentre med redundante, fremførte datalinjer fra bl.a. TDC. Hvert datacenter har sin egen særskilte infrastruktur til køl, nødstrømsgenerator, UPS etc.

Datacentrene er forbundet med flere fiberforbindelser og driftes uafhængigt af hinanden, således at kundernes it-installationer fordeles hen over begge datacentre og derved nedbringer risikoen for nedetid. Datacenter 3 i Kolding anvendes som lokation til disaster recovery.

Bygningen, som huser datacenter 1 og datacenter 2, er beskyttet af udvendig videoovervågning samt adgangskontrol på døre.

Kun særligt autoriseret personel med et driftsmæssigt behov for adgang hertil er tildelt adgang til datacenter 1 og datacenter 2. Der skal benyttes adgangskort samt unik kode for at tilgå slusen i begge datacentre. I slusen anvendes 3D ansigtsscanner i kombination med adgangskort for adgang til selve datacenteret.

Beskrivelse af datacenter 1:

- UPS nødstrøm med batteribackup
- Nødstrømsgenerator
- Brandsikring med dysedæmpere
- Frikøleanlæg
- Fysisk adgangskontrol ved hjælp af en 3D-ansigtsscanner
- 24-timers overvågning af serverrummet tilkoblet Dankontrols alarmcentral med alarmer for fugt, temperatur, brand, UPS og nødstrømsgenerator
- Fysisk reservedelslager
- Videoovervågning.

Beskrivelse af datacenter 2:

- UPS nødstrøm med batteribackup
- Nødstrømsgenerator
- Brandsikring med dysedæmpere
- Frikøleanlæg
- Fysisk adgangskontrol ved hjælp af en 3D-ansigtsscanner
- 24-timers overvågning af serverrummet tilkoblet Dankontrols alarmcentral med alarmer for fugt, temperatur, brand, UPS og nødstrømsgenerator
- Videoovervågning.

Backup og disaster recovery

Medmindre andet er aftalt, foretager Unit IT databackup af alle servere. Kunden har mulighed for at fravælge dette og i stedet levere sin egen backupløsning. For virtuelle servere tages der desuden som standard en disaster recovery-backup. Dette kan ligeledes fravælges af kunden.

Unit IT A/S' formåen til genetablering af et it-miljø bygger både på databackup og disaster recovery-backup.

Disaster recovery-backup

Ved at benytte Disaster recovery-backup kan en virtuel servers operativsystem meget hurtigt genskabes i et vilkårligt datacenter. Data kan gendannes i begge vores datacentre eller alternativt i datacenter 3, som er lokaliseret i Kolding 27 km fra Unit IT A/S' datacenter 1 og datacenter 2. Alle datacentre er forbundet med 10Gbit fiber for højeste hastighed.

Til at foretage disaster recovery (DR) benyttes der Veeam Backup & Replication, og data lagres på datacenter 3 i Kolding.

Der tages som udgangspunkt DR-backup af C-drevet på alle virtuelle servere en gang i døgnet med 7 dages historik, medmindre andet aftales med kunden.

Unit IT udfører kvartalsvise restore tests på DR-platformen for at kontrollere backupsystemets funktionalitet i forhold til at genskabe data. Disse restore tests validerer alene systemets evne til at genskabe data og kan ikke erstatte slutkundens behov for test og validering af datagenskabelse fra backup.

Unit IT opfordrer alle kunder til med jævne mellemrum at validere integriteten af deres backupdata.

Unit IT kontrollerer dagligt, at alle definerede DR-backups er udført som planlagt. I tilfælde af fejl registreres denne, og der foretages korrigerende handling for at sikre en valid backup. Afvigelser omkring ikkeønsket DR-backup er fastholdt i kundens CMDB på den pågældende server.

Nye virtuelle servere inkluderes som standard i DR-backup. Unit IT foretager ugentlige kontroller, som sikrer, at der ikke er virtuelle servere uden DR-backup, hvor dette ikke eksplicit er fravalgt af kunden.

Databackup

Til databackup bruges IBM Spectrum Protect-teknologi (tidligere kendt som TSM eller Tivoli Storage Manager). Backupdata er placeret i to separate datacentre 98 km væk fra Unit IT A/S' driftscenter hos Front-Safe i Århus. Vi har specialister på alle niveauer og inden for alle områder, der har tværgående kompetencer inden for de brugte teknologier.

Alle servere, både fysiske og virtuelle, benytter denne backup. Som udgangspunkt krypteres data med en af kunden valgt krypteringsnøgle. Dette sikrer, at de lagrede backupdata ikke er læsbare for andre end kunden selv. Kunden ejer krypteringsnøglen til backupdata, men gør denne tilgængelig for Unit IT, i det omfang driften af backup kræver dette. Der benyttes fil- og databaseagenter. Databaseagenter til fx SQL kan sikre, at der tages helt ned til timebackup af SQL-data, hvis det ønskes.

