EG Danmark A/S

Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller for perioden fra 1. januar 2025 til 31. december 2025 i relation til EG Danmark A/S' udviklings- og driftsydelser i forbindelse med Silkeborg Data

April 2026

Indhold

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet af EG Danmark A/S (EG) til brug for kunder, der har anvendt udviklings- og driftsydelser i forbindelse med Silkeborg Data, 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 deres regnskaber.

JN Data A/S, Aamazon Web Services og Redcentric er serviceleverandører, der leverer hosting- og backupydelser til EG. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos EG og ikke kontrolmål og tilhørende kontroller hos JN Data A/S, Aamazon Web Services og Redcentric. Vores vurdering har ikke omfattet kontroller hos JN Data A/S, Aamazon Web Services og Redcentric.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos kunderne, der er forudsat i udformningen af vores kontroller, er hensigtsmæssigt designet og implementeret og er operationelt effektive. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af sådanne komplementære kontroller hos kunderne.

EG bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en hensigtsmæssig præsentation af generelle it-kontroller i relation til EG's udviklings- og driftsydelser i forbindelse med Silkeborg Data, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2025 til 31. december 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til EG's udviklings- og driftsydelser i forbindelse med Silkeborg Data var designet 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 designet og implementeret til at nå disse mål
   - Kontroller, som vi med henvisning til udviklings- og driftsydelser i forbindelse med Silkeborg Data har forudsat ville være implementeret af kunderne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for generelle it-kontroller

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til udviklings- og driftsydelser i forbindelse med Silkeborg Data foretaget i perioden fra 1. januar 2025 til 31. december 2025

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af generelle it-kontroller i relation til udviklings- og driftsydelser i forbindelse med Silkeborg Data, der er beskrevet, 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 alle aspekter ved generelle it-kontroller i relation til udviklings- og driftsydelser i forbindelse med Silkeborg Data, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt designet og implementeret og var operationelt effektive i hele perioden fra 1. januar 2025 til 31. december 2025. 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

(iii) Kontrollerne var anvendt konsistent som designet og implementeret, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2025 til 31. december 2025.

Aarhus, 30. april 2026
EG Danmark A/S

Rasmus Dalby Martinussen
Vice President

2. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres design, implementering og operationelle effektivitet

Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller for perioden fra 1. januar 2025 til 31. december 2025 i relation til EG's udviklings- og driftsydelser i forbindelse med Silkeborg Data

Til: EG Danmark A/S (EG), deres kunder og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om EG's beskrivelse i afsnit 3 af generelle it-kontroller i relation til udviklings- og driftsydelser i forbindelse med Silkeborg Data, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2025 til 31. december 2025 (beskrivelsen), og om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

JN Data A/S, Aamazon Web Services og Redcentric er serviceleverandører, der leverer hosting- og backupydelser til EG. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos EG og ikke kontrolmål og tilhørende kontroller hos JN Data A/S, Aamazon Web Services og Redcentric. Vores undersøgelse har ikke omfattet kontroller hos JN Data A/S, Aamazon Web Services og Redcentric.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos kunderne, der er forudsat i udformningen af EG's kontroller, er hensigtsmæssigt designet og implementeret og er operationelt effektive. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af sådanne komplementære kontroller hos kunderne.

EG's ansvar

EG er ansvarlig for udarbejdelsen af beskrivelsen og den 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 fastlægge kontrolmålene og anføre dem i beskrivelsen; for at identificere de risici, der truer opnåelsen af kontrolmålene; for at identificere kriterierne samt for at designe, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål. Kontrolmålene er fastlagt af EG og er anført i beskrivelsen.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om hensigtsmæssigheden af præsentationen af EG's beskrivelse samt om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, 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 hensigtsmæssigt præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og implementeret og er operationelt effektive.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen af en serviceleverandørs system og om designet, implementeringen og den operationelle effektivitet af kontroller hos en serviceleverandør, omfatter udførelse af handlinger for at opnå bevis for beskrivelsen samt for kontrollernes design, implementering og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er hensigtsmæssigt præsenteret, og at kontrollerne ikke er hensigtsmæssigt designet og implementeret og ikke er operationelt effektive. Vores handlinger har også 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 mål samt relevansen af de kriterier, som EG har specificeret og beskrevet i afsnit 1.

