

---

## ***EG A/S***

ISAE 3402-erklæring, type 2, fra uafhængig revisor vedrørende generelle it-kontroller, der vedrører regnskabsaflæggelsen i relation til EG A/S' it-drift og hosting-aktiviteter

---

*Januar 2019*

---

# Indhold

---

1. Ledelsens udtalelse .....	3
2. EG's beskrivelse af generelle it-kontroller, der vedrører regnskabsafleggelsen for driftsydelser i Danmark	4
3. Uafhængig revisors erklæring om beskrivelse af kontroller, deres udformning og funktionalitet .....	11
4. Kontrolmål, kontrolaktivitet, test og resultat heraf .....	13

## 1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt EG'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. EG bekræfter, at:

- (a) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af EG's driftsydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2018 til 31. december 2018. 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 2018 til 31. december 2018
  - (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 deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for vigtigt efter dennes 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 2018 til 31. december 2018. Kriterierne for 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 anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål
  - (iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2018 til 31. december 2018.

Ballerup, den 18. januar 2019



Mikkel Bardram  
Adm. direktør, Koncernen

## **2. EG's beskrivelse af generelle it-kontroller, der vedrører regnskabsaflæggelsen for driftsydelser i Danmark**

### **Indledning**

Denne systembeskrivelse vedrører de generelle it-kontroller i tilknytning til standard-it-drift og hosting-aktiviteter i EG A/S, som er ejet af Axcel. Standard-it-drift og hosting-aktiviteter leveres af EG Managed Services, som i denne erklæring er benævnt som EG, som det også fremgår af organisationsdiagrammet.

EG anvender Global Connect A/S som underleverandør af fysisk sikkerhed i datacentre, hvor EG's kunder driftes fra. Global Connect er herunder ansvarlig for den fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage. Bemærk, at flytningen af EG A/S' datacenterydelser til underleverandøren Global Connect A/S er sket pr. 1. november 2018. Før denne dato lå ansvaret alene hos EG A/S. Global Connect udarbejder ikke en revisionserklæring for perioden 1. januar – 31. december 2018, hvorfor relevante kontroller er selvstændigt testet af PwC for ovenstående periode.

Denne erklæring er udarbejdet efter "inclusive"-metoden og inkluderer således kontroller hos underleverandøren Global Connect A/S. Disse kontroller dækkes for 2019 ved modtagelse af revisionserklæring fra Global Connect A/S.

EG varetager drift og monitorering i forbindelse med it-drift og hosting-aktiviteter og er i forbindelse hermed ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af kontrakter og god skik.

Denne beskrivelse er afgrænset til generelle standarder for administration som beskrevet i EG's standardkontrakt. Specifikke forhold, der er relateret til individuelle kundekontrakter, er ikke omfattet.

Med baggrund i den ovenstående afgrænsning og nedenfor nærmere angivne systembeskrivelse vurderer EG, at vi i alle væsentlige forhold har opretholdt effektive kontroller. EG er opmærksom på, at der kontinuerligt sker udvikling inden for området, og EG arbejder kontinuerligt på at forbedre kontrollerne.

### **Beskrivelse af ydelser, der er omfattet af erklæringen**

De ydelser, som EG leverer, er tilpasset flere forskellige typer af kunder. Betingelserne for de enkelte kunder er angivet i kontrakter, hvor der for hvert forretningsområde tages udgangspunkt i standardkontrakter, som kan indeholde individuelle tilretninger og optioner. Til specifikke kunder er disse betingelser angivet i driftshåndbøger, som er udleveret til kunden og fungerer som systemdokumentation. Følgende områder dækker over de ydelser, som EG tilbyder:

**Housing:** Omfatter kunder, som udelukkende får stillet den fysiske EG-infrastruktur til rådighed, og som selv kontrollerer systemsoftware og applikationssoftware. EG har ansvar for den fysiske sikkerhed.

**Hostede kunder:** Omfatter kunder, hvis systemer er hostet på dedikerede fysiske eller virtuelle servere. EG har ansvar for den fysiske sikkerhed samt for backup. EG har ansvar for vedligeholdelse af systemsoftware, mens tredjepart har ansvaret for applikationssoftware.

**IaaS-kunder:** Omfatter kunder, som er hostet på delte miljøer. EG har ansvar for den fysiske sikkerhed samt for backup. EG har ligeledes ansvar for vedligeholdelse af systemsoftware, mens tredjepart har ansvaret for applikationssoftware.

**IBM iSeries:** Omfatter kunder, som er hostet på delte Power-maskiner. Der er tale om EG-kunder, som benytter branchesystemer. Disse branchesystemer er udviklet i EG. EG har ansvar for den fysiske sikkerhed samt for backup.

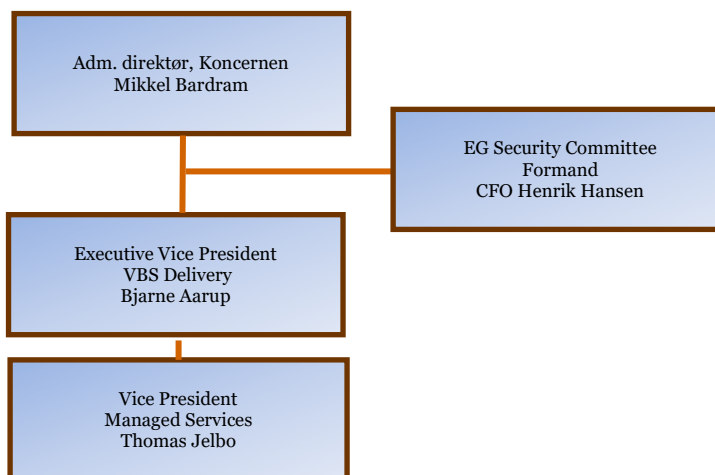
### **Kontrolmiljø**

#### **Ledelsesstruktur**

Organisationsform og ledelse bygger på en funktionsopdelt struktur, hvor lederen for den enkelte afdeling

har personaleansvar. Sikkerhedsansvaret i de enkelte processer er tildelt henholdsvis ansvarlige og udførende. Den ansvarlige har ansvar for driften og dokumentationen af de enkelte processer hos de ansatte.