Der foretages inkremental backup af alle data én gang i døgnet, medmindre andet aftales med kunden.

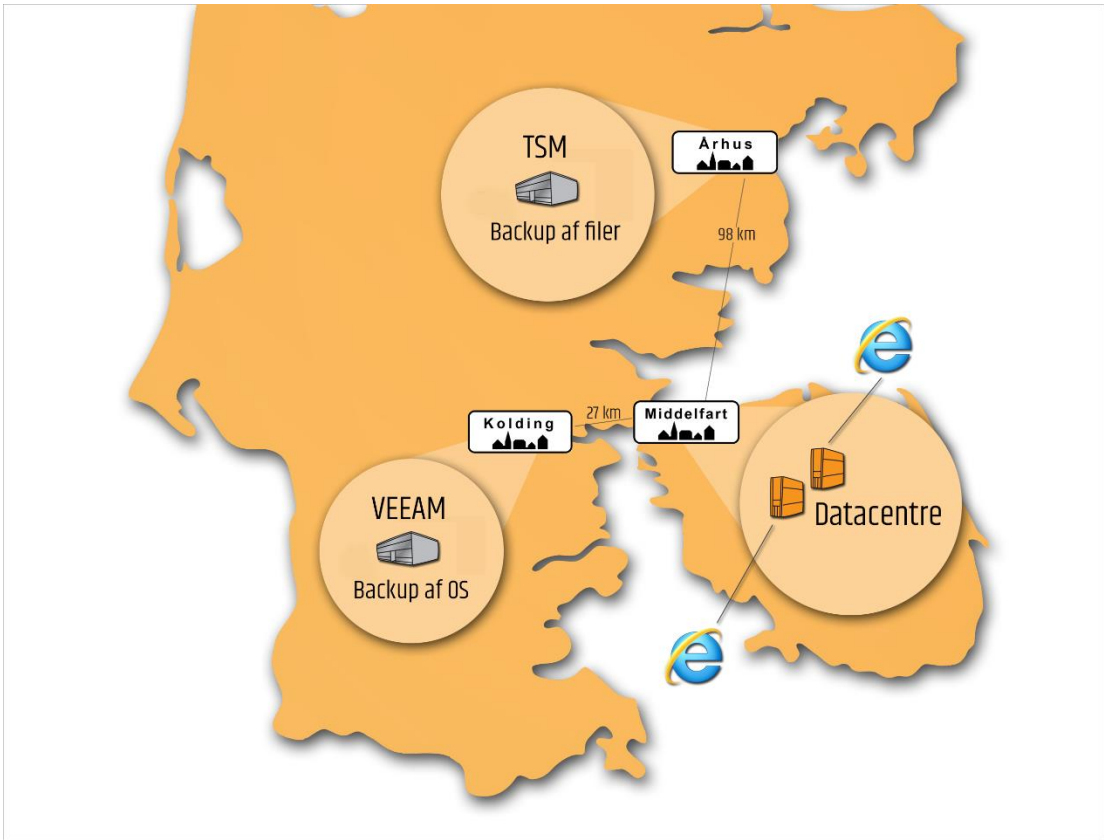
I en standarddatabackup sendes data direkte til Front-Safes IBM Spectrum Protect backupservere og storage. Derefter bliver kundens data kopieret til Front-Safes secondary data store, som har en anden fysisk lokation. Med Cloud backup-løsning har kunden 2 offsite-kopier af egen data.

For at imødegå høje krav til performance, restore-tider eller datareduktion har kunden mulighed for at tilvælge en hybrid backupløsning i stedet for standarddatabackup. I hybridløsningen har kunden en lokal kopi og en offsite-kopi af sine backupdata. Kunden har en lokal IBM Spectrum Protect-server, som er en Front-Server. Denne Front-Server synkroniserer sin backup-storage med datalageret på Front-Safes backupservere.

Unit IT kontrollerer dagligt, at alle definerede databackups er udført som planlagt. I tilfælde af fejl registreres denne, og der foretages korrigerende handling for at sikre en valid backup.

Unit IT foretager ugentlige kontroller, som sikrer, at der ikke er servere uden databackup, hvor dette ikke eksplicit er fravalgt af kunden. Afvigelser omkring ikke ønsket databackup er fastholdt i kundens CMDB på den pågældende server.

Principskitse, backup og disaster recovery



Vedligeholdelse af systemer

Patch management-strategi

Der installeres opdateringer i kategorierne Security Updates, Critical Updates og Optional Updates. Hermed kan patchninger klassificeres i forhold til relevans og vigtighed for hver kunde. Unit IT A/S tilbyder månedlig patchning af alle versioner af Windows Server, som er under aktiv maintenance fra Microsoft. Ud fra den enkelte kundes krav til løsningens tilgængelighed defineres tidspunkt (patch-tag).

