Itadel A/S

Erklæring fra uafhængig revisor vedrørende generelle it-kontroller, der vedrører regnskabsaflæggelsen i tilknytning til Itadels hostingydelser

Januar 2020

Indhold

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Itadels hostingydelser, og disses 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. Itadel bekræfter, at:

(a) Den medfølgende beskrivelse i afsnit 2 giver en retvisende beskrivelse af Itadels hostingydelser til kunder i hele perioden fra 1. januar 2019 til 31. december 2019. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

- de typer af ydelser, der er leveret, når det er relevant
- de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- relevante kontrolmål og kontroller, udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets 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 sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

(ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar 2019 til 31. december 2019

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og disses revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for at være vigtigt efter dennes særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2019 til 31. december 2019. Kriterierne for denne udtalelse var, at:

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

(ii) de identificerede kontroller ville, hvis anvendt 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 2019 til 31. december 2019.

Aarhus, den 20. januar 2020
Itadel

Nils Lau Frederiksen
Information Security Manager, Itadel

2. Itadels beskrivelse af generelle it-kontroller, der vedrører regnskabsaflæggelsen i relation til Itadels hostingydelser

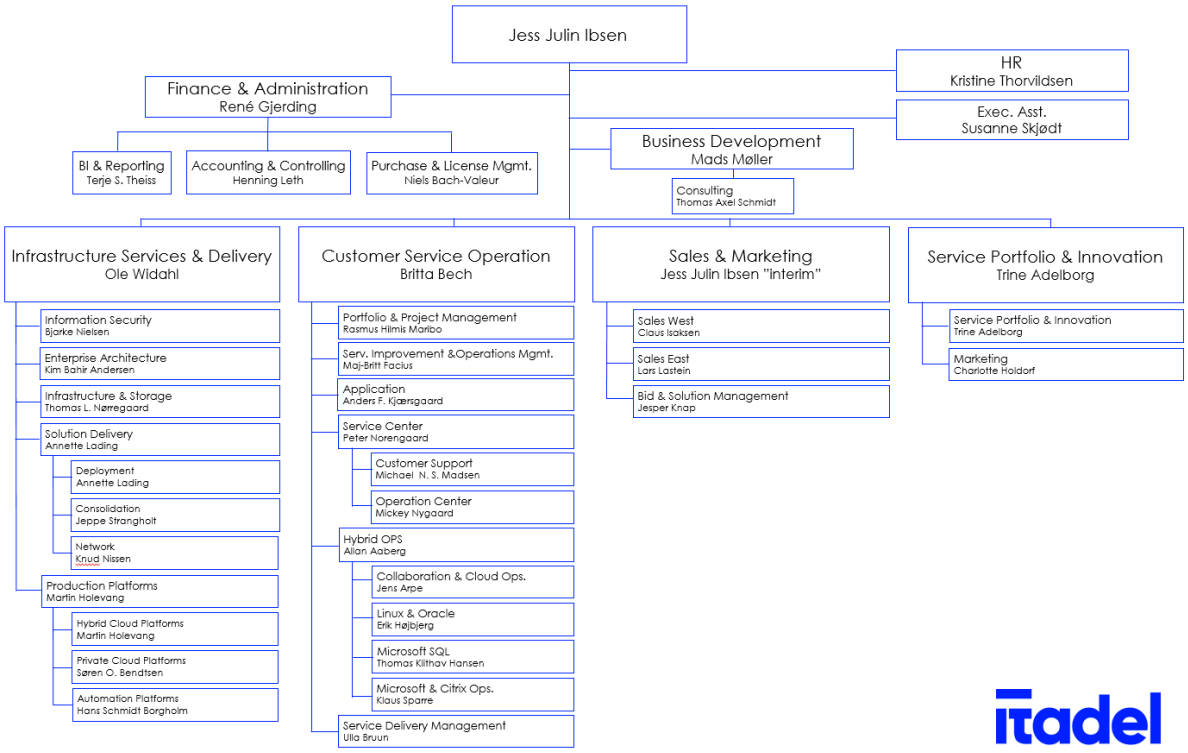
Vision
Vi vil være anerkendt for at være den it-outsourcingpartner, der leverer den højeste værdi og bedste service til vores kunder gennem leverance af sikre og skalerbare løsninger.

Mission
- Vores kunder oplever, at vi forstår deres forretning, tager ansvar og yder høj service.
- Vores kunder har lavere risici, da vi leverer sikker it-drift og databeskyttelse.
- Vores kunder kan fokusere på deres kerneforretning, fordi vi frigør ressourcer hos dem.
- Vores kunder får vores hjælp til digital transformation.
- Vi gør det let for vores kunder at gøre forretning med os.

Vores DNA:
- Vi er uformelle og i øjenhøjde – samtidigt er vi tilgængelige med fri adgang til højtuddannede og kompetente specialister.
- Vi har ikke dokumentation for dokumentationens egen skyld – men der, hvor det skaber værdi for kunden.
- Vi arbejder med processer, hvor det skaber værdi for kunden – for vi ønsker at bevare vores agilitet.
- Vi er fagligt tunge med bred og massiv driftserfaring på tværs af systemer og løsninger.
- Vi er den lille virksomhed, der har vokset sig stor, og undervejs har vi opbygget erfaring og services i tæt samarbejde med vores kunder.
- Vi er handlingsorienterede og stærkt engagerede i løsningen af kundens behov – kunden kommer altid først.
- Vores fælles "kunde-ejerskab" betyder: fælles best practice, høj vidensdeling og disciplineret driftsdokumentation på tværs af organisationen.

Organisering
Itadel har i dag ca. 300 ansatte – heraf er ca. 200 personer teknisk personale. Vi råder desuden over 5 datacentre i Danmark, hvoraf de seneste er opbygget som 'Software Defined Data Center' (SDDC), der som standard tilbydes som 2-center løsning.

Itadel er organiseret efter de væsentlige områder, som enten understøtter eller direkte leverer professionelle serviceydelser, hvilket fremgår af efterfølgende organisationsdiagram.

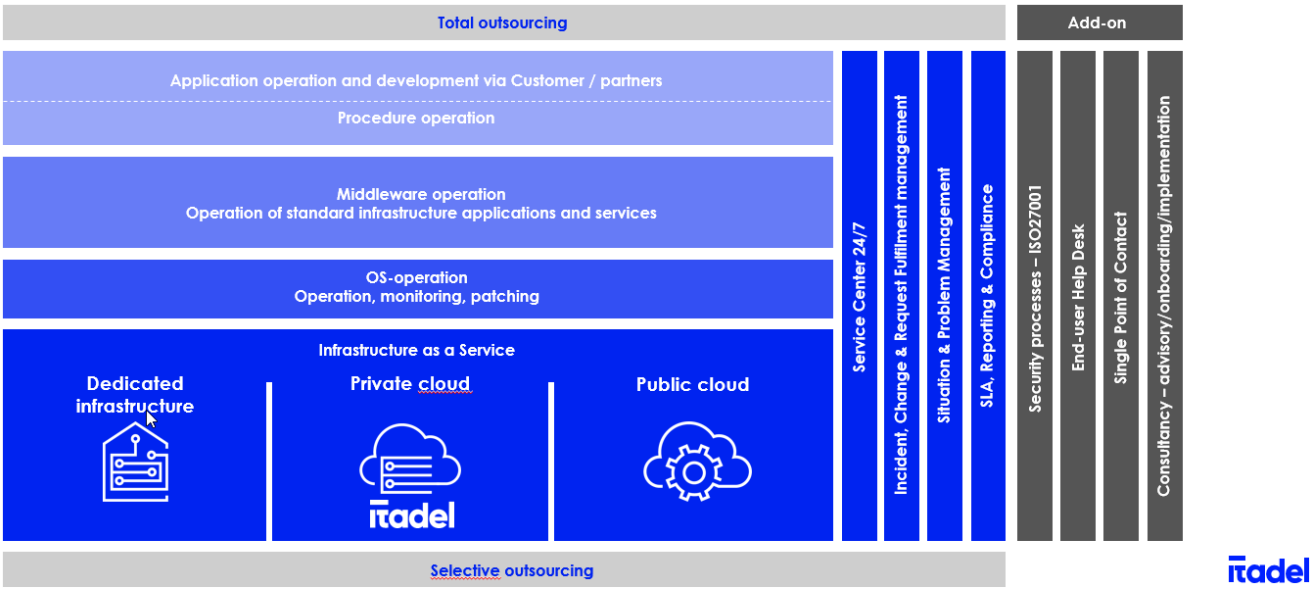


Kompetencer og bemanding
Vores teknikere arbejder i samme systemer på tværs af kunder.
Deres kompetencer, certificeringer og erfaring er kortlagt i et "knowledge map" – på den baggrund kan vi:

- sammensætte teams, der sikrer høj performance.
- sikre, at enhver ticket tildeles den rigtige tekniker eller det rigtige team første gang. Derfor løses alle tickets meget hurtigt og effektivt.
- sikre adgang til de rigtige kompetencer 24/7.