## Organisationsdiagram – EG



### **It-informationssikkerhedspolitikker og organisering af informationsikkerhed**

For at sikre sammenhæng mellem arbejdet med it-sikkerhed og organisationen er der oprettet et it-sikkerhedsudvalg. It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, mellemledere samt driftsmedarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen i EG.

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen.

Udvalget behandler alle it-sikkerhedsspørgsmål af principiel karakter.

EG har udarbejdet en sikkerhedspolitik med afsæt i ISO 27001-standarden, og udvalget foretager en årlig vurdering af denne it-sikkerhedspolitik samt de tilknyttede retningslinjer – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidig, om der er behov for fornyet risikovurdering. Sikkerhedshændelser rapporteres til medlemmer af it-sikkerhedsrådet, hvor disse behandles.

Det overordnede ansvar for it-sikkerheden i EG ligger hos direktøren. Direktøren for VBS Delivery og Direktøren for Group IT er ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer, den daglige ledelse, og er ligeledes medlem af it-sikkerhedsudvalget. Chefen for EG Managed Services og chefen for EG Datacenter er ansvarlig for håndteringen af hændelser. Det er medarbejdernes daglige leder, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken, ud til den enkelte ansatte.

Når it-sikkerhedspolitikken, it-sikkerhedshåndbogen og beredskabsplanerne opdateres, kommunikerer dette til medarbejdere, hvorigennem medarbejderne derefter kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til it-sikkerhedskoordinatoren, der sørger for relevante rettelser.

Governance-delen af it-sikkerheden håndteres igennem en organisatorisk opbygning med den øverste ledelse som ansvarlig. Arbejdet varetages igennem it-sikkerhedsrådet, som har deltagelse fra den øverste ledelse og af strategisk udvalgte medarbejdere. Medlemmer af it-sikkerhedsrådet deltager løbende i relevant efteruddannelse inden for it-sikkerhed. It-sikkerheden er effektueret igennem intern strategi, politikker, standarder, procedurer og guidelines.

### **Medarbejdersikkerhed**

HR-funktionen varetages af HR i EG A/S samt af de enkelte ledere for medarbejderne. De ansattes sikkerhedsansvar er fastlagt gennem en fyldestgørende stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Enkelte medarbejdere er sikkerhedsgodkendte, der hvor kravet er aftalt med kunden.

Medarbejderne modtager uddannelse, træning og oplysning om informationssikkerhed igennem afdelingsledere, således at niveauet er passende og relevant i forhold til medarbejderens arbejdsopgaver, ansvarsområde og evner. Ligeledes inkluderer dette aktuelle informationer om kendte trusler, samt om hvem der skal kontaktes for yderligere råd angående informationssikkerhed.

Ved ansættelse underskriver medarbejderne en ansættelseskontrakt, der indeholder erklæring om at overholde it-sikkerhedspolitikken. Den enkelte medarbejder har ansvar for at overholde it-sikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver, samt for at rapportere eventuelle brud på it-sikkerheden eller mistanke herom til it-sikkerhedsfunktionen.

### **Styring af informationsrelaterede aktiver**

#### **Risikostyring**

Til at imødegå allerede identificerede risici er der etableret faste test af beredskabsplanen med dertilhørende dokumentation. Testplanen er bygget op over test vedrørende den fysiske sikkerhed samt test af kunde-relaterede systemer.

Direktøren for Group IT er øverste ansvarlig for, at der bliver udført risikoanalyser, og cheferne for EG Managed Services og EG Datacenter er ansvarlig for udførelsen. Den samlede beredskabsplan bliver opdateret en gang årligt i starten af året. Chefen for de enkelte business units er ansvarlig for, at de risikoanalyser, der kræver ændringer i beredskabsplanen, bliver foretaget.

EG arbejder efter principperne i ITIL (IT Infrastructure Library). ITIL er en samling af best practices, som bygger på erfaringer fra private og offentlige virksomheder. ITIL definerer en række it-processer inden for it service management, og ITIL har en procesorienteret vinkel på it-organisationen. Mange supportsystemer arbejder målrettet på at etablere digitale workflow, som understøtter ITIL-processer. Til dette formål arbejder EG med et ITSM-supportsystem, som understøtter dette workflow. Supportsystemet udvikles kontinuerligt med dertilhørende fora for undervisning i ny funktionalitet. Derudover er flere ledende medarbejdere samt driftsmedarbejdere certificeret i ITIL V3 Foundation.

Incident management er forankret i EG's Servicedesk, hvor det er muligt at åbne kontakt igennem den tilhørende kundeportal, mail eller via EG's callcenter. I Servicedesk bliver alle incidents registreret og prioriteret i henhold til de gældende retningslinjer. Det er ligeledes muligt at eskalere incidents videre til relevante personer eller afdelinger, hvis medarbejderne i servicedesken ikke kan løse den pågældende incident.

Afrapportering til kunder sker kun der, hvor dette er inkluderet i aftalen med kunden. Omfanget vil være nærmere beskrevet i kundens driftshåndbog.

### **Adgangsstyring**

#### **Fysisk**

Der er etableret fysisk adgangskontrol, således at kun autoriserede personer, der har et arbejdsrelateret behov for adgang, kan opnå adgang med nøglekort og kode. Adgangsrettighederne til sikre områder gennemgås og ajourføres i en kontrolliste. Hvis ansatte mister nøgler eller adgangskort, er der indarbejdet procedure for skift af nøgler og koder. Det er muligt for ansatte at starte en overfaldsalarm.