Kunden har desuden mulighed for at tilvælge automatisk patchning af standardapplikationer som fx internetbrowsere, Adobe Reader og Adobe Flash, hvis disse er installeret på kundens løsninger. For at sikre mod kendte sårbarheder i disse standardapplikationer anbefales Unit IT A/S' kunder at benytte sig af dette.

Unit IT A/S validerer løbende, at opdateringer til operativsystemer såvel som applikationer installeres korrekt i nyeste tilgængelige version.

Change management-strategi

Unit IT A/S' strategi på dette område tilsikrer, at ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgang og processer. Dette sker bl.a. via disse midler:

- At der sker registrering og beskrivelse af ændringsanmodninger
- At alle ændringer er underlagt formel godkendelse inden idriftsætning
- At ændringer er underlagt formelle konsekvensvurderinger

- At der beskrives fallback-planer, hvor det er muligt
- At der sker identifikation af systemer, der påvirkes af ændringer
- At der sker en dokumenteret test af ændringer inden idriftsætning, hvor det er muligt
- At dokumentation opdateres, så den i al væsentlighed afspejler de påførte ændringer
- At procedurer er underlagt styring og koordination i Unit IT A/S' ITSM-system.

Changes opgøres på to måder, der tager udgangspunkt i vurdering af impact og sandsynlighed. Derved foretages en egentlig klassifikation af changes. Der udfærdiges dog altid en change form.

Hvis denne change form er LOW i impact, sandsynlighed og classification, kan den udføres uden godkendelse af den enkelte tekniker. Changes, som har en anden klassifikation end beskrevet, skal godkendes af en leder i Operations. Det er Unit IT A/S' SDM-funktion, der verificerer, at change-formularen er udfyldt jf. kravene, inden den sendes til godkendelse.

Adgangsstyring

Adgang til it-systemer

Den logiske sikkerhed omfatter logisk beskyttelse af elektroniske systemer og information, der vedrører serviceydelsen. Fx fastlægger den, at kun autoriserede personer har adgang hertil.

Unit IT A/S' strategi på området tilsikrer, at medarbejderne får stillet tilstrækkelige arbejdsredskaber til rådighed, og at disse redskaber kontinuerligt sikres i takt med sikkerhedstiltag. Unit IT A/S ønsker at være en fleksibel og attraktiv arbejdsplads, hvorfor der tilbydes muligheder for remote opkobling til såvel egne som kundernes it-systemer. For at sikre disse er nedenstående elementer taget i anvendelse.

Adgangsmuligheder

Adgang til Unit IT's administrative netværk og administrationssystemer er kun muligt for autoriserede personer, og kræver 2-faktorvalideret adgang. Autorisation kan ske via kombination af brugernavn/password og engangskode (OTP) eller via kombination af brugernavn/password og en godkendt computer, der er autoriseret via et unikt certifikat (802.11x).

Operationelle systemer kan kun tilgås via en yderligere adgangskontrol, som ligeledes er 2-faktorvalideret. Der benyttes sekundære brugernavne og passwords for adgang til operationelle systemer, og det samme gør sig gældende for al adgang til kundesystemer.

Al kommunikation med både administrative systemer, operationelle systemer og kundesystemer, som ikke sker fra en Unit IT-lokation, sker krypteret.

Unit IT A/S har givet tilladelse til, at der kan benyttes mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Adgang til disse data styres via AD-opsætning. Alle enheder, der synkroniseres, låses med kode efter 15 minutter, og dette er ikke muligt at ændre for den enkelte medarbejder.

Unit IT's passwordpolitik består af 12 tegn med tal, store bogstaver og specialtegn. For standardbrugere skal password skiftes hver 60. dag. Adgange til kundesystemer er tildelt ud fra et arbejdsrelateret behov og styres via en administratorkonto for den enkelte medarbejder. Passwordpolitikken er den samme som for en standardbruger. Ved behov for at en ekstern skal logge på, oprettes denne med bruger og midlertidig adgang, som lukkes, efter opgaven er afsluttet.

Det er et krav, at medarbejdernes personlige pc'er låses eller logges af, så snart arbejdspladsen forlades, for at forhindre utilsigtet adgang.

Begge datacentre er overvåget elektronisk af Dankontrol. Dvs. hver aften kigger de på, om der er koblet alarm til kl. 20:30, senest. Hvis ikke, ringes der til vagten, og på denne måde sikres tilkobling af alarm.

Alle pc'er er beskyttet af en harddisklås, så data ikke kan tilgås ved tyveri eller anden bortkomst.

Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer

Unit IT A/S vil sikre, at alle nyanskaffelser og implementering af servere, systemer, services og software håndteres på struktureret og sikker vis.