Vi arbejder derudover med løbende intern træning og uddannelse for at sikre, at erfaringer og viden om vores kunder og systemer formidles og videregives effektivt.

Driftskoncept og forretningskritiske services
Itadel leverer drift af it-systemer, outsourcet af såvel private som offentlige virksomheder. Kerneydelsen er løsninger baseret på Infrastructure as a Service, OS drift, middlewaredrift, proceduredrift samt applikationsdrift, som er beskrevet i nærmere detaljer i driftsaftalen.



Infrastructure as a Service

- Servere, storage, backup, netværk, load balancer, firewall
- Fuldt sikrede datacentre med adgangskontrol, brandsikring, tyverisikring, temperaturstyring (alarm), dieselgeneratorer til nødstrøm. Alarmer sendes til Service Desk og udvalgte tredjepartsleverandører (fx Brandvæsenet).
- Internetadgang direkte til TDC Backbone
- Enterprise-komponenter i et redundant setup
- Fuldt skalerbar Cloud-leverance inkluderer selvbetjeningsportal til oprettelse/nedlukning af servere, tildeling af storage, oprettelse af firewall og load balancer.

OS-drift

- Installation, drift, backup og patchning af det basale OS-system
- Antivirus – standard for Windows, kun specifikt for Linux, når kunde efterspørger
- Overvågning af servere og OS 24/7 samt adgang til Service/Operations/Help Desk
- Softwarelicenser til OS, backup og antivirus.

Middlewaredrift

- Fuldt driftsansvar af standardserverapplikationer (fx Citrix, Exchange, IIS, Apache, SQL, Oracle)
- Anvendelse af Itadel best practice på standardserverapplikationer
- Håndtering af backup, restore på middlewareapplikation samt tilhørende data
- Patchning (på sikkerhedspatchning følger vi producentens guidelines)
- Overvågning af applikation 24/7 samt adgang til Service Desk.

Proceduredrift

- Drift af kundespecifikke applikationer med udgangspunkt i definerede procedurer
- Procedurer defineres i tæt samarbejde imellem kunde, tredjepart og Itadel (procedurer spænder lige fra simple genstarter af services til release management på applikationsniveau)
- Overvågning af applikation 24/7 samt adgang til Service Desk
- Driftserfaringer indsamles og dokumenteres.

Applikationsdrift

- Vi kan desuden understøtte applikationsdrift via End-user Help Desk & SPOC.

Beskrivelse af generelle it-kontroller

Implementerede kontroller
Itadel har valgt at være ISO 27001-certificeret; de valgte kontrolområder sammen med en kort generel beskrivelse af implementerede 'ISO 27002 Controls' er anført nedenfor. Den komplette oversigt ses af Itadels 'Statement of Applicability'. Ansvaret for certificering og 'ISO 27002 Controls' er organisatorisk placeret ved afdelingen Information Security.

Risikostyring
I Itadel er risikostyring implementeret ud fra ISO 27001, hvor det er et krav, at der tages en risikobaseret tilgang til sikkerhed. Itadel har derfor indbygget risikostyring i sine processer, fx Change Management-processen.

Itadel laver løbende risikovurderinger baseret på udviklingen i det generelle trusselsbillede imod Itadel. Ligeledes laves der også risikovurderinger på interne og tekniske forhold, der kan have indvirkning på serviceleverancen. Afhængig af ændringer i det samlet risikobillede vil udvalgte risici rejses til Itadels øverste ledelse. Risikovurderinger af kundernes miljøer sker kun, i det omfang at Itadel er kontraktmæssigt forpligtet hertil, eller kunden direkte ønsker en risikovurdering.

Den følgende tabel viser, hvilke forebyggende og udbedrende tiltag Itadel har implementeret:

	Forebyggende tiltag	**Udbedrende tiltag**
Organisatoriske tiltag	• Politikker, procedurer og instruktioner • Awareness • Change management • Technical best practices • Operational acceptance test • Compliance-kontroller • Leverandørkontrakter • Service- og supportaftaler • CMDB/systemdokumentation	• Beredskabsplaner • Disaster recovery procedures • Procedure for major incidents • Incident management • Problem management
Fysiske og tekniske tiltag	• Firewalls • Antivirus • Alarmsystemer • Monitorering • Testmiljøer • Intrusion prevention • Redundans • Identity management • Clusters • UPS	• Logning • Standbyudstyr • Standbysite • Backup/restore • Server snapshots • Virtualisering • Brandslukning • Nødstrøm

Informationssikkerhedspolitikker
Itadel har udarbejdet sikkerhedspolitikker, som reflekterer Itadels strategi og mål for sikkerhed.

Ledelsen i Itadel har angivet målsætningen for informationssikkerhed igennem en informationssikkerhedspolitik, der løbende efterses af ledelsen – minimum årligt. Informationssikkerheden håndteres igennem Itadels Information Security Management System (ISMS). Her beskrives Itadels behandling af blandt andet håndtering af kodeord, auditering, retningslinjer for sikkerhedsniveau på: operativsystemer, servere og arbejdsstationer, netværk og storage. Itadels ISMS beskriver desuden krav til funktionsopdeling og brugerstyring af såvel Itadels driftskritiske systemer som delt infrastruktur samt kundeløsninger.

Organisering af informationssikkerhed
Ansvaret for anvendelsen af Informationssikkerhedspolitikken og Information Security Management System varetages af afdelingsledelsen. Dette støttes af en dedikeret sikkerhedsfunktion under ledelse af Itadels sikkerhedschef.

I Itadel er ansvar for informationssikkerhed implementeret ved klassificering af processer, systemer og data med tilhørende organisatorisk ejerskab. Der tages her hensyn til funktionsadskillelse (segregation of duties).

Der er udarbejdet procedurer for kontakt med myndigheder, hvilke er forankret i Finance- og Human Resource-afdelingerne. Kontakt med interessegrupper håndteres decentralt i de funktioner, hvor kontakten er relevant og værdiskabende.

Der er udarbejdet en politik for håndtering af informationssikkerhed i projekter. Denne har til formål at sikre, at projekter (internt og eksternt) ikke introducerer risici for Itadel og vores kunder.

Der er i Itadel særlig fokus på håndtering af mobile enheder samt teleworking, der specifikt er beskrevet i vores informationssikkerhedshåndbog, 'General rules for information security at Itadel'. Håndbogen udleveres til alle medarbejdere sammen med kontrakten.

Medarbejdersikkerhed
Itadel har definerede processer for ansættelse, rotation og fratrædelse af medarbejder. Alle medarbejdere screenes ved ansættelse. Alle medarbejdere informeres om gældende sikkerhedsprocesser, procedurer og instruktioner i forbindelse med opstart. Processerne er forankret og centralt styret fra HR-afdelingen.

Itadel har defineret og dokumenteret en disciplinær proces, der træder i kraft ved brud på sikkerheden.

Ved fratrædelse oplyses medarbejderen igen om sine forpligtigelser, herunder hvad der er gældende efter fratrædelsen. Udleveret udstyr skal leveres tilbage, og tildelte adgange og rettigheder lukkes ned efter fratrædelsen.