#### **Logisk**

For at styre adgangen til virksomhedens systemer, informationer og netværk er der etableret adgangsregler og -rettigheder. Medarbejderadgang til virksomhedens systemer sker gennem brug af SMS Passcode eller token, hvormed der sikres tofaktorautentifikation.

Ved besøg af gæster, der skal have adgang til bygningen, skal disse være under konstant opsyn af værten. Der føres logning over, hvilke gæster der har været i bygningen samt i hvilket tidsrum.

## **Komplementerende kontroller**

Forudsætninger vedrørende kundernes ansvar er beskrevet i individuelle kontrakter og driftshåndbøger. Kunden er ansvarlig for egne data. Det betyder, at kunden er ansvarlig for de ændringer, der måtte foretages i data, når der er logget på systemet med individuelle brugernavne og adgangskoder. Ved tredjepartsadgang bestilt af kunden er det kunden, som har ansvaret for opfølgning af kontrollen.

Der er enkelte kunder, som ifølge deres kontrakt har mulighed for test af backup. Kunderne er selv ansvarlige for at initiere test af backupplan.

Detaljerne fremgår af kontrolmål og kontrolaktiviteter ifølge skema med opstilling og test heraf.

### **Kryptering**

Der anvendes kryptering på al ekstern kommunikation til og fra datacentret. Der anvendes enten IPsec VPN eller SSL.

### **Fysisk sikkerhed og miljøsikring**

Der er etableret en sikker fysisk afgrænsning, som sikrer beskyttelse af områder med informationsbehandlingsudstyr samt lagringsmedier, herunder brudsikret glas i vinduer, stålgitre for vinduer, alarmsystemer, ståldøre og kameraovervågning.

I samarbejde med G4S, FireEater og DBI sikres det, at forhold vedrørende alarmsystemer og brandsikkerhed bliver kontrolleret, samt at krav om tiltag bliver overholdt.

### **Driftssikkerhed**

Tilgængeligheden af systemer og data sikres gennem en fortsat drift i tilfælde af mulige forstyrrelser. Dette sikres bl.a. gennem kontroller, der er forebyggende, detektive og korrigerende. Kontrollerne ligger inden for fysiske kontroller, procedurekontroller, tekniske kontroller og lovmæssigt styrede kontroller. Disse kontroller dækker bl.a. over følgende: autentifikation, antivirus, firewall, incident management, låse, brandalarmer, driftscenteret (er skalsikret med brudsikret glas), UPS, nødstrømsanlæg, Inergen-brandslukning, monitorering, backup og beredskabsplaner.

Der er indarbejdet adgangsstyring for håndtering og godkendelse af såvel interne som kunders brugerid'er. Der er fastlagte passwordpolitikker for autentifikation og tofaktorautentifikation, som er udmøntet i standarder.

Leverandøren foretager patchning af operativsystem (Windows). Fuldt patched systemer gælder også der, hvor det specifikt er angivet i kontrakter og driftshåndbøger.

Kundens data sikres, ved at struktureringen af netværket opbygges af VLANs, således at de enkelte kunder kun kan tilgå deres eget netværk.

Der er udarbejdet formelle forretningsgange for ændringsstyring. Formålet med dette er, at risikoen for kompromittering af virksomhedens og kundernes informationer minimeres. Introduktionen af nye systemer og større ændringer til de eksisterende systemer følger en formel proces med dokumentation, specifikation og styret implementering. Retningslinjerne for programændring gælder særligt for de SaaS-kunder, som benytter EG's egenudviklede applikationssystemer. Ændringsstyring i EG følger retningslinjer og procedurer for ændringsstyring.

Effektiv monitorering af processer giver vigtige oplysninger til både proaktivt og reaktivt at kunne undgå events, der ellers ville have påvirket overholdelsen af kundernes SLA. Målet er at minimere den tid, det tager at genetablere normal drift.

For at imødegå dette arbejder EG med forebyggende monitorering og dertilhørende korrigerende handlinger. Ved denne metode sker der ingen eller minimal påvirkning af kundens SLA.

Der, hvor det ikke er muligt at forudse events, benyttes detekterende monitorering med dertilhørende korrigerende handlinger. Denne metode gør det muligt at reagere i henhold til kundernes SLA.

EG anvender event management-værktøj til at varetage automatisk monitorering af servere, systemsoftware og applikationssoftware. Monitoreringen dækker typisk ram, diskplads, CPU-forbrug, eller om specifikke applikationer er kørende. Monitorering og advisering er sat op efter gældende aftale med kunden og dokumenteret i driftshåndbogen.

EG anvender et security information- og event management-system, der giver mulighed for logning. Værktøjet giver mulighed for at få et sikkert og centraliseret logarkiv, der automatisk analyserer logmeddelelserne i realtid. Logkonsolidering og sikker opbevaring af dokumentation via en enkelt konsol gør det muligt at få adgang til og administrere alle oplysninger. Arkivet vil sikre, at der ikke mistes nogen log-meddelelser på grund af et systemnedbrud eller et hackerangreb.

Værktøjet kan automatisk detektere og alarmere, når en kritisk hændelse opstår. En event (hændelse) kunne være et løbende angreb, et kompromitteret system, et systemnedbrud eller brugergodkendelse.

Værktøjet kan opnå et overblik over netværk. Værktøjet indeholder prædefinerede skabeloner til de mest almindelige compliance- og sikkerhedsrapporter. Logpoint indeholder standardskabeloner til fx rapportering om compliance som PCI, SOX, ISO 27001, HiPAA mv. og er en del af værktøjets standardversion. Skabelonerne kan også tilpasses efter behov eller bruges til at oprette en brugerdefineret rapport.

For systemer, der ikke kan monitoreres automatisk, er der etableret fastlagte manuelle driftsrutiner og backuprutiner. Ved fejl eskaleres disse til den ansvarlige.

