www.pwc.dk

EG A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. februar 2020 til 31. december 2020 i relation til EG A/S' support- og udviklingsydelser i relation til SonWin

Juni 2021

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for EG A/S' kunder, der har anvendt EG A/S' support- og udviklingsydelser i relation til SonWin, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som EG A/S' kunder selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber.

EG A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af EG A/S' support- og udviklingsydelser i relation til SonWin, der har behandlet kunders transaktioner i hele perioden fra 1. februar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til EG A/S' support- og udviklingsydelser i relation til SonWin var udformet og implementeret, herunder redegør for:

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

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til EG A/S' support- og udviklingsydelser i relation til SonWin foretaget i perioden fra 1. februar 2020 til 31. december 2020

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. februar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. februar 2020 til 31. december 2020.

Ballerup, 24. juni 2021

Rasmus Dalby Martinussen
Adm. direktør

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

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. februar 2020 til 31. december 2020 i relation til EG A/S' support- og udviklingsydelser i relation til SonWin

Til: EG A/S, EG A/S' kunder og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om EG A/S' beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til EG A/S' support- og udviklingsydelser i relation til SonWin, der har behandlet kunders transaktioner i hele perioden fra 1. februar 2020 til 31. december 2020 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

EG A/S' ansvar

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

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

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

Revisors ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af support- og udviklingsydelser i relation til SonWin samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne

ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som EG A/S har specificeret og beskrevet i ledelsens udtalelse.

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

Begrænsninger i kontroller hos en serviceleverandør

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

Konklusion

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

a) at beskrivelsen af, hvordan generelle it-kontroller i relation til EG A/S' support- og udviklingsydelser i relation til SonWin, således som de var udformet og implementeret i hele perioden fra 1. februar 2020 til 31. december 2020, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. februar 2020 til 31. december 2020, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. februar 2020 til 31. december 2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt EG A/S' support- og udviklingsydelser i relation til SonWin, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 24. juni 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
statsautoriseret revisor

3 EG's beskrivelse af generelle it-kontroller, der vedrører regnskabsaflæggelsen for udviklings- og driftsydelser i Danmark

Indledning

Denne systembeskrivelse vedrører de generelle it-kontroller i tilknytning til applikationsudvikling og hosting-aktiviteter i EG A/S, som er ejet af kapitalfonden Francisco Partners. Standard-it-drift og hosting-aktiviteter leveres af EG Managed Services, og applikationsudvikling varetages af EG Utility, som i denne erklæring er benævnt EG.

Applikationsudviklingen omfatter bl.a. applikationen SonWin. Der arbejdes efter de samme procedurer og metoder på alle udviklingsopgaver hos EG Utility.

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 fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage.

Denne erklæring er udarbejdet efter "exclusive"-metoden og inkluderer således ikke kontroller hos underleverandøren Global Connect A/S. Disse kontroller dækkes for 2020 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 for 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:

- **Hostede kunder**: Omfatter kunder, hvis systemer er hostet på dedikerede fysiske eller virtuelle servere. EG har det samlede ansvar for setuppet, men udfører primært udvikling og vedligehold af applikationssoftware.

- **Udvikling af applikationer**: Omfatter kunder, som får udviklet applikationer hos EG. Denne erklæring omfatter kun EG Utility.

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.

It-informationssikkerhedspolitikker og organisering af informationssikkerhed

Det overordnede ansvar for it-sikkerheden i EG ligger i It-sikkerhedsudvalget, (EG Security Commitee), der behandler alle it-sikkerhedsspørgsmål af principiel karakter.

It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, mellemledere samt driftsmedarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen i EG.

EG's It-sikkerhedsudvalg består af:

- CFO, Henrik Hansen, formand
- CEO, Mikkel Bardram
- EVP, Jesper Andersen
- EVP Johnny Iversen
- EVP Erik Tomren
- VP Corporate IT, Brian Wested Laursen
- Director Compliance, Søren Wolstrup

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

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.

VP for Corporate IT er ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer, den daglige ledelse, samt medlem af it-sikkerhedsudvalget.

Det er medarbejdernes daglige leder, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken, ud til den enkelte ansatte.