Styring af informationsrelaterede aktiver
Itadel har implementeret ejerskab for informationsrelaterede aktiver for delt infrastruktur og kundemiljøer. Ejerskabet af de enkelte aktiver registreres og spores i et centralt register. Den udpegede ejer af et aktiv er ansvarlig for aktivets fulde livscyklus; en af opgaverne er at klassificere aktivet ud fra CIA (Confidentiality, Integrity og Availability). Medarbejdere informeres om acceptabel anvendelse af udstyr; dette er nærmere beskrevet i informationssikkerhedshåndbogen. Aflevering af aktiver udleveret til medarbejdere sker jævnfør processen for fratrædelse af medarbejdere.

Udstyr, der indeholder data, bortskaffes ved destruktion jævnfør specificeret procedure, når det ikke længere anvendes. Udstyr er fra nedtagning til destruktion beskyttet imod misbrug.

Adgangsstyring
Itadel har etableret adgangsstyring på flere niveauer for at begrænse risikoen for uautoriseret adgang til systemer og data. Adgangsstyring er etableret både fysisk og logisk. Adgangsstyringen er understøttet af processer og kontroller i forbindelse med tildeling og vedligeholdelse af adgange til systemer og data.

Brugere oprettes, administreres og nedlægges i henhold til den gældende sikkerhedspolitik, hvor privilegier og adgange tildeles ud fra et arbejdsrelateret behov. Sikre log-on-procedurer er realiseret i passwordpolitikker, der er implementeret i henhold til anbefalinger fra etablerede systemleverandører.

Der foretages periodisk gennemgang af brugere, rettigheder og adgange. Eventuelle uoverensstemmelser undersøges og rettes uden yderligere ophold.

Kryptering
Der stilles krav til kryptering ud fra informationsklassificeringen af data.

I henhold til Itadels informationssikkerhedshåndbog skal følsomme data beskyttes med kryptering. Eksempler på dette er udstyr udleveret til medarbejdere og backup af kunders data.

Fysisk sikkerhed og miljøsikring
Itadel håndterer fysisk sikkerhed gennem en række implementerede sikkerhedstiltag, herunder 'clear desk and screen' policy, styring af adgangskontrol på lokationer og datacentre, hvor alle personer skal bære synligt identifikationskort, med henblik på at sikre at det kun er personer med autorisation, som befinder sig i virksomheden. Personer uden autorisation, som har ærinde på lokationen, har kun adgang via receptionen, der sørger for registrering og gæstekort samt fysisk afhentning ved den medarbejder, som gæsten har en aftale med.

Der er procedurer for på- og aflæsningsområder, vedligehold af udstyr samt genbrug og bortskaffelse af udstyr.

Itadels datacentre er fysisk sikret mod trusler som brand, vand og varme samt svigt i forsyningslinjer som elektricitet. Der er etableret strømforsyning med backup (batterier og generatorer), brandsikring, brandalarmer og slukningsudstyr samt overvågning af datacentrenes fysiske forhold. Datacentrenes fælles infrastrukturenheder er dimensioneret med redundante systemer, hvor hvert system har individuel backup. Netværksforbindelser fra datacentrene er ligeledes redundante.

Driftssikkerhed
Itadel har som en del af sit Information Security Management System (ISMS) dokumenteret en række procedurer og instruktioner, der understøtter en stabil og sikker drift. Disse er etableret igennem vores forretningsprocesser og kontroller, der er baseret på ITIL best practice framework. Af specifikke processer kan nævnes change management, incident management og capacity management. Sårbarheder forebygges blandt andet igennem patch management, anti-malware-systemer og døgnbemandet overvågning. I tilfælde af driftsforstyrrelser har Itadel backup.

Backup sker efter kundens krav. Den primære backupmetode er gennem fuld backup, ved start af asset sættes i drift, og derefter inkrementelle daglige backups af både kunde- og Itadel-systemer. Dette håndteres af vores certificerede backupservicepartner, B4Restore.

Backup testes regelmæssigt. Hvis en sårbarhed opdages, fx i forbindelse med en it-sikkerhedshændelse, registreres den, og passende foranstaltninger implementeres.

Kommunikationssikkerhed
Netværksadgang i Itadel er opdelt i en teknisk samt en ikke-teknisk adgang tildelt efter arbejdsrelateret behov. Adgang til infrastruktur og driftssystemer er isoleret på et tekniknet. For at sikre mod risiko for uautoriseret adgang på tekniknettet er multifaktorautentifikation påkrævet.

Itadels driftsinformation og kommunikation er centralt forankret i virksomhedens interne driftsportal. Portalen indeholder alle væsentlige retningslinjer, processer og værktøjer forbundet med driften af Itadels infrastruktur, interne systemer og kundeløsninger.

Itadel anvender Non-Disclosure Agreements, hvor dette er nødvendigt, for at beskytte følsomme og fortrolige data.

Anskaffelse, udvikling og vedligeholdelse af systemer
Itadel har sin egen politik i forhold til at sikre informationssikkerhed i egne projekter. Politikken sikrer sammen med den implementerede change management-proces, at de nødvendige risikovurderinger foretages. Dette gælder den fulde livscyklus for anvendte systemer og løsninger.

I driftsfasen er risikostyringen en eksplicit del af det implementerede change management-system. I systemet skal væsentlige ændringer på driftssystemer dokumenteres, vurderes, evt. justeres, godkendes, planlægges og gennemføres efter fast definerede rutiner og processer. Såfremt kunden har behov for at fravige aftalte sikkerhedsstandarder/best practices, aftales dette nærmere mellem Itadel og kunden. Aftalen dokumenteres i et Risk Letter.

Itadels interne systemer er placeret i en infrastruktur, der er adskilt fra kundesystemernes infrastruktur. Systemerne drives efter samme servicemodel som beskrevet i en standardleverancebeskrivelse. Modellen adresserer risici ved ændringsstyring, adgangskontrol, backup, understøttende infrastrukturredundans mv.

Leverandørforhold
Ydelser fra væsentlige serviceleverandører til Itadel er underlagt samme krav til informationssikkerhed som beskrevet under Informationssikkerhedspolitikker. Itadel har udpeget en leverandøransvarlig i egen organisation, der varetager den fulde livscyklus, såsom klassificering af leverandører, sikring af Non-Disclosure Agreements og auditeringer.

Styring af sikkerhedshændelser
Itadels sikkerhedsafdeling har ansvaret for rapporteringer og håndtering af såvel sikkerhedshændelser som sikkerhedssårbarheder. Sikkerhedshændelser dokumenteres og undersøges jævnfør formaliserede procedurer – og hvis de vurderes at udgøre en væsentlig risiko, så igangsættes relevante aktiviteter. Fremdrift forelægges jævnligt for Itadels øverste ledelse.

Itadel foretager systematisk risikovurdering af interne kritiske aktiver såsom centrale infrastrukturelementer, systemer og processer, der understøtter driften. Risikovurderingen foretages i forhold til parametrene tilgængelighed, fortrolighed og integritet.

Nød-, beredskabs- og reetableringsstyring
Itadel har taget nødvendige forholdsregler for at reetablere driftssystemer, såfremt en katastrofesituation måtte indtræffe. Forholdsreglerne består blandt andet af beredskabsplaner, der beskriver etablering af katastrofeorganisationen, herunder lokaler og adgangsforhold, retningslinjer for beredskabsledelsen, beredskabsbemanding, systemlister, reetablering/katastrofedrift, andre aktiviteter, kommunikation og kontaktlister.

Compliance
Itadel har implementeret procedurer for godkendelse, anskaffelse og benyttelse af software. Der er løbende samarbejder med softwareleverandører om licensstyring og opgørelse af deres produkter. Afhængig af licensform (eje/leje) sker en løbende rapportering til regnskabsafdelingen.

Der er implementeret en portal, der fungerer som Itadels fortegnelse over nøgleinformationer og systemer. Portalen fungerer som medarbejdernes generelle indgang til at løse opgaver i dagligdagen.

Data behandles i overensstemmelse med klassifikation og princippet for funktionsadskillelse; dette gælder også for personhenførbare data. Itadel har i informationssikkerhedshåndbogen beskrevet retningslinjer for, hvilket sikkerhedsniveau der skal anvendes på medarbejderudstyr.