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

Iboende begrænsninger

EG'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 aspekter ved udviklings- og driftsydelser i forbindelse med Silkeborg Data, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør eller serviceunderleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser i udviklings- og driftsydelser i forbindelse med Silkeborg Data. Herudover er fremskrivningen til fremtidige perioder af enhver vurdering af hensigtsmæssigheden af præsentationen af beskrivelsen, eller af konklusioner om hensigtsmæssigheden af designet og implementeringen samt den operationelle effektivitet af de kontroller, der er nødvendige for at nå de tilhørende kontrolmål, undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

På baggrund af kriterierne og de kontrolmål, der er beskrevet i EG's udtalelse i afsnit 1, er det vores opfattelse:

a) at beskrivelsen af generelle it-kontroller i relation til udviklings- og driftsydelser i forbindelse med Silkeborg Data, som designet og implementeret i hele perioden fra 1. januar 2025 til 31. december 2025, i alle væsentlige henseender er hensigtsmæssigt præsenteret

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret med henblik på at opnå høj grad af sikkerhed for, at de anførte kontrolmål ville være opnået, hvis de beskrevne kontroller var operationelt effektive i hele perioden fra 1. januar 2025 til 31. december 2025, og hvis kunderne udførte de komplementære kontroller, der er omtalt i afsnit 3

c) at de testede kontroller i alle væsentlige henseender har fungeret effektivt i hele perioden fra 1. januar 2025 til 31. december 2025. De testede kontroller var de kontroller, som sammen med de komplementære kundekontroller omtalt i afsnit 3, forudsat at de var operationelt effektive, var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Vi har af EG fået til opgave at afgive erklæring, og derfor er denne erklæring samt beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf tiltænkt EG.

Vi tillader kun, at EG – efter eget skøn – offentliggør denne erklæring i dens fulde længde, herunder beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf. Offentliggørelse må kun ske til kunder, der har anvendt EG's udviklings- og driftsydelser i forbindelse med Silkeborg Data i hele eller dele af perioden fra 1. januar 2025 til 31. december 2025, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information om kontroller, som kunderne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. PwC påtager sig intet ansvar over for kunderne eller deres revisorer.

Vores erklæring må ikke anvendes til andre formål og må ikke udleveres til andre parter.

Aarhus, 30. april 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3. Systembeskrivelse

3.1. Beskrivelse af tjenester dækket af rapporten

EG udfører systemudvikling, vedligeholdelse, support, uddannelse, installation, drift af løn- og vagtplansystem, der anvendes til offentlige kunder i Danmark.

Følgende løsninger og moduler tilbydes til kunder:

SD Løn

- SD APOS
- SD Arbejdsgange
- SD Arbejdstidsopgørelser
- SD Arbejdstidsplaner
- SD Arkiv
- SD Basisløn 3270
- SD BI
- SD Bogholderi
- SD Brugeradministration
- SD Budget
- SD Dataleverancer for udtræk (BSL)
- SD Datawarehouse
- SD ESDH
- SD Fraværspolitikker
- SD Fremmødeprofiler
- SD Fremmødeprofiler v2
- SD Funktionshierarki
- SD Integration til LMS (Plan2learn)
- SD Kontrol
- SD Løn (Main)
- SD Lønadministration - stor pakke
- SD Medarbejdernet
- SD MinLøn
- SD Notifikationer
- SD Organisationskomponent
- SD Organisationsstruktur
- SD Personaleweb
- SD Refusion
- SD Snitflader og Webservices
- SD Vis lønseddel.

Vagtplanssystemer

- EG Altiplan
- Altiplan Infoskærm
- Altiplan Medarbejder
- Altiplan Vikar
- EG Optima
- Optima Afløser
- Optima Aktivitet
- Optima Datahub
- Optima Integration
- Optima Medarbejder
- Optima Storskærm
- SD Tjenestetid

- SD MinTid
- SD Vagtplanoversigt.