For opgaver af en vis størrelse – det kan være væsentlige ændringer i vores generelle driftssystem på tværs af kunder eller implementering af kundeløsninger – har vi en procedure, og enten håndteres de via change management eller vores project manager (projektstyringsmodel).

Vores projektstyringsmodel er baseret på vores egen og praktiske metodik, men er inddelt i en rækker faser: foranalyse, design, test, implementering, test og evaluering. Hver fase indeholder accept fra interessent.

Styring af sikkerhedshændelser

Unit IT A/S arbejder med it-sikkerhed på et forretningsstrategisk og risikobaseret niveau gennem Unit IT's IT-Sikkerhedsudvalg. IT-Sikkerhedsudvalget er repræsenteret af den øverste ledelse, CEO, CFO, COO og CISO, hvor udvalget refererer direkte til bestyrelsen. Udvalget behandler it-sikkerhedsspørgsmål af væsentlig karakter og effektueres gennem politikker, procedurer og guidelines. Unit IT's CISO har direkte reference til CEO'en, hvor der foretages afrapportering om Unit IT's trusselsniveau.

Unit IT A/S er medlem af NC3Skyt hos Center for Cybersikkerhed (NC3) under Forsvarets Efterretningstjeneste og modtager desuden ugentlig trusselsinformation fra European Cybercrime Centre (EC3).

Vores medarbejdere indgår i en vagtordning, således at vi kan reagere 24 timer i døgnet. Opstår en hændelse uden for normal arbejdstid, er det den vagthavende medarbejder, der vurderer, hvilken reaktion der skal ske. Herefter foretages det fornødne for at orientere kunder og omverden. Dette sker ved at involvere Situation Management-vagten, som består af SDM'erne.

Sker en hændelse inden for normal arbejdstid, vil medarbejderne håndtere og eskalere sagen på samme vis som andre sager, og med den prioritering som er nødvendig.

Det er medarbejdernes ansvar at rapportere sikkerhedsbrister eller mistanke herom til ledelsen omgående. Ligeledes vil virksomhedens overvågningssystem være opsat til at identificere udvalgte sikkerhedsbrister.

Vi holder os fagligt opdaterede vha. producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Via vores medlemskab af Danish Cloud Community (=DCC) er vi forpligtet til at sikre, at kritiske sikkerhedsopdateringer implementeres inden for to måneder efter frigivelse. Dette sikrer vi ved, at alle væsentlige opdateringer afvejes og implementeres inden for tidsrammen.

Beredskabsstyring

Information og kommunikation

Det er den enkelte teamleders ansvar at kommunikere internt i Unit IT A/S. Det er ledelsen, der er ansvarlig for kommunikationen ud til kunder og presse. Rapportering udarbejdes af de enkelte enheder og godkendes af ledelsen, inden den sendes til kunden.

Måden, der kommunikeres på, er afspejlet i Unit IT A/S' vejledning til håndtering af Major Incidents. Heri fremstår telefonisk kontakt, SMS-kommunikation og mails i en struktureret kommunikationsplatform, som Unit IT A/S benytter. Det er ligeledes i proceduren defineret, hvem der i Unit IT A/S kommunikerer hvad, hvordan og til hvem. Proceduren er defineret ud fra roller og ikke enkeltpersoner i Unit IT A/S.

Beredskabsplaner

Identifikation af kritiske processer

Indsatsen med at udarbejde forretningsnødplaner er identificeret, og arbejdet vil i takt med identificeret behov blive udført. I sammenhæng med de tekniske beredskabsplaner vil disse håndteres af den samlede ledelse i Unit IT A/S.

Kommunikation i situationen

Et af hovedelementerne i en succesfuld styring af en beredskabssituation er at sikre en passende kommunikation til alle relevante interessenter i rette tid og med det rette indhold. Kommunikation skal sikre, at organisationens interessenter informeres så godt om situationen, at forvirring minimeres mest muligt.

I Unit IT A/S er der kortlagt en ønsket kommunikationsform og rollefordeling berammet i et framework omhandlende Major Incidents. Ansvaret for vedligeholdelse af denne proces og rollefordeling påhviler ledelsen i Unit IT A/S. Proceduren for håndtering af Major Incidents er tilgængelig for alle medarbejdere på virksomhedens intranet og forefindes ligeledes i hardcopy i virksomheden.

Den effektive kommunikation forventes at forebygge et unødigt stort antal henvendelser om hændelsen og unødigt forbrug af tid og kræfter frem for at håndtere selve situationen. Kommunikation skal også sikre, at interessenterne får de fornødne oplysninger til at kunne minimere eventuelle følgevirkninger og til at kunne etablere eventuelle alternative løsninger.

Beredskab for kommunikation skal i lighed med teknisk beredskab afprøves, hvilket sker, når der indtræffer en hændelse. Derudover revurderes processen kvalitativt løbende.