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-sikkerhedudvalget, hvor disse behandles.

Når it-sikkerhedspolitikken, it-sikkerhedshåndbogen og beredskabsplanerne opdateres, kommunikeres dette til medarbejdere, hvorigennem medarbejderne derefter kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til de lokale it-sikkerhedskoordinatorer / Security Incident Managers , der sørger for relevante rettelser.

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, så 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 kunderelaterede systemer.

VP for Corporate IT er øverste ansvarlig for, at der bliver udført risikoanalyser. , 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.

Adgangsstyring

Fysisk
Der er etableret fysisk adgangskontrol, så 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.

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.

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.

Kryptering

Der anvendes kryptering på al ekstern kommunikation til og fra datacenteret. 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 brudsikkert 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 brudsikkert glas), UPS, nødstrømsanlæg, Inergen-brandslukning, monitorering, backup og beredskabsplaner. Disse kontroller udføres primært af EG's underleverandører.

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

EG foretager patchning af operativsystem efter leverandørens anbefalinger (Windows). Fuldt patchede systemer gælder også der, hvor det specifikt er angivet i kontrakter og driftshåndbøger.

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 logmeddelelser 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 en 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

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. Funktionsadskillelse implementeres, hvor det er forretningsmæssigt muligt.

Anskaffelse, udvikling og vedligeholdelse af systemer

EG har ansvaret for at udføre patch management på systemer i datacentrene. 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).

Anskaffelse, udvikling og vedligeholdelse af applikationer

Udvikling foregår efter moderne agile principper, hvor vi gennem brugerinddragelse og involvering sikrer en løsning, der lever op til kravene hos vores kunder.

Sikkerhed, brugervenlighed og stabilitet er grundstenene og fundamentet for alle produkter udviklet af EG Utility.

Udviklingen er drevet af både interne initiativer og input fra kunder. Vi arbejder altid efter en fast ramme/skabelon, der dog varierer alt efter størrelse og kompleksitet af den enkelte opgave. Ved nye features, mindre rettelser, opdatering og fejlrettelser følges processen beskrevet i 'Generelle Samarbejdsvilkår' som opdateres årligt.

Opgaver, projekter og planlægning foregår i opgavestyringssystem. Opgavestyringssystemet kobles direkte til rettelser i kildekoden og muliggør fuld sporbarhed vedr. nye features og fejlrettelser.

Support og hjælp fås via Sonlinc ServiceDesk, som beskrevet i Generelle Samarbejdsvilkår.

Hjælp til selvhjælp og generelle vejledninger findes på support-site og er tilgængelig for alle.

Interne procedurer sikrer gennem overvågning og monitorering, at vi lever op til vores opstillede mål for oppetider og svartider.

Leverandørforhold

EG har formelle aftaler og kontrakter med leverandører, som sikrer hurtige leverancer, hvis der skulle indtræffe 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 besluttes ud fra en afvejning af risici imod

sikringsomkostninger og udmøntes i SLA'er. Ift. beredskabsplaner er de driftsmæssige forhold håndteret hos underleverandører.

Beredskabsplanerne skal omfatte:

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

Der forefindes beredskabsplaner for følgende scenarier:

- Ildebrand/vandskade.
- 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.

Komplementerende kontroller

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.

Processer og kontroller hos kunden er ikke omfattet af nærværende erklæring. Kunden er selv ansvarlig for at anvende SonWin på en måde, der er i overensstemmelse med lovgivningens krav. Dette omfatter blandt andet:

- At varetage oplysningsforpligtelser over for kundens kunder.
- At sikre, at de personoplysninger, kunderne har registreret om deres kunder, overholder lovgivningen.
- At varetage it-drift og fysisk sikring i den forbindelse.
- At have ansvaret for at etablere betryggende kontroller i forhold til administrationen af egne brugere, herunder, men ikke begrænset til, periodisk gennemgang og vurdering af brugernes adgange samt deres fortsatte anvendelse.
- At sikre, at kommunikationen med EG følger de officielle kanaler, herunder at e-mail ikke anvendes til udveksling af personoplysninger om kundens kunder.
- At sikre, at eventuelle integrationer til andre systemer overholder lovgivningen.
- At sikre, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger.
- At sikre, at oplysninger om behandling af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.
- At sikre, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder sikre besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