Der gennemføres ca. kvartalsvist en gennemgang af informationssikkerhedssystemet (ISMS) – tre eller flere interne og én ekstern audit per år. Derudover udarbejdes et antal revisionserklæringer, en generel ISAE 3402, en generel ISAE 3000 (GDPR), samt et antal kundespecifikke erklæringer. Procedurer og politikker revideres efter behov.

Nærværende beskrivelse dækker og er udelukkende til brug for de virksomheder, der har indgået aftale om serviceleverancer på basis af standardleverancedokumentet, og disse virksomheders revisorer, og må ikke anvendes til andre formål.

Forbedringer
I 2019 har Itadel indført følgende tiltag for at forbedre sikkerhedsniveauet:

Måned	Tiltag
Februar - april 2019	Gennemført seks forskellige interne audits på en bred række af centrale services.
Juli 2019	Implementeret nyt patch management-system, Tanium, der fremadrettet kan tillade mange nye sikkerhedsintegrationer.

3. Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet

Til ledelsen i Itadel, Itadels kunder af hostingydelser og disses revisorer

Omfang
Vi har fået til opgave at afgive erklæring om Itadels beskrivelse, afsnit 2, af udformningen og funktionen af generelle it-kontroller, der vedrører regnskabsaflæggelsen i relation til Itadels hostingydelser (på fysiske lokationer i Danmark og Sverige), jf. den gældende SoA og sikkerhedspolitik for Itadel (samlet efterfølgende omtalt som driftsydelser), der knytter sig til de kontrolmål, som er anført i beskrivelsen for perioden fra 1. januar til 31. december 2019.

Itadels ansvar
Itadel er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, 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 og implementeringen af effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores 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.

Vores ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Itadels beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for 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, hvor der afgives 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 sit system 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 nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet.

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
Itadels beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og disses revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter dennes 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 transak-

tioner. 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. Det er vores opfattelse,

a) at beskrivelsen af Itadels hostingydelser, således som de var udformet og implementeret på fysiske lokationer i Danmark og Sverige i hele perioden fra 1. januar 2019 til 31. december 2019, i alle væsentlige henseender er retvisende

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 2019 til 31. december 2019

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 nået, i alle væsentlige henseender har fungeret effektivt i hele perioden fra 1. januar 2019 til 31. december 2019.

Vores konklusion dækker alene hostingydelser i henhold til den gældende SoA og sikkerhedspolitik for Itadel og omfatter ikke kundespecifikke krav og forhold. Såfremt kunderne ønsker en erklæring vedrørende dette, skal der indgås en aftale med Itadel herom.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests 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 Itadels hostingydelser, og disses revisorer, som har en tilstrækkelig forståelse til at overveje disse sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 22. januar 2020
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
statsautoriseret revisor

Iraj Bastar
senior manager

4. Specifikke kontrolmål, kontroller, test og resultat heraf

A.5 Kontrolmål: Informationssikkerhedspolitikker

Itadel-kontrol	PwC-test	Resultat af test
5.1.1 Politikker for informationssikkerhed *Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.* Sikkerhedspolitikken er dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken er godkendt af ledelsen. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere via intranettet.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har ved inspektion observeret, at der eksisterer en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har ved inspektion konstateret, at sikkerhedspolitikken gennemgås mindst én gang årligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
5.1.2 Gennemgang af politikker for informationssikkerhed *Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Informationssikkerhed og tiltag herunder varetages af afdelingsledelsen i driftsorganisationen og støttes af en dedikeret sikkerhedsfunktion, der er en stabsfunktion, som er tilknyttet teknikorganisationen.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har ved inspektion observeret at politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i forbindelse med væsentlige ændringer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.6 Kontrolmål: Organisering af informationssikkerhed

Itadel kontrol	PwC-test	Resultat af test
6.1.1 Roller og ansvarsområder for informationssikkerhed *Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Informationssikkerhed og tiltag herunder varetages af afdelingsledelsen i driftsorganisationen. Denne støttes af en dedikeret sikkerhedsfunktion, der er en stabsfunktion.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer. Vi har observeret, at informationssikkerhed og tiltag herunder varetages af afdelingsledelsen og støttes af en stabsfunktion.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6.1.2 Funktionsadskillelse *Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.* Itadels ledelse har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse. Dette sikrer, at udviklings- og driftsaktiviteter samt adgang til primære og sekundære data er adskilt, medmindre der eksisterer et arbejdsbetinget behov for andet.	Vi har overordnet drøftet proceduren/kontrolaktiviteterne, der udføres, med ledelsen. Vi har stikprøvevis ved inspektion kontrolleret, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos Itadel, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6.2.1 Politik for mobilt udstyr *Der skal vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.* Itadel har særlig fokus på håndtering af mobilt udstyr, der specifikt er beskrevet i vores informationssikkerhedshåndbog, 'General rules for information security at Itadel'. Håndbogen udleveres til alle medarbejdere sammen med kontrakten og er tilgængelig på intranettet for alle medarbejdere.	Vi har overordnet drøftet procedurer og retningslinjer, som sikrer sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr. Vi har påset, at der forefindes procedurer for anvendelse af mobilt udstyr.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.6 Kontrolmål: Organisering af informationssikkerhed

Itadel kontrol	PwC-test	Resultat af test
6.2.2 Fjernarbejdspladser *Der skal implementeres en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.* Itadel har etableret retningslinjer, som sikrer systemer og data uden for virksomhedens netværk. Der er ligeledes indarbejdet to-faktor-autentifikation for tilgang til VPN-forbindelsen, som sikrer, at kun medarbejdere med et arbejdsbetinget behov kan tilgå data fra fjernarbejdspladser.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har overordnet drøftet procedurer og retningslinjer for fjernarbejdspladser med ledelsen. Vi har ved inspektion observeret, at der foreligger retningslinjer for overholdelse af sikkerhedsreglerne i forbindelse med anvendelse af fjernarbejdspladser. Vi har vurderet, at adgangskontroller via en to-faktor-VPN-forbindelse overholder de sikkerhedsmæssige krav i persondataloven. Vi har observeret, at den sikkerhedserklæring, som underskrives af medarbejderne hos Itadel ved ansættelsen, indeholder de omtalte retningslinjer for brug af hjemmearbejdspladser, herunder forbud mod at downloade personfølsomme oplysninger på pc'er, som anvendes på hjemmearbejdspladser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.7 Kontrolmål: Personalesikkerhed

Itadel-kontrol	PwC-test	Resultat af test
7.1.2 Ansættelsesvilkår og -betingelser *Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.* Itadel har fastlagt regler for fortrolighedsaftaler, som medarbejdere underskriver ved ansættelse, og erklæringer, som eksterne konsulenter underskriver forud for deres arbejde.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Ved stikprøver har vi observeret, at fortrolighedsaftaler anvendes i henhold til retningslinjerne, herunder: • at medarbejdere underskriver fortrolighedsaftaler ved ansættelsen • at eksterne konsulenter underskriver fortrolighedsaftaler forud for det aftalte arbejde.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
7.2.1 Ledelsesansvar *Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.* Itadel har for både medarbejdere og leverandører fremsat krav gennem kontrakter, som sikrer, at organisationens fastlagte politikker og procedurer opretholdes.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der foreligger underskrevne kontrakter for både medarbejdere og leverandører, så organisationens krav til informationssikkerhed opretholdes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed *Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.* Itadel introducerer medarbejderne til informationssikkerheden i forbindelse med ansættelse via både menneskelig introduktion og krav til gennemlæsning af sikkerhedspolitikken og sikkerhedshåndbogen. Der laves også yderligere awareness-tiltag i løbet af forretningsåret. Itadel har i kontrakter med leverandører fastsatte krav vedrørende informationssikkerhed, som er i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at Itadel afholder introduktionskurser for nye medarbejdere, hvor informationssikkerheden gennemgås. Desuden har vi observeret, at medarbejdere periodisk skal gennemføre et undervisningsforløb for at opretholde organisationens sikkerhedskrav. Vi har for leverandører observeret, at der er udarbejdet kontrakter, som sikrer, at organisationens krav vedrørende informationssikkerheden opretholdes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.7 Kontrolmål: Personalesikkerhed