Minimumskrav for god hosting anser Unit IT A/S som væsentligt, og Unit IT A/S sikrer gennem sin procedure, at Unit IT A/S til enhver tid lever op til de gældende krav til god hosting, som Brancheforeningen for IT-hostingvirksomheder måtte kræve.

Teknisk beredskab

Unit IT A/S' tekniske beredskabsplaner er sammenfattet i procedurebeskrivelse omhandlende Generelle procedurer og driftsrutiner 1.17 og omhandler bl.a. FrozenZone, nødstrøm og test heraf, backup, brandslukning, Denial-of-Service, oprettelse og sletning af medarbejdere.

Kontrolaktiviteter

Unit IT A/S anvender kun standardsystemer. Katastrofeplan er tilgængelig på intranettet. Desuden findes en kopi på datacenter 3. Detaljerne fremgår af kontrolmål og kontrolaktiviteter ifølge skema med oplistning og test heraf.

Overensstemmelse med lovbestemte og kontraktlige krav

Vi lader os årligt revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelse af kontrollerne nævnt i denne beskrivelse. I kraft af at vi er medlemmer af Danish Cloud Community, skal vi årligt attestere, at vi følger rammerne inden for ISAE 3402. Omtalte revisorerklæring sikrer dette, ligesom Danish Cloud Community ønsker ekstern revisors bekræftelse på vores overholdelse af foreningens øvrige krav omhandlende forsikringsforhold, gennemsigtighed i forretningsvilkår, selskabsretlige forhold for vores virksomhed mv. Disse bekræftelser fra revisor er en hjælp til Danish Cloud Communitys certificering af vores virksomhed.

3 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 2020 til 31. december 2020 i relation til Unit IT A/S' it-drift og hosting-aktiviteter til kunder

Til: Unit IT A/S samt kunder af Unit IT A/S' it-drift og hosting-aktiviteter og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Unit IT A/S' beskrivelse i afsnit 2 af deres generelle it-kontroller i relation til Unit IT A/S' it-drift og hosting-aktiviteter, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2020 til 31. december 2020, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Unit IT A/S anvender Front-Safe A/S som serviceunderleverandør for opbevaring af backupdata. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Front-Safe A/S varetager for Unit IT A/S.

Unit IT A/S' ansvar

Unit IT A/S 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 FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Unit IT A/S' beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, 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 sin it-drift og sine hosting-aktiviteter samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, 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 Unit IT A/S 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

Unit IT A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved it-drift og hosting-ydelser, 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, hvordan generelle it-kontroller i relation til it-drift og hosting-aktiviteter, således som de var udformet og implementeret i hele perioden fra 1. januar 2020 til 31. december 2020, i alle væsentlige henseender er retvisende, 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 2020 til 31. december 2020, 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 2020 til 31. december 2020.

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 Unit IT A/S' it-drift og hosting-aktiviteter 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 7. januar 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
statsautoriseret revisor

Iraj Bastar
director

4 Kontrolmål, kontrolaktiviteter, 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 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 2020 til 31. december 2020. 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 A: Informationssikkerhedspolitik

Ledelsen har udarbejdet en informationssikkerhedspolitik, som udstikker en klar målsætning for it-sikkerhed, herunder valg af referenceramme samt tildeling af ressourcer. Informationssikkerhedspolitikken vedligeholdes under hensyntagen til en aktuel risikovurdering.

Kontrolmål/kontrol	PwC-test	Resultat af test
Skriftlig politik for informationssikkerhed Unit IT A/S har udarbejdet en sikkerhedspolitik. Denne er til rådighed for medarbejdere på intranettet. Den revideres mindst én gang årlig. Den er godkendt af ledelsen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum er revurderet én gang årligt. Endvidere har vi påset, at den forefindes let tilgængelig for medarbejderne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

Det organisatoriske ansvar for informationssikkerhed er passende dokumenteret og implementeret, ligesom håndtering af eksterne parter sikrer en tilstrækkelig behandling af sikkerhed i aftaler.