### **Kommunikationssikkerhed**

Vores kommunikation til kunderne i forbindelse med drifts- og datasikkerhed er i høj grad tilpasset den individuelle kunde, men vores standard er, at kunderne modtager en månedlig rapport fra vores overvågningssystem samt en daglig rapport fra backupsystemet. Overvågningsrapporten indeholder oplysninger om servernedetid samt belastninger og ressourceforbrug. Backuprapporten indeholder en detaljeret oversigt over, hvilke filer der er foretaget korrekt backup af, og hvilke filer der er fejlet samt hvorfor.

I forbindelse med eventuelle sikkerhedshændelser kontaktes berørte kunder så hurtigt som muligt pr. telefon.

Informationssikkerhed vedrører virksomhedens samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte EG's informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed i relevant omfang.

Som brugere af EG's informationer skal alle medarbejdere følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende virksomhedens informationer i overensstemmelse med det arbejde, de udfører i virksomheden, og de skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed og særlige og/eller kritiske natur.

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsniveau. Hvor funktionsadskillelse ikke er praktisk eller økonomisk hensigtsmæssigt, skal det være muligt for medarbejdere at bryde med dette princip.

### **Anskaffelse, udvikling og vedligeholdelse af systemer**

Vi udfører patch management på systemer i datacentre. Formålet er at sikre, at der sker sikkerhedsopdatering af kritiske systemer. Det gælder både systemer, som benyttes internt, og systemer, som benyttes af eksterne kunder (kundesystemer). Alle kundesystemer bliver som standard patchet med et interval på 2 måneder eller efter gældende SLA. Dokumentation for patchniveauet er angivet i den tilhørende dokumentation for hvert system. Såfremt der er undtagelser fra standardpatchniveau, bliver det valgte patchniveau beskrevet og begrundet i de specifikke driftshåndbøger. Som udgangspunkt leveres der standardpatchning, men kunderne kan mod fakturering have undtagelser.

### **Standardpatchning:**

Forudsætningen er, at leverandøren kan vælge servicevindue til patchning.



Forudsætningen er, at patch management kan foretages med automatisk genstart af system/servere via Config Manager.

### **Undtagelser, der kræver speciel håndtering:**

Såfremt systemer ikke kan patches automatisk, og der kræves assistance fra systemkonsulenter, hver gang der patches, skal dette klart fremgå af aftalen med kunden.

- Alle sikkerhedsopdateringer installeres grundet sikkerheden hurtigst muligt.
- Alle operativsystem Update Rollups. Det anbefales, at disse opdateringer installeres, efter at de er blevet vurderet og testet.
- Alle operativsystem Service Packs. De har generelt gennemgående ændringer og forbedringer til systemerne og skal testes nøje i miljøet, før de installeres.

### **Udrulning af opdateringer**

Microsoft frigiver opdateringer den 2. tirsdag i måneden. Disse opdateringer godkendes og udrulles til en gruppe testservere, som er udvalgt på forhånd. Installation af opdateringer på de udvalgte servere skal godkendes, inden de frigives og installeres på de resterende servere i miljøet. Opdateringer udrulles til produktionsmiljøet ud fra de fastdefinerede servicevinduer. Det tilstræbes, at frigivne patches installeres inden for 2 måneder.

### **Proces for godkendelse af servicepacks**

Halvårligt vurderes alle servicepacks i samarbejde med de relevante personer, som har kendskab til det pågældende miljø. Hvis det er muligt, testes servicepacks i et evt. preprod-miljø, inden de installeres i produktionsmiljøet.

### **Håndtering af fejl**

Alle patchrutiner køres via af en RFC, hvor man vurderer de risici, der eventuelt vil være ved installation af de pågældende opdateringer. Heri er der ligeledes en vurdering af en fallbackplan samt af, hvordan man håndterer eventuelle fejl.

### **Leverandørforhold**

EG har formelle aftaler og kontrakter med leverandører, som sikrer hurtige leverancer, hvis der skulle indtræde en katastrofesituation. Disse aftaler vedligeholdes gennem en tæt dialog samt jævnlige møder med vores leverandører. Leverandøraftalerne optimeres jævnligt i forhold til vores situation og vores kunder.

### **Styring af sikkerhedshændelser**

Hvis der konstateres en sikkerhedshændelse, adviseres de berørte kunder så hurtigt som muligt, og samtidigt tages der skridt til at sikre data og systemer. Efterfølgende udarbejdes en "root cause analysis"-rapport til kunden, for så vidt muligt at sikre at hændelsen ikke kan optræde igen.

Er der tale om en intern medarbejder, der har overtrådt, eller forsøgt at overtræde, sikkerhedsreglerne uforsætligt, gives vedkommende ved første tilfælde en mundtlig advarsel og ved andet tilfælde en skriftlig advarsel. Sker det tredje gang, tages der skridt til afskedigelse af den pågældende medarbejder.

Hvis medarbejdere forsætligt overtræder, eller forsøger at overtræde, sikkerhedsreglerne, tages der straks skridt til afskedigelse, og i særligt grove tilfælde vil der være tale om bortvisning.

Alle sikkerhedshændelser rapporteres til it-sikkerhedsudvalget og dermed til ledelsen.

### **Nød-, beredskabs- og reetableringsstyring**

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Omfanget af disse foranstaltninger besluttet ud fra en afvejning af risici imod sikringsomkostninger og udmøntes i SLA'er.

Beredskabsplanerne skal omfatte:

- Skadebegrænsende tiltag
- Etablering af temporære nødløsninger
- Genetablering af permanent løsning.

Der forefindes beredskabsplaner for følgende scenarier:

- Ildebrand/vandskade, DataCenter 1 eller DataCenter 2 udbrænder.
- Oversvømmelse.
- Indbrud/ødelæggelse af udstyr.
- Langvarigt strømsvigt.
- Ulovlig indtrængen af uvedkommende personer – sabotage/terror – fysisk.
- Ulovlig indtrængen af uvedkommende personer – hacking, virusangreb.
- Medarbejder i EG begår ulovlige handlinger/ødelæggelser.