Itadel-kontrol	PwC-test	Resultat af test
7.3.1 Ansættelsesforholdets ophør eller ændring *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.* Itadel sikrer, at brugerrettigheder til operativsystemer, netværk, databaser mv. vedrørende fratrådte medarbejdere inaktiveres rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at medarbejderes rettigheder til operativsystemer, netværk, databaser, mv. nedlægges i forbindelse med fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.8 Kontrolmål: Styring af aktiver

Itadel-kontrol	PwC-test	Resultat af test
8.1.1 Fortegnelse over aktiver *Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.* Itadel har udarbejdet en fortegnelse over kritiske aktiver og implementeret procedurer, der sikrer løbende vedligeholdelse heraf.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er etableret de fornødne kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
8.3.2 Bortskaffelse af medier *Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.* Itadel har udarbejdet retningslinjer for bortskaffelse, salg, kassation, reparation og service af it-udstyr.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at Itadel har tilrettelagt formaliserede processer for behandling og destruktion af ind- og uddatamateriale. Vi har påset, at kontrollerne vedrørende valideringskontroller for inddatamateriale samt retningslinjerne for sikker destruktion af uddata udføres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.9 Kontrolmål: Adgangsstyring

Itadel-kontrol	PwC-test	Resultat af test
9.1.1 Politik for adgangsstyring *En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.* Itadel har etableret retningslinjer, som sikrer, at medarbejderne tildeles rettigheder ud fra et arbejdsbetinget behov, og som opfylder organisationen krav til informationssikkerhedskrav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er etableret retningslinjer for adgangskontroller, herunder både via fjernadgang, på lokationen og for leverandører.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
9.1.2 Adgang til netværk og netværkstjenester *Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.* Itadel gennemgår alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler for at sikre overensstemmelse med virksomhedens politikker og dermed sikre, at rettigheder er tildelt ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved stikprøvevis inspektion gennemgået udvalgte servere og klarlagt, hvorvidt medarbejderne oprettes på den enkeltes maskine og bliver oprettet ud fra et arbejdsbetinget behov. Vi har observeret, at der hos Itadel findes dokumentation for, hvilke medarbejdere, relateret til kunden, der har tilladelse til at ændre i disse rettigheder.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.2.1 Brugerregistrering og -afmelding *Der skal implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.* Itadel har beskyttet adgange til operativsystemer, netværk, databaser mv. med password, som overholder gældende sikkerhedskrav til længde, kompleksitet, levetid mv. Endvidere låses brugere ved gentagende fejlforsøg i forbindelse med login. Adgangskoder til kunders systemer oprettes, administreres og slettes fra et centralt identity management-system (ISIM). Dette system benytter politikker og roller til at tildele adgangskoder.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er procedurer for brugeradministrationen, og ved stikprøvevis inspektion observeret: • at der jf. retningslinjerne foretages periodisk opfølgning på brugernes rettigheder på driftsmiljøerne • at disse rettigheder er tildelt ud fra et arbejdsbetinget behov. Vi har ved stikprøvevis inspektion af de tekniske opsætninger observeret: • at der anvendes password i henhold til retningslinjerne • at programmerede kontroller sikrer, at passwords skiftes regelmæssigt • at kontroller i anvendelsen af ISIM sikrer passende sikkerhedsmæssig kvalitet af password.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.9 Kontrolmål: Adgangsstyring

Itadel-kontrol	PwC-test	Resultat af test
9.2.2 Tildeling af brugeradgang *Der skal implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.* Itadel har tilrettelagt processer, som sikrer, at tildelte brugeradgange er i overensstemmelse med et arbejdsbetinget behov. Alle tekniske autorisationer hos Itadel, der har berøring med kundemiljøer, godkendes løbende af medarbejdernes nærmeste chef og indeholder en begrundelse for den ønskede adgang. De implementerede autorisationsprocedurer hos Itadel sikrer, at oprettelse af brugere og tildeling af rettigheder sker efter godkendelse fra en bemyndiget person. Alle adgange hos Itadel er personlige og behandles fortroligt, ligesom der foretages verificering af en brugers identitet, inden denne autoriseres.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring. Vi har observeret, at der er tildelte autorisationer hos Itadel, hvor der foreligger en begrundelse for den ønskede adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
9.2.3 Styring af privilegerede adgangsrettigheder *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* Itadel har tilrettelagt formaliserede processer, som sikrer, at tildelte brugeradgange, inklusive brugere med privilegerede rettigheder, er i overensstemmelse med arbejdsrelaterede behov. Alle brugerkonti hos Itadel er personlige og behandles fortroligt, ligesom der foretages verificering af brugers identitet, inden denne autoriseres. Anvendelse af privilegerede rettigheder overvåges løbende. Afvigende forhold undersøges og løses rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring, som tillige omfatter brugere med privilegerede rettigheder. Vi har observeret, at der for tildelte autorisationer foreligger en begrundelse for den ønskede adgang og en godkendelse fra nærmeste chef.	Vi har ikke konstateret væsentlige afvigelser.

A.9 Kontrolmål: Adgangsstyring

Itadel-kontrol	PwC-test	Resultat af test
9.2.5 Gennemgang af brugeradgangsrettigheder *Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.* Itadel foretager løbende gennemgang af medarbejdernes privilegerede tekniske rettigheder i både interne og kundevendte systemer. Dermed sikres overensstemmelse med medarbejderens arbejdsbetingede behov. Denne gennemgang sker hver uge. Her gennemgås automatisk alle servere, der brugerstyres gennem ISIM, for inaktivitet i over 90. dage, hvorefter inaktive konti slettes fra de pågældende systemer. Ikketeknisk privilegerede medarbejdere får nødvendige rettigheder til brug af interne systemer. Disse standardrettigheder tilføjes og fjernes ved enten ansættelse, flytning eller fratrædelse hos Itadel.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at brugeradgange revurderes én gang hvert halve år.	Under vores revision har vi observeret at den automatisk oprydning af inaktive brugerkonti ikke har været afviklet på en række servere. Vi er blevet informeret at Itadel har etableret ugentlig kontrol af inaktive brugerkonti indtil den automatiske kontrol fungerer stabilt. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
9.2.6 Inddragelse eller justering af adgangsrettigheder *Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.* Itadel sikrer, at brugerrettigheder til operativsystemer, netværk, databaser mv. vedrørende fratrådte medarbejdere inaktiveres rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion kontrolleret, at der jf. retningslinjerne foretages periodisk opfølgning på brugernes rettigheder på driftsmiljøerne, og at disse rettigheder er tildelt ud fra et arbejdsbetinget behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
9.4.1 Begrænset adgang til informationer *Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring.* Itadel har udarbejdet retningslinjer for administration af og kontrol med autorisationer. Herunder har Itadel sikret, at der er implementeret kontrolforanstaltninger i systemerne, som sikrer, at kun autoriserede bruger kan få adgang til personoplysninger og anvendelser, som de er autoriseret til. Dette sker ved brug af medarbejderens tilknytning i AD'et samt ved brug af Itadels Identity Management System (ISIM). Itadel har implementeret retningslinjer, som sikrer korrekt oprettelse og nedlæggelse.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har udarbejdet retningslinjer for administration af, og kontrol med, autorisationer. Vi har observeret, at adgange til systemerne hos Itadel er givet ud fra et arbejdsbetinget behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.9 Kontrolmål: Adgangsstyring