For at sikre et tilstrækkeligt sikkerhedsniveau, uanset hvilken model en given applikation leveres i, anvender EG et fælles rammeværk for kontroller, som er beskrevet nærmere i dette dokument, med fokus på både applikationsudvikling og vedligeholdelse af applikationer og underliggende infrastruktur. Som en del af dette rammeværk er EG ansvarlig for at sikre implementering og drift af kontrolsystemer, der skal forebygge og opdage fejl, herunder bevidste fejl, for at overholde kontrakter og best practice.

EG anvender JN Data A/S, AWS og Redcentric som underleverandører, der er væsentlige for beskrivelsen og forståelsen af rapportens omfang. JN Data A/S, AWS og Redcentric leverer hosting-ydelser, herunder datacenter, hardware, lagring og backup (op til virtualiseringsplatformsniveau). De kontroller, som disse serviceudbydere anvender, er ikke omfattet af denne rapport. EG overvåger nøje det sikkerhedsniveau, som disse leverandører sikrer, og har for 2025 indhentet revisionsrapporter fra disse leverandører.

3.2. Beskrivelse af kontrolmiljøer

3.2.1. Informationssikkerhedspolitik (kontrolmål A)

EG har udarbejdet en overordnet cyber- og informationssikkerhedspolitik (herefter benævnt it-sikkerhedspolitik) med afsæt i sikkerhedsstandarder som ISO 27001 og CIS version 8.

Det overordnede sikkerhedsrammeværk i EG består af:

- Cyber- og informationssikkerhedspolitikken
- Koncernrelaterede politikker, procedurer og retningslinjer, der gælder for alle EG-selskaber
- Lokale sikkerhedsprocedurer og instrukser hos de enkelte forretningsenheder eller EG-selskaber.

EG Cyber&Information Security foretager en årlig gennemgang af it-sikkerhedspolitikken samt de tilhørende procedurer og retningslinjer – herunder at disse opfylder de eksterne forpligtelser, der er fastsat i lovgivningen og kontrakter/aftaler.

Politikkerne og aktiviteterne i cyber- og informationssikkerhedsstyringssystemet introducerer et sæt af ufravigelige sikkerhedskontroller, som skal implementeres i alle produkter og systemer, der drives i EG. Eventuelle undtagelser fra disse kontroller registreres som formelle risici og overvåges:

- Endpoint Detection & Response (EDR)-løsning med Managed Detection & Response (MDR)-tjeneste skal implementeres på alle EG-endpoints.
- Eksterne sårbarhedsscanninger skal udføres på alle internetvendte systemer.
- Interne sårbarhedsscanninger skal udføres regelmæssigt på al intern it-infrastruktur.
- Multifaktorgodkendelse (MFA) skal bruges overalt for al adgang til vores systemer.
- Sikre og testede sikkerhedskopier skal opretholdes for alle kritiske data og systemer.
- Cloud-miljøer skal følge godkendte sikkerhedsbaselines og overvåges løbende.

3.2.2. Organisering af informationssikkerhed (kontrolmål B)

Det overordnede ansvar for it-sikkerheden i EG og tilhørende selskaber ligger i it-sikkerhedsudvalget, (EG Security Committee), der behandler alle større relevante it-sikkerhedsspørgsmål af principiel karakter.

It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, divisionschefer, vice president for IT, CIO og CISO, samt leder af Group Legal & Compliance. 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. Sikkerhedshændelser og status bliver rapporteret til it-sik-

kerhedsudvalget, som beslutter sig for håndteringen af hændelsen. Medlemmer af it-sikkerhedsudvalget deltager ligesom alle øvrige medarbejdere løbende i relevant awareness-træning inden for it-sikkerhed. It-sikkerheden er effektueret igennem intern strategi, politikker, standarder, procedurer og guidelines.