Kontrolmål/kontrol	PwC-test	Resultat af test
Ledelsens forpligtelse i forbindelse med informationssikkerhed Den enkelte afdelingsleder er ansvarlig for, at nye medarbejdere gøres bekendt med retningslinjerne som en del af introduktionen til virksomheden. I takt med at der sker opdatering af retningslinjerne, vil der blive givet besked herom via mail og USTC-nettet, hvor man også kan finde den ajourførte og gældende version af sikkerhedspolitikken.	Vi har overordnet drøftet styring af informationssikkerheden med ledelsen. Vi har påset, at det organisatoriske ansvar for informationssikkerheden er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Eksterne parter Unit IT A/S beder samarbejdspartnere og eksterne leverandører om at sende revisorerklæring vedrørende de aftalte serviceydelser eller underskriver en kontrakt, der beskriver fortrolighed og sikkerhedsforanstaltninger. Unit IT A/S sikrer, at eksterne partnere er bekendt med Unit IT A/S' sikkerhedspolitik.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret betryggende procedurer for samarbejdet med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter, og vi har påset, at der er modtaget revisorerklæring fra backupleverandører for den relevante periode.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader forårsaget af fysiske forhold som fx brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/kontrol	PwC-test	Resultat af test
Fysisk sikkerhedsafgrænsning Alle medarbejdere hos Unit IT A/S har adgang til lokalerne ved hjælp af alarmsystemer. Kontorerne låses automatisk kl. 16.30 og åbnes kl. 7.30. Uden for åbningstiden skal medarbejdere bruge kode og brik for at få adgang til bygningen. Datacentre er adgangsreguleret ved hjælp af kode på døren til værkstedet og 3D-ansigtsscanner til datacentre. Adgang til datacentrene bliver tildelt efter arbejdsmæssigt behov. Datacentrene er videoovervågede. Unit IT A/S kan herved dokumentere handlinger i datacentrene. Gæster bliver ledsaget af en medarbejder med adgang til datacenteret.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har under vores besøg i Unit IT A/S' datacentre observeret, at adgang til sikre områder er begrænset ved anvendelse af adgangssystem. Vi har ved stikprøvevis inspektion gennemgået procedurerne for fysisk sikkerhed vedrørende de sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt om personer uden godkendelse til de sikrede områder skal registreres og ledsages af en medarbejder med behørig godkendelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikring af kontorer, lokaler og faciliteter Datacentre er adgangsregulerede ved hjælp af kode på døren til værkstedet og 3D-ansigtsscanner til datacentre. Bygningerne er videoovervågede og besøges uden for arbejdstid af et vagtselskab minimum fire gange pr. døgn.	Vi har forespurgt ledelsen om de anvendte procedurer. Vi har gennemført inspektion af alle serverrum og påset, at alle adgangsveje er sikret med kortlæser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Placering og beskyttelse af udstyr I datacentre er installeret Inergen-anlæg, temperaturmåling og videoovervågning. Inergen-anlæg testes én gang om året ifølge gældende lovgivning. Testen udføres af RMG-Inspektion A/S, og der foreligger en godkendt erklæring. Ledelsen og driftsvagten modtager alarmer både på sms og mail ved eventuelle hændelser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion gennemgået driftsfaciliteterne og har påset, at der er etableret de fornødne kontroller i form af: • Brandbekæmpelsessystemer • Fugtsikring • UPS og generatorforsyning • Fysisk adgangskontrolsystem • Overvågning af indeklima. Vi har ved stikprøvevis inspektion gennemgået dokumentationen for vedligeholdelse af udstyr til bekræftelse af, at dette løbende vedligeholdes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader forårsaget af fysiske forhold som fx brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/kontrol	PwC-test	Resultat af test
Understøttende forsyninger (forsyningssikkerhed) Datacentre er beskyttet mod strømafbrydelse ved anvendelse af UPS. Dieselgenerator overtager strømforsyning efter beskrevet tidsplan. Dette testes hver måned. Brændstofniveau aflæses løbende.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har under vores besøg i datacentrene observeret, at der foretages monitorering af UPS eller nødstrømsanlæg. Vi har ved stikprøvevis inspektion gennemgået dokumentationen for vedligeholdelse til bekræftelse af, at UPS eller nødstrømsanlæg løbende vedligeholdes og testes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikring af kabler Kabler og elforsyning ligger i kabelbakker. Krydsfelt og tilhørende netværksenheder forefindes alle i datacentre.	Vi har ved inspektion observeret, at kabler til elektricitetsforsyning og datakommunikation er sikret mod skader og uautoriserede indgreb.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift og brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed og fortrolighed.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Dokumenterede driftsprocedurer Unit IT A/S har beskrevet driftsprocedurerne for driftsmiljøet. Der gennemføres et dagligt tjek af serverrum. Efterfølgende bliver der udarbejdet en daglig rapport, der bliver godkendt af ledelsen hver dag. Unit IT A/S har tre forskellige typer medarbejdere; support, drift og konsulent (storage, firewall og adgangskontrol ligger hos drift). Adgang til fællesdrev er tildelt i forhold til funktion. Til hver stilling findes en stillingsbetegnelse. Unit IT A/S har ingen udviklings- eller applikationsvedligehold.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenteret. I forbindelse med revision af de enkelte driftsområder er det ved inspektion kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. Vi har endvidere ved inspektion påset, at der foretages tilstrækkelig overvågning og opfølgning herpå.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Funktionsadskillelse Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen. Disse politikker og procedurer omfatter krav til, • at ansvar for udvikling og opdateringer til produktionsmiljøet er adskilte • at it-afdelingen ikke har adgang til applikationer og transaktioner • at udviklings- og driftsaktiviteter er adskilte.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen mellem udviklings- og produktionsmiljøer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Foranstaltninger mod virus og lignende skadelig kode Der er installeret antivirusprogrammer, som bliver opdateret regelmæssigt. Unit IT A/S benytter anerkendt værktøj til antivirus med automatisk versionskontrol.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion gennemgået den tekniske opsætning, til bekræftelse af at der er installeret antivirusprogrammer, samt at disse er opdaterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift og brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed og fortrolighed.