Itadel-kontrol	PwC-test	Resultat af test
9.4.3 System for administration af adgangskoder *Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet.* Itadel har udarbejdet retningslinjer for foranstaltninger for logisk sikkerhed, herunder logning og kontrol af afviste loginforsøg. Disse kontroller omfatter: • Applikationskrav om brug af password • Kvalitetskrav til password • Krav til lockoutpolitikken • Log og opfølgning over afviste adgangsforsøg • Kontrol af afviste adgangsforsøg • Krav om passwordskifte ved første login. Itadel har implementeret kontroller i systemerne, som sikrer, at brugerne valideres, inden ny adgangskode tildeles.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har opsat retningslinjer for foranstaltninger til logisk sikkerhed, som overholder datatilsynets retningslinjer. Vi har observeret, at opsætningen omfatter: • Applikationskrav om brug af password • Kvalitetskrav til password • Krav til lockoutpolitikken • Log og opfølgning over afviste adgangsforsøg • Kontrol af afviste adgangsforsøg • Krav om passwordskifte.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
9.4.4 Brug af privilegerede systemprogrammer *Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.* Itadel har etableret begrænsning i adgangen til systemer og netværk via to-faktor-autentifikation, og rettighederne styres gennem roller i Windows Active Directory. Desuden kan systemer og data kun tilgås gennem organisationens interne netværk, hvortil VPN-adgang fra eksterne lokationer kan etableres.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at alle rettigheder, herunder også adgange fra andre netværk, styres via roller i Windows Active Directory. Vi har observeret, at enhver adgang til data og systemer er betinget af, at brugeren er placeret på det interne netværk, og at ekstern adgang derfor kræver brug af VPN.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

Itadel-kontrol	PwC-test	Resultat af test
11.1.1 Fysisk perimetersikring *Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.* Itadel har udarbejdet retningslinjer for sikring af den fysiske sikkerhed. Herunder etableret en sikkerhedsorganisation, som er ansvarlig for Itadels samlede fysiske sikring. Disse kontroller omfatter en række adgangskontroller i bygninger, hvor der behandles personoplysninger (adgangskort og adgangskode). Ved indgåelse af aftaler med eksterne parter sikres det, at den eksterne part modtager den fornødne information om de it-sikkerhedsmæssige krav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at Itadel har udarbejdet retningslinjer for den fysiske sikkerhed, herunder etableret en it-sikkerhedsorganisation. Vi har påset, at Itadel har udarbejdet retningslinjer for sikring af den fysiske sikkerhed, og vi har påset, at de fysiske adgangskontroller fungerer som beskrevet. Vi har desuden påset, at der er indhentet en revisionserklæring fra Itadels underleverandør, som sikrer, at tilsvarende krav overholdes, på områder hvor der er foretaget outsourcing.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
11.1.2 Fysisk adgangskontrol *Sikre områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.* Itadel har udarbejdet retningslinjer for sikring af den fysiske sikkerhed, herunder etableret en sikkerhedsorganisation, som er ansvarlig for Itadels samlede fysiske sikring. Disse kontroller omfatter en række adgangskontroller i bygninger, hvor der behandles personoplysninger (adgangskort og adgangskode). Ved indgåelse af aftaler med eksterne parter sikres det, at den eksterne part modtager den fornødne information om de it-sikkerhedsmæssige krav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har udarbejdet retningslinjer for den fysiske sikkerhed, herunder etableret en it-sikkerhedsorganisation. Vi har observeret, at Itadel har udarbejdet retningslinjer for sikring af den fysiske sikkerhed, og vi har påset, at de fysiske adgangskontroller virker som beskrevet. Vi har observeret, at der er indhentet en revisionserklæring fra Itadels underleverandør, som sikrer, at tilsvarende krav overholdes, på områder hvor der er foretaget outsourcing.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

Itadel-kontrol	PwC-test	Resultat af test
11.1.3 Sikring af kontorer, lokaler og faciliteter *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og etableres.* Itadel har udarbejdet retningslinjer for sikring af fysisk sikkerhed. Disse retningslinjer omfatter en række adgangskontroller i bygninger, hvor der behandles personoplysninger (adgangskort og kode). Adgang til alle Itadel-områder, både kontorer og datacentre, sker ved periodegodkendte ID-kort. Disse er sat til tre år fra ansættelsestidspunkt. Gennemgang af disse rettigheder sker kontrolleret i forbindelse med ændringer i medarbejderes tiltræden, ny intern stilling eller ved fratrædelse. Ændring af disse fysiske adgangsrettidigheder udføres af HR. Adgang til hhv. datacentre og kontorer er funktionsmæssigt bestemt. Infrastrukturteknikere har adgang til begge dele, mens det ikke er tilfældet for resten af Itadel. Alle bortset fra infrastrukturteknikere skal søge adgang via Infrastructure & Storage ved besøg i datacentre. Ved indgåelse af aftaler med eksterne parter sikres det, at den eksterne part modtager den fornødne information om de it-sikkerhedsmæssige krav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at Itadel har udarbejdet retningslinjer for sikring af adskillelse mellem det offentlige rum og de interne kontorlokaler. Vi har observeret, at de fysiske adgangskontroller fungerer som beskrevet. Vi har desuden påset, at der er indhentet revisionserklæring fra underleverandøren, som sikrer, at tilsvarende krav overholdes, på områder hvor der er foretaget outsourcing.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
11.1.5 Arbejde i sikre områder *Procedurer for arbejde i sikre områder skal tilrettelægges og etableres.* Personer uden autorisation, som har ærinde på Itadels lokationer, tildeles adgang via receptionen eller ude i datacentrene, som sørger for registrering og gæstekort og fysisk afhentning via den medarbejder, som gæsten har en aftale med. I datacentrene tildeles gæstekort ikke nødvendigvis, da Itadels medarbejdere følger gæsten rundt under hele besøget.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at alle gæster med ærinde hos Itadel tildeles et gæstekort og under hele besøget bliver fulgt rundt af en ansat hos Itadel.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

Itadel-kontrol	PwC-test	Resultat af test
11.2.1 Placering og beskyttelse af udstyr *Udstyr skal placeres og beskyttes, således at risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.* *Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker skal tilrettelægges og etableres.* Itadels aktive datacentre er sikret mod forhold som brand, vand og varme. Itadel har placeret sine datacentre i bygninger beskyttet mod naturkatastrofer samt ondsindede angreb eller ulykker. Der er etableret brandsikring, brandalarmer og slukningsudstyr samt døgnbemandet overvågning af datacenterinfrastruktur.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har etableret retningslinjer for sikring mod brand, vand og varme. Vi har desuden observeret, at der er indhentet revisionserklæring fra underleverandøren, som sikrer, at tilsvarende krav overholdes, på områder hvor der er foretaget outsourcing.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
11.2.2 Understøttende forsyninger (forsyningssikkerhed) *Udstyr skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger. Udstyret vedligeholdes løbende.* Alle Itadels aktive datacentres fælles infrastrukturenheder er dimensioneret med fuldt redundante systemer, hvor hvert system har individuel backup. Itadel har etableret serviceaftaler samt vagtordninger på beskyttelsesudstyret i datacenteret, som tilses mindst en gang årligt. Netværksforbindelser fra Itadels aktive datacentre er ligeledes fuldt redundante.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har etableret en fuld redundant infrastruktur med individuel backup.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
11.2.5 Fjernelse af aktiver *Udstyr, information og software må ikke fjernes fra organisationen uden forudgående tilladelse.* Itadel har etableret retningslinjer, som sikrer, at udstyr, informationer og software ikke fjernes fra organisationen uden forudgående tilladelse.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der er etableret retningslinjer, som sikrer, at udstyr, information og software ikke fjernes fra Itadel uden forudgående tilladelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