Beredskabsplanerne skal ajourføres efter behov samt testes løbende. Planerne opdateres som minimum en gang årligt.

### ***Minimumskrav for god hosting***

EG tilstræber til enhver tid at leve op til BFIH's gældende krav til god hosting samt til højt niveau af etik og troværdighed.

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

Til ledelsen i EG A/S samt kunder af EG A/S' it-drift og hostingaktiviteter i perioden 1. januar – 31. december 2018 og disses revisorer.

#### Omfang

Vi har fået til opgave at afgive erklæring om EG A/S' (EG) beskrivelse i afsnit 2 af EG's driftsydelser og om udformningen og funktionen af generelle it-kontroller, der vedrører regnskabsaflæggelsen, i relation til de kontrolmål, som er anført i beskrivelsen for perioden 1. januar 2018 - 31. december 2018.

#### EG A/S' ansvar

EG A/S 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 implementeringen og 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 revisors 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 EG A/S' beskrivelse samt om udformningen og funktionen af 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. 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 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 sit system samt for kontrollerens 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 og EG A/S' opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

#### Begrænsninger i kontroller hos en serviceleverandør

EG A/S' 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 vigtigt 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 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 afsnit 1. Det er vores opfattelse:

- (a) at beskrivelsen af EG A/S' driftsydelser, således som den var udformet og implementeret i hele perioden fra 1. januar 2018 til 31. december 2018, 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 2018 til 31. december 2018.
- (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 2018 til 31. december 2018.

### 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 EG A/S' driftsydelser i perioden 1. januar 2018 – 31. december 2018 og disses revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.


Aarhus, den 21. januar 2019

**PricewaterhouseCoopers**

Statsautoriseret Revisionspartnerselskab



Jesper Parsberg Madsen  
statsautoriseret revisor



Iraj Bastar  
senior manager

## 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

### Kontrolmål A: Informationssikkerhedspolitik

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

Kontrolmål/kontrol	PwC-test	Resultat af test
<p><b>Skriftlig politik for informationssikkerhed</b></p> <p>Ledelsen har dokumenteret et sæt politikker for informationssikkerhed, som gennemgås og vedligeholdes mindst en gang årligt samt i tilfælde af væsentlige ændringer. Sikkerhedspolitikken er godkendt af ledelsen.</p> <p>Sikkerhedspolitikken er gjort tilgængelig for medarbejdere og relevante eksterne parter via den fælles dokumentation.</p> <p>Sikkerhedspolitikken indeholder krav til opretholdelse af relevant funktionsadskillelse for at reducere risikoen for uautoriseret adgang, anvendelse eller misbrug af retigheder.</p> <p>HR er ansvarlig for tjek af jobkandidaters baggrund, herunder personligt og professionelt, i overensstemmelse med relevante love, forskrifter og etiske regler.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har påset, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum revurderes én gang årligt. Endvidere har vi påset, at den forefindes let tilgængelig for medarbejderne.</p>	<p>Under revision af overordnede procedure og retningslinjer har vi observeret, at it-sikkerhedspolitikken ikke har været formelt godkendt i erklæringsperioden.</p> <p>Vi har fået oplyst, at den manglende opdatering bl.a. skyldes overdragelsen af dele af driften til Global Connect.</p> <p>Yderligere har vi fået oplyst, at der er taget en bevidst beslutning om, at EG Managed Services er underlagt EG's overordnede it-sikkerhedspolitik, som er revideret i 2018. Der kan være særlige behov i EG Managed Services, så i 2019 vil ledelsen undersøge, om det er nødvendigt og i givet fald udarbejde et tillæg til EG's it-sikkerhedspolitik.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>

## 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
<p><b>Ledelsens forpligtelse i forbindelse med informationssikkerhed</b></p> <p>De organisatoriske ansvarsområder for informationssikkerhed, herunder ansvar og roller, er defineret i sikkerhedspolitikken.</p> <p>Endvidere er der fastlagt regler for fortrolighedsaftaler og rapportering om informationssikkerhedshændelser samt udarbejdet en fortegnelse over aktiver.</p> <p>Informationssikkerhedsbrud i datacenters ydelser håndteres af EG IT, mens EG Managed Services håndterer informationssikkerhedsbrud på OS-niveau. De udpegede security incident managers i Managed services er ansvarlige for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.</p> <p>Informationssikkerhedshændelser skal rapporteres, og Security Incident Manager skal kontaktes så hurtigt som muligt.</p> <p>Brugere, som oplever softwarefejl, rapporterer dette til Service Desk, og Security Incidentets tildeles enten Security Incident Managers i VBS- eller CS- (Citizen Solutions) divisionen alt efter typen af incident.</p> <p>I sikkerhedspolitikken står det beskrevet, at alle rapporterede informationssikkerhedshændelser skal klassificeres.</p>	<p>Vi har overordnet drøftet styring af informationssikkerheden med ledelsen.</p> <p>Vi har påset, at det organisatoriske ansvar for informationssikkerheden er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at fortrolighedsaftaler, rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Eksterne parter</b></p> <p>Identifikation af risici sker i relation til eksterne parter, herunder håndtering af sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har påset, at der er etableret betryggende procedurer for samarbejdet med eksterne leverandører.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

---

Ved ændringer, der påvirker driftsmiljøet, og hvor der anvendes services fra ekstern tredjepart, bliver disse udvalgt af driftschefen og godkendt af it-chefen. Der benyttes udelukkende anerkendte leverandører.

Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter.