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

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

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

4.2 Testhandlinger

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

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål A: Informationssikkerhedspolitik

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Skriftlig politik for informationssikkerhed 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. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere og relevante eksterne parter via den fælles dokumentation. Sikkerhedspolitikken indeholder krav til opretholdelse af relevant funktionsadskillelse for at reducere risikoen for uautoriseret adgang, anvendelse eller misbrug af rettigheder. HR er ansvarlig for tjek af jobkandidaters baggrund, herunder personligt og professionelt, i overensstemmelse med relevante love, forskrifter og etiske regler.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Ledelsens forpligtelse i forbindelse med informationssikkerhed De organisatoriske ansvarsområder for informationssikkerhed, herunder ansvar og roller, er defineret i sikkerhedspolitikken. Endvidere er der fastlagt regler for fortrolighedsaftaler og rapportering om informationssikkerhedshændelser samt udarbejdet en fortegnelse over aktiver. De udpegede security incident managers i forretningsenheden og i koncernen er ansvarlige for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. Informationssikkerhedshændelser skal rapporteres, og security incident manager skal kontaktes så hurtigt som muligt. Brugere, som oplever softwarefejl, rapporterer dette til Servicedesk. I sikkerhedspolitikken står det beskrevet, at alle rapporterede informationssikkerhedshændelser skal klassificeres.	Vi har overordnet drøftet styring af informationssikkerheden med ledelsen. Vi har påset, at det organisatoriske ansvar for informationssikkerheden er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at fortrolighedsaftaler, rapportering om informationssikkerhedshændelser, samt fortegnelse over aktiver er udarbejdet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Eksterne parter Identifikation af risici sker i relation til eksterne parter, herunder håndtering af sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder. Ved ændringer, der påvirker driftsmiljøet, og hvor der anvendes services fra ekstern tredjepart, bliver disse udvalgt og godkendt af ledelsen. Der benyttes udelukkende anerkendte leverandører.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret betryggende procedurer for samarbejdet med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Fysisk sikkerhedsafgrænsning 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. Personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse, eksempelvis ved service på brand- eller køleanlæg.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved vores besøg i datacentrene observeret, at adgang til sikrede områder er begrænset ved anvendelse af et adgangssystem. Vi har ved stikprøvevis inspektion gennemgået procedurerne 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. Vi har ligeledes ved stikprøvevis inspektion gennemgået medarbejdere med adgang til sikrede områder og påset, at relevant dokumenteret ledelsesmæssig godkendelse foreligger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Sikring af kontorer, lokaler og faciliteter 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. 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. Der føres log med service på alle relevante understøttende foranstaltninger som brandsluk, køl og UPS. Der er udarbejdet en politik om, at skriveborde holdes ryddet for papir og flytbare lagringsmidler, samt at der skal være blank skærm på informationsbehandlingsfaciliteter.	Vi har forespurgt ledelsen om de anvendte procedurer. Vi har gennemført inspektion af alle serverrum og påset, at alle adgangsveje er sikret med kortlæser. Vi har foretaget stikprøvevis kontrol af, at periodisk gennemgang foretages.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Placering og beskyttelse af udstyr Datacentre er beskyttet mod miljøkatastrofer som brand, vand og varme. Serverrum er yderligere sikret med panserglas. 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. Datacentre driftes af tredjepart.	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 datacentrene 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.
Understøttende forsyninger (forsyningssikkerhed) 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 leverandør. Datacentre driftes af tredjepart.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har under vores besøg i datacentrene observeret, at der foretages monitorering af UPS eller nødstrømsanlæg. Vi har ved stikprøvevis inspektion gennemgået dokumentationen for vedligeholdelse, til bekræftelse af at UPS eller nødstrømsanlæg løbende vedligeholdes og testes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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
Sikring af kabler Alle netværkskabler er placeret i serverrum, som reducerer risikoen for miljøtrusler samt uautoriseret adgang. Kabler til datakommunikation og elektricitet er beskyttet mod uautoriseret forstyrrelse og skade. Datacentre driftes af tredjepart.	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 og 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