Itadel-kontrol	PwC-test	Resultat af test
11.2.7 Sikker bortskaffelse eller genbrug af udstyr *Alt udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.* Itadel har etableret retningslinjer for bortskaffelse eller genbrug af udstyr, der sikrer, at oplysninger ikke kommer til uvedkommendes kendskab.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har etableret retningslinjer, som sikrer bortskaffelse eller genbrug af udstyr. Vi har observeret, at Itadel har implementeret relevante kontroller i forhold til B4Restores håndtering af backup. Vi har desuden modtaget revisionserklæringen fra B4Restore og gennemgået Itadels krav til B4Restore som underleverandør.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.12 Kontrolmål: Driftssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
12.1.1 Dokumenterede driftsprocedurer *Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem.* Generelle og kundespecifikke driftsprocedurer er dokumenteret i Itadels interne driftsportal, herunder intranet, fællesdrev samt configuration management database (CMDB).	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der eksisterer driftsprocedurer, som mindst én gang årligt ajourføres. Vi har desuden observeret, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.1.2 Ændringsstyring *Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres.* Itadel har formaliserede interne retningslinjer, forretningsgange og beskrivelser. Disse omfatter: • Incident management • Problem management • Change management • Release og patch management • Brugeradministration.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at Itadel har udarbejdet procedurer for årlig gennemgang og ajourføring af: • Incident management • Problem management • Change management • Release og patch management • Brugeradministration.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.1.3 Kapacitetsstyring *Anvendelsen af ressourcer skal overvåges og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.* Itadel har udarbejdet procedurer for driftsrapportering på månedsbasis. Disse driftsrapporter indeholder oplysninger om driften på produktionsmiljøerne, herunder også oplysninger vedr. kapacitet. Der er etableret automatisk overvågning af driftsmiljøet og relevante systemparametre, herunder kapaciteten, som sikrer, at fremtidige kapacitetskrav kan overholdes.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der månedsvis sendes driftsrapporter til kunden vedrørende driften på produktionsmiljøerne hos Itadel. Vi har ligeledes observeret, at kapaciteten overvåges på produktionssystemerne hos Itadel, så fremtidige krav til kapaciteten overholdes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.1.4 Adskillelse af udviklings-, test- og driftsmiljøer *Udviklings-, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.* Itadel har etableret separate it-miljøer for udvikling, test og produktion. Kun personale med funktionsadskilte rettigheder kan migrere ændringer mellem miljøerne.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og observeret, at der, jf. retningslinjerne, er etableret separate miljøer til udvikling, test og drift samt passende funktionsadskillelse i forbindelse med idriftsættelse af ny funktionalitet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.12 Kontrolmål: Driftssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
12.2.1 Kontroller mod malware *Der skal implementeres kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.* Itadel har etableret en procedure, som sikrer systemer og data mod skadelige data og programmer. Som minimum er der på alle Windows-maskiner og klienter hos Itadel installeret anti-virus eller anti-spyware-systemer, som løbende skal være holdt ajour. På Linux er der kun installeret antimalware, hvis kunden efterspørger det.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved stikprøvevis inspektion observeret, at medarbejdernes pc'er og servere hos Itadel er beskyttet med antivirussoftware – og at disse er ajourført.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.3.1 Backup af information *Der skal tages backupkopier af information, software og systembilleder, og disse skal testes regelmæssigt i overens-stemmelse med den aftalte backuppolitik.* Itadel foretager sikkerhedskopiering af data med fast definerede intervaller ved brug af sin certificerede leverandør B4Restore. Sikkerhedskopierede data testes periodisk gennem restore, med henblik på at skabe vished for at data kan genskabes fra sikkerhedskopier. Der er etableret en proces for kontrol af, at backup og restore fungerer umiddelbart inden idriftsættelse af projektsalgsløsninger. Backup monitoreres, og der sættes rettidigt ind ved konstaterede fejl, som påvirker driftsydelsen.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at de implementerede kontroller fungerer i henhold til retningslinjerne: • at sikkerhedskopier testes periodisk • at overvågning er implementeret for at sikre, at vedvarende og korrekt backup udføres. En tredjepart varetager driften og backup-løsningen. Vi har observeret, at procedurer og kontroller i øvrigt fungerer i henhold til Itadels sikkerhedsstandarder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.4.2 Beskyttelse af logoplysninger *Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.* Itadel har etableret logningsfacilitet, og disse er beskyttet mod uautoriseret adgang.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov. Vi har observeret, at logoplysningerne ikke kan manipuleres eller destrueres. Desuden foretager Itadel backup af logoplysningerne flere gange dagligt, hvor adgangen er begrænset til få personer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.12 Kontrolmål: Driftssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
12.4.4 Tidssynkronisering *Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne skal være synkroniseret til en enkelt referencetidskilde.* Itadel har synkroniseret alle relevante informationsbehandlingssystemer ud fra en enkel referencetidskilde.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Itadel har etableret en referencetidskilde for tidssynkronisering af alle relevante informationsbehandlingssystemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.5.1 Softwareinstallation på driftssystemer *Der skal implementeres procedurer til styring af softwareinstallationen på driftssystemer.* Itadel sikrer, at ændringer på operativsystemer, databaser, middleware og netværk testes/evalueres af kvalificeret personale inden ændring på driftssystemer. Test af ændringer i operativsystemer, databaser, middleware og netværk godkendes inden ændring i driftssystemer. Ændringer på driftssystemer foretages af kvalificerede driftsteknikere. Nødændringer i operativsystemer, databaser, middleware og netværk, som af driftsmæssige hensyn implementeres uden om den normale forretningsgang, testes/evalueres og godkendes efterfølgende.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved stikprøvevis inspektion af systemet, der anvendes til dokumentation af ændringer, kontrolleret, at der, jf. retningslinjerne, foretages ændringer til driftsmiljøet i en kontrolleret proces, herunder: • at der foretages godkendt test af ændringer inden idriftsættelse • at test og godkendelse i relation til nødændringer til driftsmiljøet dokumenteres umiddelbart efter idriftsættelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.6.1 Styring af tekniske sårbarheder *Der skal løbende indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.* Tekniske sårbarheder håndteres løbende af Itadel. Dette sker ved hjælp af: • Et centralt styret patch management-system, der er installeret på hovedparten af infrastrukturen, og som patcher Itadel- og kundeinfrastruktur efter definerede patch levels og aftalte patchvinduer. • Sårbarhedsscanninger på infrastruktur. • Monitorering af trusler igennem åbne og lukkede efterretningskilder. • Der udføres efter aftale penetrationstests til sikring af kundenetværk.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at driftssystemerne monitoreres, og at disse er konfigureret til at identificere fejl i driftssystemerne, baseret på prædefinerede kriterier. Vi har desuden observeret, at registrerede fejl undersøges og løses rettidigt. Vedrørende sikkerhedsopdateringer på platforme og databaser har vi observeret, at der er indgået kontraktmæssige aftaler om planlagte servicevinduer.	Under vores revision har vi observeret at der ikke udarbejdet Risk Letters vedrørende tildelte privilegerede kundeadgang på en række UNIX server. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

A.12 Kontrolmål: Driftssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
12.6.2 Begrænsninger på softwareinstallation *Der skal fastlægges og implementeres regler om softwareinstallation, som foretages af brugerne.* Itadel har etableret retningslinjer for softwareinstallation foretaget af brugerne.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der er udarbejdet retningslinjer for brugeres rettigheder til download af software. Vi har stikprøvevis observeret, at der i operativsystemet er indbygget begrænsninger, så kun tilladte applikationer kan installeres/downloades.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.13 Kontrolmål: Kommunikationssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
13.1.1 Netværksstyring *Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer.* Itadel styrer netværkssikkerhed gennem flere kontroltiltag. Itadel har tilrettelagt datakommunikationen på en hensigtsmæssig måde for at sikre mod risiko for tab af integritet, tilgængelighed samt fortrolighed. Der er desuden foretaget opdeling af netværket i et teknisk og administrativt netværk samt i private netværk efter aftale med kunderne. Kunder tildeles egne VLAN, hvorunder kundens løsning desuden opdeles i en sikkerhedsarkitektur bestående af bl.a. sikre zoner. Der er etableret retningslinjer for at sikre åbninger og forbindelser mellem kundemiljøer og internet. Eksempelvis sikres det, at ikke-krypterede forbindelser ikke tillades til fx interne net fra internettet. Al redigering af netværksinfrastruktur og kundemiljøer udføres udelukkende af autoriseret personale verificeret af to-faktor-autentifikation og AD-grupper. Ændringsopgaver, som ikke er standardændringer, er underlagt change management-processen. Der udføres efter aftale penetrationstests til sikring af kundenetværk.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved stikprøvevis inspektion kontrolleret, at der, jf. retningslinjerne, er etableret en passende sikkerhedsarkitektur i netværket, herunder: • at netværket er opdelt i sikre zoner, og at kundemiljøer er adskilt fra Itadels eget miljø • at fjernadgang er tildelt ved brug af to-faktor-autentifikation • at de i vores stikprøve udvalgte ændringer foretaget til netværksmiljøet sker på kontrolleret vis i henhold til change management-reglerne.	Under vores revision har vi observeret at en central netværksenhed ikke er opgraderet til ny version da enhedens operativt system har haft "end of support" i maj 2018. Vi er blevet informeret at Itadel vil koordinere servicevindue i Q1 2020. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
13.1.3 Opdeling af netværk *Grupper af informationstjenester, brugere og informationssystemer skal opdeles i netværk.* Itadel styrer netværkssikkerhed gennem flere kontroltiltag. Kunder tildeles egne VLAN, hvorunder kundens løsning desuden opdeles i en sikkerhedsarkitektur bestående af bl.a. sikre zoner. Al redigering af netværksinfrastruktur og kundemiljøer udføres udelukkende af autoriseret personale, verificeret af to-faktor-autentifikation og AD-grupper.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har gennemgået den tekniske sikkerhedsarkitektur og ved stikprøvevis inspektion kontrolleret, at der, jf. retningslinjerne, er etableret et passende sikkerhedsniveau, herunder: • at sikre zoner og kundemiljøer er adskilt fra Itadels eget miljø • at adgang til netværket er opdelt i relevante grupper baseret på arbejdsrelaterede behov • at fjernadgang er tildelt ved brug af to-faktor-autentifikation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.13 Kontrolmål: Kommunikationssikkerhed