---

## Kontrolmål C: Fysisk sikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
<p><b>Fysisk sikkerhedsafgrænsning</b></p> <p>Der er fysisk sikret mod adgang til sikrede områder, som indeholder enten følsomme eller kritiske informationer (for såvel nye som eksisterende medarbejdere) ved at begrænse adgang til autoriserede medarbejdere via adgangskort. Dette forudsætter dokumenteret ledelsesmæssig godkendelse.</p> <p>Personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse, eksempelvis ved service på brand- eller køleanlæg.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har ved vores besøg i datacentre observeret, at adgang til sikrede områder er begrænset ved anvendelse af et adgangssystem.</p> <p>Vi har ved stikprøvevis inspektion gennemgået procedureerne for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt om personer uden godkendelse til sikrede områder skal registreres og ledsages af en medarbejder med behørig godkendelse.</p> <p>Vi har ligeledes ved stikprøvevis inspektion gennemgået medarbejdere med adgang til sikrede områder og påset, at relevant dokumenteret ledelsesmæssig godkendelse foreligger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Sikring af kontorer, lokaler og faciliteter</b></p> <p>Der er etableret adgangskontrolsystem til alle serverrum, som sikrer, at alene ledelsesgodkendte medarbejdere har adgang. Der foretages gennemgang af eksisterende adgangsrettigheder en gang årligt samt ved ændringer.</p> <p>I sikkerhedspolitikken er en procedure for arbejde i sikrede områder beskrevet. Her er det også beskrevet, at adgangssteder som af- og pålæsningsområder, hvor uautoriserede personer kan få adgang til området, er minimeret, og at adgang kun gives til identificerede og godkendte personer.</p> <p>Der føres log med service på alle relevante understøttende foranstaltninger som brandsluk, køl og UPS.</p> <p>Der er udarbejdet en politik om, at skriveborde holdes ryddet for papir og flytbare lagringsmidler, samt at der</p>	<p>Vi har forespurgt ledelsen om de anvendte procedurer.</p> <p>Vi har gennemført inspektion af alle serverrum og påset, at alle adgangsveje er sikret med kortlæser.</p> <p>Vi har foretaget stikprøvevis kontrol af, at halvårlig gennemgang foretages.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>



### Kontrolmål C: Fysisk sikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
skal være blank skærm på informationsbehandlingsfaciliteter.		
<b>Placering og beskyttelse af udstyr</b> Datacentre er beskyttet mod miljøkatastrofer som brand, vand og varme. Serverrum er yderligere sikret med panserglass. Sikkerheden og vedligehold bliver jævnligt testet i samarbejde med serviceleverandører som G4S, FireEater og DBI. Det er i sikkerhedspolitikken beskrevet, at adgang til udstyr og kabler kun kan ske med sikkerhedsgodkendelse eller ved ledsagelse af EG IT eller andet EG-personale godkendt af IT.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion gennemgået driftsfaciliteterne og har påset, at brandbekæmpelsessystemer, monitorering af indeklima og køling i datacentre er til stede. 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.
<b>Understøttende forsyninger (forsyningsikkerhed)</b> Datacentre er beskyttet mod strømafbrydelse ved anvendelse af UPS (uninterruptible power supply) og nødstrømsanlæg. Disse anlæg bliver testet jævnligt efter testplan. Anlægget bliver også testet jævnligt i samarbejde med serviceleverandøren Atek.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har under vores besøg i datacentre 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.
<b>Sikring af kabler</b> Alle netværksskabler er placeret i serverrum, som reducerer risikoen for miljøtrusler samt uautoriseret adgang. Kabler til datakommunikation og elektricitet er beskyttet mod uautoriseret forstyrrelse og skade.	Vi har ved vores 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 samt brugerfunktioner*
- *Passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolmål/kontrol	PwC-test	Resultat af test
<p><b>Dokumenterede driftsprocedurer</b></p> <p>Ledelsen har implementeret driftsrutiner med dertilhørende proces for udførelse og opfølgning af driftschefen.</p> <p>Driftsprocedurerne er dokumenterede og tilgængelige for alle, som har behov for dem.</p> <p>NTP anvendes til tidssynkronisering.</p>	<p>Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenterede.</p> <p>I forbindelse med revision af de enkelte driftsområder har vi ved inspektion kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres.</p> <p>Vi har endvidere ved inspektion påset, at der foretages tilstrækkelig overvågning og opfølgning herpå.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Funktionsadskillelse</b></p> <p>Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen. Disse politikker og procedurer omfatter krav til,</p> <ul style="list-style-type: none"><li>• at ansvar for udvikling og opdateringer til produktionsmiljøet er adskilte</li><li>• at it-afdelingen har ikke adgang til applikationer og transaktioner</li><li>• at udviklings- og driftsaktiviteter er adskilt.</li></ul> <p>Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsniveau. Hvor funktionsadskillelse ikke er praktisk eller økonomisk hensigtsmæssig, skal det være muligt for medarbejdere at bryde med dette princip. Det gælder bl.a. udviklere, som har ret til at foretage ændringer direkte i driftsmiljøerne, hvis det er nødvendigt. Der gælder altså visse steder et</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har gennemgået brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelse mellem udviklings- og produktionsmiljøer.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

forbehold for funktionsadskillelse. Ved kritiske systemer er der dog funktionsadskillelse.

### **Foranstaltninger mod virus og lignende skadelig kode**

Der er etableret kontroller til beskyttelse mod malware og lignende skadelig kode. EG Managed Services sikrer, at antivirus findes på alle computere, og at disse opdateres regelmæssigt.

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.

### **Sikkerhedskopiering af informationer**

IBM's Tivoli Storage Manager (TSM) benyttes til backup af kunders data. Der modtages daglige rapporter fra TSM-systemet vedrørende, om backup er fuldført med succes. Hvis dette ikke er tilfældet, eskaleres dette til den ansvarlige.

Der bliver foretaget sikkerhedskopiering af data, og der foretages regelmæssig test af, at data kan genskabes fra sikkerhedskopier.

Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået backupprocedurer samt påset, at de er tilstrækkelige og formelt dokumenterede.

Vi har ved stikprøvevis inspektion gennemgået log vedrørende backup til bekræftelse af, at backups er gennemført fejlfrit, alternativt at der foretages afhjælpning i tilfælde af mislykkede backups.

Vi har ved stikprøvevis inspektion gennemgået restore-log.