Dokumenterede driftsprocedurer Ledelsen har implementeret driftsrutiner med dertilhørende proces for udførelse og opfølgning på driften. Driftsprocedurerne er dokumenterede og tilgængelige for alle, som har behov for dem. NTP anvendes til tidssynkronisering.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenterede. 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. Vi har endvidere ved inspektion påset, at der foretages tilstrækkelig overvågning og opfølgning herpå.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Funktionsadskillelse Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen. Disse politikker og procedurer omfatter krav til, • at ansvar for udvikling og opdateringer til produktionsmiljøet er adskilt • at driftsafdelingen ikke har ikke adgang til applikationer og transaktioner • at udviklings- og driftsaktiviteter er adskilt. 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	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelse mellem udviklings- og produktionsmiljøer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
ret til at foretage ændringer direkte i driftsmiljøerne, hvis det er nødvendigt. Der gælder altså visse steder et forbehold for funktionsadskillelse. Ved kritiske systemer er der dog funktionsadskillelse. Backupdata opbevares separat fra produktionsdata i overensstemmelse med principperne om funktionsadskillelse.		
Foranstaltninger mod virus og lignende skadelig kode Der er etableret kontroller til beskyttelse mod malware og lignende skadelig kode. Det sikres, 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 Der tages løbende backup af kunders data. Der modtages daglige rapporter fra backupsystemet, 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.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Monitorering af systemanvendelse og auditlogning Der er implementeret logning ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl. Security incident managers følger op på sikkerhedshændelser og sikrer, at adgang til systemkomponenter bliver logget. Det står beskrevet i sikkerhedspolitikken, at logfaciliteter samt loginformation er beskyttet mod manipulation og tekniske fejl. **Administrator- og operatørlog** Særligt risikofyldte operativsystemer og netværkstransaktioner eller aktivitet samt brugere med privilegerede rettigheder bliver monitoreret. Afvigende forhold undersøges og løses rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametrene for logning 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 logge fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Fejlrettelser Ledelsen har etableret procedurer for håndtering af support. Dette omfatter bl.a. en umiddelbar vurdering af, hvorvidt et incident klassificeres som kritisk og derfor bliver prioriteret anderledes. Denne vurdering foretages ud fra faste retningslinjer, der er tilgængelige for alle, der varetager support: Klassificering af incidents (prioritering ud fra impact og urgency): • Matche incidents med tidligere konstaterede Incidents, Problems og Known Errors • Igangsætte relevante RFC, når forhold er afklaret. Der foretages løbende opfølgning på indrapporterede incidents, og der foretages om nødvendigt eskalering heraf.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået proceduren for håndtering af incidents. Vi har ved stikprøvevis inspektion påset, at incidents klassificeres, at der er match mellem incidents og tidligere konstaterede incidents samt at relevante RFC igangsættes rettidigt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Brugerregistrering og administration af privilegier 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. Det sikres, at rettigheder er tildelt ud fra et arbejdsbetinget behov, er godkendt og oprettet korrekt i systemer. Afdelingsleder godkender brugerrettigheder.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion kontrolleret, at oprettelse af brugere og tildeling af adgang er dokumenteret og godkendt i overensstemmelse med forretningsgangene.	Vi har ved vores test konstateret, at der er implementeret formaliserede centrale procedure for adgangsstyring, men der for specifikke systemer ikke er etableret særskilte procedurer. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
Administration af brugeradgangskoder (passwords) 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 passwords ikke kan genbruges. Endvidere bliver brugeren lukket ude ved gentagne fejlforsøg på login. Der anvendes værktøj til styring af adgangskoder.	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. 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.	Vi har ved vores test konstateret, at 1 fratrådt bruger ikke er nedlagt i specifikke systemer. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Evaluering af brugeradgangsrettigheder 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 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.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion kontrolleret, at der foretages periodiske gennemgange til bekræftelse af, at disse har fundet sted, samt påset, at identificerede afvigelser afhjælpes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Inddragelse af adgangsrettigheder Der er implementeret fast procedure, som sikrer, at brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver inaktiveret rettidigt. Alle medarbejdere og eksterne brugeres adgangsrettigheder – herunder også fjernadgang – inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter ændring i kontrakt eller aftale.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og at der foretages opfølgning i henhold til forretningsgangene på de tildelte adgangsrettigheder. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugerkonti på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Politik for anvendelse af netværkstjenester, herunder autentifikation af brugere med ekstern forbindelse For at beskytte informationer i systemer og applikationer er datakommunikationen tilrettelagt på en hensigtsmæssig måde og tilstrækkeligt sikret mod risiko for tab	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og påset, at der anvendes en passende autentifikationsproces for driftsmiljøet. Vi har ved stikprøvevis inspektion kontrolleret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