Itadel-kontrol	PwC-test	Resultat af test
13.2.3 Elektroniske meddelelser *Informationer i elektroniske meddelelser skal beskyttes på passende måde.* Itadel har tilrettelagt formaliserede processer for behandling og destruktion af ind- og uddatamateriale. Disse kontroller omfatter: • Valideringskontroller for inddatamateriale • Retningslinjer for sikker destruktion af uddata • Håndtering af transmission af data • Itadel har retningslinjer, der foreskriver, at når der sendes fortrolig information, skal denne krypteres eller på anden vis overføres sikkert.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at Itadel har tilrettelagt formaliserede processer for behandling og destruktion af ind- og uddatamateriale. Vi har påset, at der er etableret kontroller vedrørende valideringskontroller for inddatamateriale samt retningslinjer for sikker destruktion af uddata.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.14 Kontrolmål: Anskaffelse, udvikling og vedligeholdelse af systemer

Itadel-kontrol	PwC-test	Resultat af test
14.1.1 Analyse og specifikation af informationssikkerhedskrav *Informationssikkerhedsrelaterede krav skal være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.* Itadel har udarbejdet procedurer, der sikrer håndtering af informationssikkerhed i projekter. Formål er at sikre, at projekter (internt og eksternt) og informationssystemer opfylder de relevante sikkerhedskrav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der er etableret en sikkerhedsorganisation hos Itadel, der sikrer et passende og tilstrækkeligt informationssikkerhedsniveau på systemerne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.15 Kontrolmål: Leverandørforhold

Itadel-kontrol	PwC-test	Resultat af test
15.1.1 Informationssikkerheds-politik for leverandør-forhold *Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til organisationens aktiver skal aftales med leverandøren og skal dokumenteres.* Ved indgåelse af aftaler med eksterne parter sikrer Itadel den fornødne information om it-sikkerhedsmæssige krav, indgåelser af tavshedserklæringer o. lign.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at kontrakterne med underleverandørerne indeholder it-sikkerhedsmæssige krav.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
15.1.2 Håndtering af sikkerhed i leverandøraftaler *Alle relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere it-infrastrukturkomponenter til organisationens information.* *Aftaler med leverandører skal indeholde krav til håndtering af informationssikkerhedsrisici forbundet med forsynings-kæden for IKT-tjenester og -produkter.* Ved indgåelse af aftaler med eksterne parter sikrer Itadel fastlæggelse af relevante sikkerhedskrav i forhold den enkelte leverandør. Der er udarbejdet procedurer, der sikrer, at aftaler, der indgås med leverandører, indeholder håndtering af relevante risici forbundet med forsyningskæden ved at udføre risikostyring af leverancen og tilgængelighed af tjenester.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at kontrakterne med underleverandørerne indeholder it-sikkerhedsmæssige krav. Vi har påset, at Itadel modtager uafhængig revisorerklæring fra underleverandøren B4Restore.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
15.2.1 Overvågning og gennemgang af leverandørydel-ser *Organisationer skal regelmæssigt overvåge, gennemgå og auditere leverandørydelser.* Itadel overvåger, gennemgår, auditerer og genforhandler leverandørydelser. Overvågningen og gennemgangen sker i forbindelse med leverandørens leverance. Auditeringen af leverandører bliver besluttet ud fra en forretningsmæssig vurdering ift. Itadels serviceleverancer til kunderne.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der månedligt udarbejdes en driftsrapport over systemerne hos Itadel. Vi har desuden observeret, at disse driftsrapporter har tydelige referencer til gældende SLA.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.16 Kontrolmål: Styring af informationssikkerhedsbrud

Itadel-kontrol	PwC-test	Resultat af test
16.1.1 Ansvar og procedurer *Ledelsesansvar og procedurer skal fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret hos Itadel. Informationssikkerhed og tiltag herunder varetages af afdelingsledelsen i driftsorganisationen og støttes af en dedikeret sikkerhedsfunktion, der er en stabsfunktion, som er tilknyttet teknikorganisationen.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har kontrolleret, at der eksisterer en hensigtsmæssig sikkerhedsorganisation, der understøtter Itadels forretningsområder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
16.1.2 Rapportering og håndtering af informationssikkerhedshændelser og sikkerhedsbrud *Informationssikkerhedshændelser skal rapporteres ad passende ledelseskanaler så hurtigt som muligt.* *Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.* Itadel har implementeret regler og procedurer, som sikrer, at der sker rapportering om informationssikkerhedsrelaterede hændelser. De retningslinjer sikrer, at mistanke om svagheder i informationssystemer og -tjenester registreres og efter aftale rapporteres til kunderne.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at der er implementeret procedurer for rettidig rapportering af sikkerhedsrelaterede hændelser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.17 Kontrolmål: Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Itadel-kontrol	PwC-test	Resultat af test
17.1.1 Planlægning af informationssikkerhedskontinuitet *Organisationen skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.* Itadel har taget de nødvendige forholdsregler og etableret beredskabsplaner for at reetablere driftssystemer, hvis en katastrofesituation måtte indtræffe. Beredskabsplanen beskriver etablering af katastrofeorganisationen, herunder lokaler og adgangsforhold, retningslinjer for beredskabsledelsen, beredskabsbemanding, systemlister, reetablering/katastrofedrift, instrukskort for aktiviteter og kommunikation, kontaktlister mv.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at der, jf. retningslinjerne, er udarbejdet en passende beredskabsplan for driftsafviklingen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
17.1.2 Implementering af informationssikkerhedskontinuitet *Organisationen skal fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.* Itadel har taget de nødvendige forholdsregler og etableret beredskabsplaner for at reetablere driftssystemer, hvis en katastrofesituation måtte indtræffe. Beredskabsplanen beskriver etablering af katastrofeorganisationen, herunder lokaler og adgangsforhold, retningslinjer for beredskabsledelsen, beredskabsbemanding, systemlister, reetablering/katastrofedrift, instrukskort for aktiviteter og kommunikation, kontaktlister mv.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at der, jf. retningslinjerne, er udarbejdet en passende beredskabsplan for driftsafviklingen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten *Organisationen skal verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.* Itadel har etableret procedurer, der sikrer, at der årligt sker en gennemgang af beredskabsplanen såvel som test via high impact-driftsforstyrrelser, såsom nedbrud på central datacenterinfrastruktur.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at der, jf. retningslinjerne, foretages periodisk test af beredskabsplanen, at eventuelle uhensigtsmæssigheder dokumenteres, og at udbedring indarbejdes i beredskabsplanen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

A.18 Kontrolmål: Overensstemmelse

Itadel-kontrol	PwC-test	Resultat af test
18.1.1 Identifikation af gældende lovgivning og kontraktkrav *Alle relevante lov-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen.* Itadel har udarbejdet procedurer, der sikrer, at gældende lovgivning og kontraktkrav overholdes.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at Itadel indgår aftaler ift. de specifikke kontrolaktiviteter, der udføres hos Itadel i relation til driftskontrakten.	Vi har ikke ved vores test konstateret væsentlige afvigelser.