Vi har gennemgået proceduren for ekstern opbevaring af backupbånd, til bekræftelse af at backups opbevares på betryggende vis.

Vi har ikke ved vores test konstateret væsentlige afvigelser.

### **Monitorering af systemanvendelse og auditlogging**

Der er implementeret logging ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl.

Security Incident Managers følger op på sikkerhedshændelser og sikrer, at adgang til systemkomponenter bliver logget.

Det står beskrevet i sikkerhedspolitikken, at logfaciliteter samt logininformation er beskyttet mod manipulation og tekniske fejl.

Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametrene for logging er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget.

Vi har endvidere ved stikprøvevis inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logs fra kritiske systemer.

Vi har ikke ved vores test konstateret væsentlige afvigelser.

---

### **Administrator- og operatørlog**

Særlig risikofyldte operativsystemer og netværkstransaktioner eller aktivitet samt brugere med privilegerede rettigheder bliver monitoreret. Afvigende forhold undersøges og løses rettidigt.

---

## 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
<p><b>Brugerregistrering og administration af privilegier</b></p> <p>Der er fastlagt en politik for adgangsstyring, som involverer, at tildeling og anvendelse af adgangsrettigheder for nye og eksisterende brugere vedrørende operativsystemer, netværk, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med virksomhedens politikker.</p> <p>Det sikres, at rettigheder er tildelt ud fra arbejdsbetinget behov, er godkendt og oprettet korrekt i systemer. Afdelingsleder godkender brugerrettigheder, og oprettelsen udføres af tekniker.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende.</p> <p>Vi har ved stikprøvevis inspektion kontrolleret, at oprettelse af brugere og tildeling af adgang er dokumenteret og godkendt i overensstemmelse med forretningsgangene.</p>	<p>Under revision af proceduren for oprettede brugere på DIH-domænet har vi observeret, at 9 teknikere med standardrettigheder er blevet oprettet uden af følge gældende og godkendte retningslinjer.</p> <p>Vi har observeret, at EG udfører intern audit på brugere med eleverede rettigheder. Ledelsen vil overveje at indføre intern audit på alle brugere i 2019.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>

## 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
<p><b>Administration af brugeradgangskoder (password)</b></p> <p>Adgange til operativsystemer, netværk, databaser og datafiler er beskyttet med password. For at sikre god kvalitet i adgangskoderne er der opsat kvalitetskrav til password, således at der kræves en minimumslængde, kompleksitet og maksimal løbetid, ligesom passwordopsætninger medfører, at password ikke kan genbruges. Endvidere bliver brugeren lukket ude ved gentagne fejl-forsøg på login.</p> <p>EG Vault anvendes til styring af adgangskoder.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og påset, at det sikres, at der anvendes en passende autentifikation af brugere på alle adgangsveje.</p> <p>Vi har ved inspektion kontrolleret, at der anvendes en passende passwordkvalitet i EG's driftsmiljø, samt ved stikprøvevis test påset, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.</p>	<p>Under revision af passwordpolitikken på DIH-domænet har vi observeret, at denne ikke er i overensstemmelse med gældende retningslinjer. Vi har observeret, at domænet er konfigureret med en maksimal password age på 180 dage, hvor proceduren foreskriver maksimalt 45 dage.</p> <p>Vi har fået oplyst, at der til dato har været en divergens mellem EG's passwordpolitik og passwordpolitikken i EG Managed Services. EG's politik siger 180 dage, og EG Managed Services indretter sig herefter. Dog vil de overveje at udfærdige et tillæg til EG's passwordpolitik, som beskriver strengere retningslinjer i hostingmiljøer.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>
<p><b>Evaluerings af brugeradgangsrettigheder</b></p> <p>Der foretages løbende periodisk gennemgang af brugerrettigheder til sikring af, at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Det sikres på disse gennemgange, at brugere kun har adgang til de</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.</p> <p>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.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

## 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
<p>netværk og netværkstjenester, som de specifikt er autoriseret til at benytte. Uoverensstemmelser undersøges og rettes rettidigt for at sikre, at adgang begrænses til dem, som har behov for adgang.</p> <p>Ansaret for dette ligger hos it-sikkerhedsudvalget.</p>		
<p><b>Inddragelse af adgangsrettigheder</b></p> <p>Der er implementeret fast procedure, som sikrer, at brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver inaktiveret rettidigt.</p> <p>Alle medarbejdere og eksterne brugeres adgangsrigheder – herunder også fjernadgang – inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter ændring i kontrakt eller aftale.</p>	<p>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 adgangsrigheder.</p> <p>Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugerkonti på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Politik for anvendelse af netværkstjenester, herunder autentifikation af brugere med ekstern forbindelse</b></p> <p>For at beskytte informationer i systemer og applikationer er datakommunikationen tilrettelagt på en hensigtsmæssig måde og tilstrækkeligt sikret mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.</p> <p>Der benyttes SMS-passcode, token eller VPN, når medarbejdere skal tilgå systemer udefra. Der er endvidere</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og påset, at der anvendes en passende autentificeringsproces for driftsmiljøet.</p> <p>Vi har ved stikprøvevis inspektion kontrolleret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN.</p> <p>Vi har ved inspektion konstateret, at netværket er segmenteret i mindre net ved hjælp af VLAN's og DMZ's for at reducere risikoen for uautoriseret adgang.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