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

Kontrolmål/kontrol	PwC-test	Resultat af test
af autenticitet, integritet, tilgængelighed samt fortrolighed. Der benyttes SMS-passcode, token eller VPN, når medarbejdere skal tilgå systemer udefra. Der er endvidere foretaget en opdeling af netværk, hvor dette er fundet nødvendigt eller er aftalt med kunden. Tildeling af adgang via ekstern forbindelse sker gennem formel administrationsproces, og det er et krav, at brugere, som benytter ekstern forbindelse, følger organisationens praksis. Det er i sikkerhedspolitikken beskrevet, at anvendelse af hemmelig autentifikationsinformation skal ske i overensstemmelse med organisationens praksis for dette.	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.	
Styring af netværksforbindelser Der udføres halvårlige penetrationstest med en sikkerhedsscanner. Der udføres test af udvalgte IP ranges for at teste, at regler i firewallen er sat rigtigt op. 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.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at styre netværksforbindelser. Vi har ved inspektion konstateret, at der er foretaget periodiske penetrationstest, samt kontrolleret, at der er taget stilling til konstaterede svagheder. Vi har ved stikprøvevis inspektion gennemgået firewall-konfigurationen og påset, at reglerne i firewallen er sat hensigtsmæssigt op.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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
Begrænset adgang til informationer Kun personer med behov for adgang til kundespecifikke systemer har adgang. Alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med virksomhedens politikker, til sikring af at rettigheder tildeles ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer. I sikkerhedspolitikken er det beskrevet, at adgang til systemer er styret af procedure for sikker log-on. I sikkerhedspolitikken er der beskrevet formelle politikker og procedurer for overførsel af beskyttede informationer, herunder personfølsomme data, via elektroniske meddelelser. Disse politikker og regler omhandler sikker overførsel af følsom information mellem organisationen og eksterne parter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at begrænse adgangen til informationer. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion kontrolleret, at tildeling af adgang til data og systemer udføres ud fra et arbejdsrelateret behov og er godkendt i overensstemmelse med forretningsgangene.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Styring af software på driftssystemer Der er etableret separate it-miljøer for udvikling, test og produktion. Kun funktionsadskilt personale kan migrere ændringer mellem de enkelte miljøer. Der er implementeret procedure til styring af softwareinstallation og ændringer på driftssystemer. Der følges løbende op på tekniske sårbarheder i anvendte informationssystemer med evaluering af eksponering for sådanne sårbarheder. Ved ændringer på kundespecifikke systemer bliver der udført test, der hvor dette er aftalt. Applikationer, operativsystemer, databaser og tredjepartssoftware patches i overensstemmelse med anbefalingerne fra de respektive leverandører. Hertil opdateres eller erstattes applikationer, operativsystemer, databaser og tredjepartssoftware, hvis de ikke længere supporteres af leverandøren. Netværksenheder patches i overensstemmelse med anbefalingerne fra netværksproducenten. Tilsvarende opdateres eller erstattes netværksenheder, hvis ikke firmware eller hardware længere supporteres af netværksproducenten.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at adskillelse mellem de enkelte miljøer opretholdes. Vi har ved inspektion påset, at ændringerne testes i testmiljøet. Vi har ved stikprøvevis inspektion gennemgået ændringer i perioden og har påset, at ændringerne er dokumenteret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringsstyring Ændringer af organisationen, processer, faciliteter og systemer, som påvirker informationssikkerheden, styres gennem en formel proces. Dette involverer, at ændringer til operativsystemer og netværk bliver testet af kvalificeret personale inden flytning til produktion.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået change management-procedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Kontrolmål/kontrol	PwC-test	Resultat af test