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Sikkerhedskopiering af informationer Backup og validering foretages til Front-Safe A/S. En kunde udvælges i rækkefølge pr. kvartal for test af restore-proceduren. Der benyttes Veeam til backup/restore af virtuelle servere. Veeam benyttes som disaster recovery-backup, der kun skal sørge for at bringe systemdrev i drift, hvorefter data på andre drev genetableres med TSM. Veeam benyttes til hurtig backup og reetablering og bruges løbende i driften efter aftale med kunden. Dermed testes det løbende, om backup er valid.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået backupprocedurer samt påset, at de er tilstrækkelige og formelt dokumenteret. Vi har gennemgået aftalen med Front-Safe A/S samt påset, at proceduren for backup er i overensstemmelse med de i kontrakten beskrevne oppetidsmål. Vi har ved stikprøvevis inspektion gennemgået log vedrørende backup, til bekræftelse af at backupper er gennemført fejlfrit, alternativt at der foretages afhjælpning i tilfælde af mislykkede backupper.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Monitorering af systemanvendelse og auditlogning Der er implementeret logning ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl. Unit IT A/S har ikke ansvaret for opsætning og drift af databaserne. Alle brugeres rettigheder bliver kontrolleret mindst én gang om året eller ved til-/afgang af medarbejdere. Alt hardware er overvåget. Der afsendes rapport i tilfælde af fejl. Endvidere er der sat infotavle op, der giver overblik over installationen. Overvågningssystem sender sms og mail i tilfælde af fejl. **Administrator- og operatørlog** Unit IT A/S logger transaktioner og handlinger, der er gennemført af brugere og administratorer via domain controllers (AD) auditlog. Brugerkontis rettigheder på AD gennemgås halvårligt. Logge fra AD og andre væsentlige systemer bliver gennemgået løbende og ved begrundet mistanke om uautoriserede handlinger.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget. Vi har ved stikprøvevis inspektion påset, at der er etableret overvågning og alarmering for nedsat tilgængelighed samt for forsøg på brud på den etablerede sikringsforanstaltning. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logge fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Brugerregistrering og administration af privilegier Oprettelse og nedlæggelse af brugere er ledelsesgruppens (LG) ansvar. Brugerne oprettes i forhold til arbejdsrelaterede behov. Proceduren er godkendt af ledelsen. Alle brugeres rettigheder bliver kontrolleret mindst én gang om året eller ved til-/afgang af medarbejdere. Adgang til kundernes systemer er kundens ansvar. Derfor har Unit IT A/S ikke beskrevet dette. Brugere oprettes i grupper. Det er disse grupper, der har rettighederne til, hvad den enkelte medarbejder har adgang til. Det er LG, der beslutter, hvilke grupper en medarbejder skal være medlem af. LG vurderer løbende, om Unit IT A/S' medarbejdere har de rigtige rettigheder. Samtlige brugere i Unit IT A/S' AD og disses rettigheder bliver gennemgået minimum fire gange årligt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion påset, at det er LG, der godkender tildeling af adgang til systemerne, samt stikprøvevis kontrolleret, at forretningsgangene er overholdt for oprettede brugere på Unit IT A/S' systemer. Vi har foretaget stikprøvevis kontrol af, at årlige gennemgange foretages.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Administration af brugeradgangskoder (password) Der er implementeret programmerede kontroller, der sikrer, at password har den fornødne kvalitet, jf. sikkerhedspolitikkens bestemmelser. Password skal bestå af minimum 12 tegn, og tegnene skal være en blanding af tal og bogstaver. Password er gyldigt i maks. 60 dage og bør ikke genbruges.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og påset, at det sikres, at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har ved inspektion kontrolleret, at der anvendes en passende passwordkvalitet i Unit IT A/S' driftsmiljø, ved stikprøvevis test af, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Evaluering af brugeradgangsrettigheder Unit IT A/S foretager periodisk review af brugerrettigheder, til sikring af at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Uoverensstemmelser undersøges og rettes rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion kontrolleret, at der foretages periodiske gennemgange, til bekræftelse af at disse har fundet sted, samt påset, at identificerede afvigelser afhjælpes. Vi har endvidere stikprøvevis kontrolleret, at forretningsgangene er overholdt for oprettede brugere i Unit IT A/S' systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Inddragelse af adgangsrettigheder Brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver deaktiveret ved disse medarbejderes fratrædelse. Ledelsen godkender inddragelse af rettigheder og nedlæggelse af brugere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og at der foretages opfølgning i henhold til forretningsgangene på de tildelte adgangsrettigheder. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugere på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Politik for anvendelse af netværkstjenester, herunder autentifikation af brugere med ekstern forbindelse Al trafik til og fra internettet styres via en firewall. Opsætning af denne er elektronisk dokumenteret. Adgang fra fx hjemmearbejdsplads sker ved hjælp af VPN. Kunder har deres egen DMZ-zone. Ekstern adgang fra hjemmearbejdsplads eller eksterne samarbejdspartnere valideres ved hjælp af "SSL-VPN".	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og vi har påset, at der anvendes en passende autentifikationsproces for driftsmiljøet. Vi har ved stikprøvevis inspektion kontrolleret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN. Vi har ved inspektion konstateret, at netværket er segmenteret i mindre net ved hjælp af VLAN og DMZ for at reducere risikoen for uautoriseret adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Styring af netværksforbindelser Netværksforbindelser testes sammen med kunden, såfremt kunden ønsker dette. Unit IT A/S gennemgår firewallopsætning for at sikre unødig penetration. Som udgangspunkt er der lukket for trafik udefra. Ønsker kunder dette ændret, sker dette efter skriftlig anmodning.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at styre netværksforbindelser. Vi har ved inspektion konstateret, at der er foretaget periodiske penetrationstest, samt kontrolleret, at der er taget stilling til konstaterede svagheder. Vi har ved stikprøvevis inspektion gennemgået firewall-konfigurationen og påset, at reglerne i firewallen er sat hensigtsmæssigt op.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Begrænset adgang til informationer Kun personer med behov for adgang til kundespecifikke systemer har adgang. Alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med Unit IT A/S' politikker, til sikring af at rettigheder tildeles ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at begrænse adgangen til informationer. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion kontrolleret, at tildeling af adgang til data og systemer udføres ud fra et arbejdsrelateret behov og er godkendt i overensstemmelse med forretningsgangene.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