## 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
<p>foretaget en opdeling af netværk, hvor dette er fundet nødvendigt eller er aftalt med kunden.</p> <p>Tildeling af adgang via ekstern forbindelse sker gennem formel administrationsproces, og det er et krav, at brugere, som benytter ekstern forbindelse, følger organisationens praksis.</p> <p>Det er i sikkerhedspolitikken beskrevet, at anvendelse af hemmelig autentifikationsinformation skal ske i overensstemmelse med organisationens praksis for dette.</p>		
<p><b>Styring af netværksforbindelser</b></p> <p>Der udføres halvårslige penetrationstest med en sikkerhedsscanner. Der udføres test af udvalgte IP ranges for at teste, at regler i firewall er sat rigtigt op.</p> <p>Det er i sikkerhedspolitikken beskrevet, at EG IT har det overordnede ansvar for at beskytte organisationens netværk. Medarbejdere må forbinde udstyr til netværket efter aftale med it-afdelingen, og adgang til netværket må kun ske gennem sikkerhedsgodkendte løsninger. Gæster skal benytte EG's gæstenetværk.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at styre netværksforbindelser.</p> <p>Vi har ved inspektion konstateret, at der er foretaget periodiske penetrationstest samt kontrolleret, at der er taget stilling til konstaterede svagheder.</p> <p>Vi har ved stikprøvevis inspektion gennemgået firewall-konfigurationen og påset, at reglerne i firewallen er sat hensigtsmæssigt op.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Begrænset adgang til informationer</b></p> <p>Kun personer med behov for adgang til kundespecifikke systemer har adgang. Alle adgangssøskere for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med virksomhedens politikker, til sikring af at</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at begrænse adgangen til informationer.</p> <p>Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>



## 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
<p>rettigheder tildeles ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.</p> <p>I sikkerhedspolitikken er det beskrevet, at adgang til systemer er styret af procedure for sikker log-on.</p> <p>I sikkerhedspolitikken er der beskrevet formelle politikker og procedurer for overførsel af beskyttede informationer, herunder personfølsom data, via elektroniske meddelelser. Disse politikker og regler omhandler sikker overførsel af følsom information mellem organisationen og eksterne parter.</p>	<p>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.</p>	

## 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
<p><b>Styring af software på driftssystemer</b></p> <p>Der er etableret separate it-miljøer for udvikling, test og produktion. Kun funktionsadskilt personale kan migrere ændringer mellem de enkelte miljøer.</p> <p>Der er implementeret procedure til styring af software-installation og ændringer på driftssystemer.</p> <p>Der følges løbende op på tekniske sårbarheder i anvendte informationssystemer med evaluering af eksponering for sådanne sårbarheder.</p> <p>Ved ændringer på kundespecifikke systemer bliver der udført test, der hvor dette er aftalt.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at adskillelse mellem enkelte miljøer opretholdes.</p> <p>Vi har ved inspektion påset, at ændringerne testes i testmiljøet.</p> <p>Vi har ved stikprøvevis inspektion gennemgået ændringer i perioden og har påset, at ændringerne er dokumenteret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p><b>Ændringsstyring</b></p> <p>Ændringer af organisationen, processer, faciliteter og systemer, som påvirker informationssikkerheden, styres gennem formel proces. Dette involverer, at ændringer til operativsystemer og netværk bliver testet af kvalificeret personale inden flytning til produktion.</p> <p>I sikkerhedspolitikken står det beskrevet, at sikkerhedstests skal udføres efter behov.</p> <p>Test af ændringer til operativsystemer og netværk godkendes før flytning til produktion. Ændringer i kundespecifikke systemer registreres i helpdesk-systemet som incidents. Dette inkluderer bl.a. information om dato, status og opfølgende kommentarer. Nødændringer af operativsystemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået change management-procedureernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur.</p> <p>Vi har desuden konstateret, at en formel change management-procedure er blevet implementeret i en hele organisationen.</p> <p>Vi har ved stikprøvevis inspektion gennemgået ændringsønsker for følgende:</p> <ul style="list-style-type: none"><li>• Registrering af ændringsanmodninger i det dertil etablerede system.</li><li>• Dokumenteret test af ændringer, herunder godkendelse.</li><li>• Godkendelse skal være opnået før implementering. Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende.</li><li>• Dokumenteret plan for tilbagerulning, hvor relevant.</li></ul>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

## Kontrolmål G: Katastrofeplan

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

Kontrolmål/kontrol	PwC-test	Resultat af test
<p><b>Opbygning/struktur af katastrofeberedskab</b></p> <p>Den samlede katastrofeplan består af en overordnet katastrofestyringsprocedure samt operationelle katastrofeplaner for de konkrete katastrofeområder, som har til formål at sikre kontinuitet i kritiske situationer.</p> <p>Den operationelle katastrofeplan indeholder beskrivelse af katastrofeorganisationen med de ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser for de nødvendige indsatsgrupper. For de enkelte platforme er udarbejdet detaljerede indsatsgruppeinstrukser for reetablering i forhold til nød-drift, så informationssikkerhedskontinuitet sikres i kritiske situationer. Planen revideres en gang årligt.</p>	<p>Vi har forespurgt ledelsen om de procedurer/kontrolakti-viteter, der udføres.</p> <p>Vi har gennemgået det udleverede materiale vedrørende ka-tastrofeberedskab samt påset, at den organisatoriske og ope-rationelle it-katastrofeplan indeholder ledelsesmæssige funk-tionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.</p>	<p>Under revision af procedurer for beredskabsplaner og relaterede do-kumenter har vi observeret, at denne ikke har været opdateret og godkendt i 2018.</p> <p>Vi har observeret, at it-nødplanen har været testet ved stikprøvevis restore af it-systemer, men den or-ganisatoriske og forretningsmæs-sige del af beredskabsplanen har ikke været testet i 2018.</p> <p>Vi har fået yderligere oplyst, at fremadrettet er Global Connect an-svarlig for beredskabsplaner og test af disse i forhold til datacenterydel-ser op til og med Hypervisor.</p> <p>EG har indført business continuity-planer for at sikre driftssikkerhe-den. Heraf fremgår processer for håndtering af nedbrud.</p> <p>Vi har ikke ved vores test konstate-ret yderligere væsentlige afvigelser.</p>
<p><b>Test af katastrofeberedskab</b></p> <p>Der sker årlig test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier.</p> <p>Der sker test af dele af beredskabsplan efter en testplan. Dette inkluderer realtidstest, hvor dette giver mening.</p>		