I sikkerhedspolitikken står det beskrevet, at sikkerhedstests skal udføres efter behov. 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.	Vi har desuden konstateret, at en formel change management-procedure er blevet implementeret i hele organisationen. Vi har ved stikprøvevis inspektion gennemgået ændringsønsker for følgende: • Registrering af ændringsanmodninger i det dertil etablerede system. • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. • Dokumenteret plan for tilbagerulning, hvor relevant.	
Ændringsstyring/udvikling af applikationer EG anvender formelle procedurer og værktøjer til at styre ændringer og udvikling af applikationer. Håndtering af ændringerne og udvikling er en del af release og deployment management. Ingen udvikling igangsættes, medmindre der er et kundedefineret eller lovgivningsmæssigt behov herfor. Ingen ændringer i produktionen implementeres, før change er godkendt af en intern udvikler samt testet, og fallback-plan er udformet. Adgang til kildekode er begrænset til personer med et arbejdsbetinget behov. Der anvendes kun anonyme testdata. Der er adskilte udviklings-, test- og driftsmiljøer. Miljøerne er alle underlagt sikkerhedskrav.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået change management-procedurernes tilstrækkelighed, som er en del af release og deployment management, samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur.	Vi har ved vores test konstateret, at formaliseringen af udviklingsopgaver ikke dokumenteres i overensstemmelse med proceduren. Men releases testes ud fra flere teststrategier, før de lægges i produktion. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Release management-applikationer EG varetager styring af release. Der releases efter behov og ofte flere gange i løbet af ugen. En typisk løsning af en opgave omfatter følgende: • Specificering af opgave i opgavestyringsværktøj • Nedbrydning af opgave i samarbejde med relevante personer (udvikler, product manager, etc.) • Udvikling af funktionalitet og løbende feedback • Udvikling af automatiseret test • Code-review af anden udvikler • Evt. tilretninger jvf. review • Klargøring af deploy til testmiljø. Jf. EG's projektmodel indgår sikkerhed i alle faser af udviklingen. For hver release sikres følgende: • Sporbarhed i indholdet af releases til releasens enkeltdele • Koordination, involvering og styring af de relevante parter i forbindelse med en release • Sammenhængende test af den samlede release, herunder integrationstest og en samlet performance- og load-test • Code review • Tilstedeværelsen af rollback-planer for en release • Kommunikation til kunder om nye releases.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået release management-procedurernes tilstrækkelighed. Vi har ved stikprøvevis inspektion kontrolleret, hvorvidt der er etableret sporbarhed, koordinering, styring, tilstrækkelig og effektiv test, code review, rollback-planer samt proces for kommunikation til kunder for hver release.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Kontrolmål/kontrol	PwC-test	Resultat af test
Deployment management For hver release er der procedurer, der sikrer, at: • Kode på testmiljø opdateres • Automatiserede tests af forretningsregler eksekveres • Automatiserede tests af brugergrænseflade eksekveres • Manuel regressionstest gennemføres efter behov • Kode efter succesfulde tests gøres klar til opdatering og arkivering • Alle relevante miljøer opdateres.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået deployment management-procedurernes tilstrækkelighed. Vi har ved stikprøvevis inspektion kontrolleret, hvorvidt koden opdateres og automatisk testes ud fra forretningsregler og brugergrænseflader.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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
Opbygning/struktur af katastrofeberedskab 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. 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 nøddrift, så informationssikkerhedskontinuitet sikres i kritiske situationer. Planen revideres en gang årligt. **Test af katastrofeberedskab** Der sker årligt test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier. Der sker test af dele af beredskabsplan efter en testplan. Dette inkluderer realtidstest, hvor dette giver mening.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået det udleverede materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

PENNEO

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

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

Rasmus Dalby Martinussen
Underskriver
På vegne af: EG A/S
Serienummer: PID:9208-2002-2-877756227248
IP: 185.128.xxx.xxx
2021-06-24 09:41:39Z
NEM ID

Jesper Parsberg Madsen
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: PID:9208-2002-2-427963640472
IP: 83.136.xxx.xxx
2021-06-24 10:01:53Z
NEM ID