Kontrolmål/kontrol	PwC-test	Resultat af test
Styring af software på driftssystemer Unit IT A/S har separate udviklings-, test- og produktionsmiljøer. Unit IT A/S udvikler ikke software. It-miljøet for kundernes systemer er adskilt fra det interne it-miljø. Unit IT A/S benytter patch management til at styre fx OS-opgraderingen. Patchning af kundeservere aftales og accepteres i samarbejde med den enkelte kunde. Patchning udføres i aftalt servicevindue. Proceduren omfatter kun OS, da kunden selv har ansvar for applikationerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at adskillelse mellem de enkelte miljøer opretholdes. Desuden har vi forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at holde kritiske systemer opdateret, og vi har gennemgået opdateringsprocedurernes tilstrækkelighed, for så vidt angår Unit IT A/S' egne væsentlige systemer samt kundernes systemer i henhold til kontraktlige aftaler. Vi har ved stikprøvevis inspektion gennemgået ændringerne i perioden og påset, at disse er dokumenteret. Vi har endvidere stikprøvevis efterprøvet kontrollerne, herunder at: • der er tilstrækkelig kommunikation med leverandørerne med henblik på at modtage nødvendige informationer om kritiske og vigtige opdateringer, samt at der foretages de fornødne risikovurderinger af de enkelte opdateringer • de kritiske systemer er blevet opdateret hensigtsmæssigt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringsstyring Unit IT A/S bruger change management til at styre ændringer. Ændringer af daglige arbejdsopgaver er beskrevet i standard change, som er forhåndsgodkendt. Ingen ændringer i produktion implementeres, før change er godkendt af kunden og ledelsen samt testet, og fall-back-plan er udformet. Nødændringer uden om den normale forretningsgang testes og godkendes efterfølgende. Ingen ændring må udføres uden godkendelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået change managementprocedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Vi har ved stikprøvevis inspektion gennemgået ændringsønsker for følgende: • Registrering af ændringsanmodninger i det dertil etablerede system. • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. • Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. • Dokumenteret plan for tilbagerulning, hvor relevant.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål G: Katastrofeplan

Unit IT A/S er i stand til at fortsætte servicering af kunder i en katastrofesituation.

Kontrolmål/kontrol	PwC-test	Resultat af test
Opbygning/struktur af katastrofeberedskab Unit IT A/S har udarbejdet en katastrofeplan. Denne beskriver sandsynligheder og de nødvendige tiltag. Planen er godkendt af ledelsen og revideres årligt. **Test af katastrofeberedskab** Der sker årlig test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier. Såfremt testen afslører uhensigtsmæssigheder, opdateres planen umiddelbart herefter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået det udleverede materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.