Det operationelle ansvar for styring af cyber- og informationssikkerheden i EG er placeret hos det centrale cyber- og informationssikkerhedsteam ledet af chief information security officer (CISO). Dette team definerer sikkerhedspolitikker, krav og vejledning for hele EG-organisationen, koordinerer implementeringen af sikkerhedsforanstaltninger på tværs af organisationen samt driver centralt leverede sikkerhedsprocesser. Cyber- og informationssikkerhedsteamet er ansvarligt for at sikre, at EG-medarbejdere holdes opdateret med sikkerhedsreglerne.

Ansvaret for at følge sikkerhedspolitikker, krav og vejledning samt implementering af nødvendige sikkerhedsforanstaltninger ligger hos de organisatoriske enheder, der udvikler og vedligeholder EG-systemer: EG IT, CloudOps, DevOps og individuelle forretningsenheder. Disse enheder udpeger sikkerhedskoordinatorer, der fungerer som forbindelsesled til cyber- og informationssikkerhedsteamet og koordinerer sikkerhedsaktiviteter i deres enheder. De udpeger også lokale sikkerhedshændelseskoordinatorer, der er ansvarlige for håndtering af sikkerhedshændelser i disse enheder.

Alt EG-personale, herunder medarbejdere samt tredjeparter med adgang til EG-systemer, har et ansvar for at beskytte EG's information mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Derfor bliver alle medarbejdere gjort bekendt med sikkerhedshåndbogen og skal gennemføre de nødvendige sikkerhedstræninger eller opgaver. Afhængigt af rollen i organisationen bliver medarbejdere også informeret om specifikke sikkerhedspolitikker og procedurer.

EG har etableret og vedligeholder et cyber- og informationssikkerhedsstyringssystem (C&ISMS) med det formål at sikre et tilstrækkeligt højt sikkerhedsniveau, der er i overensstemmelse med relevante lovgivningsmæssige og andre eksterne krav. C&ISMS tager en risikobaseret tilgang til at sikre det tilstrækkelige sikkerhedsniveau. Sikkerhedsmål, sikkerhedsstrategi samt beslutninger om, hvilke sikkerhedsforanstaltninger der skal anvendes, tager hensyn til påvirkningen og sandsynligheden af de adresserede risici. Ydeevne og effektivitet af C&ISMS overvåges og evalueres, herunder effektiviteten af nøgleprocesser, status for handlinger for at opnå sikkerhedsmål eller risikobehandlingsplaner, effektiviteten af sikkerhedsforanstaltninger samt risikoniveauer og sikkerhedsniveauer. En kombination af foranstaltninger kan anvendes, såsom KPI-måling, revisioner, penetrationstests, sikkerhedsscanninger, risikovurderinger og ledelsesgennemgange. Alle identificerede afvigelser, svagheder og forbedringsmuligheder resulterer i udarbejdelse af handlingsplaner for løbende at forbedre C&ISMS' egnethed, tilstrækkelighed og effektivitet.

Medarbejdersikkerhed

HR-funktionen varetages af HR i EG Danmark 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 i og oplysning om informationssikkerhed igennem awareness-træning inden for it-sikkerhed, så niveauet er passende og relevant i forhold til medarbejderens arbejdsopgaver, ansvarsområde, roller 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, hvori medarbejderen forpligter sig til at overholde virksomhedens it-sikkerhedspolitik og løbende holde sig ajour med eventuelle ændringer. Alle retningslinjer og politikker er tilgængelig for medarbejderen på EG's intranet. EG orienterer medarbejderne skriftligt på EG's intranet ved opdateringer/ændringer af it-sikkerhedspolitikken.

Den enkelte medarbejder har ansvar for at overholde it-sikkerhedspolitikken, Sikkerhedshåndbogen, og de regler, der er relevante for den enkelte medarbejders arbejdsopgaver, samt for at rapportere eventuelle brud på it-sikkerheden eller mistanke herom til it-sikkerhedsfunktionen. EG har interne procedurer til håndtering af medarbejders overtrædelse af EG's sikkerhedsregler- og procedurer.

Styring af sikkerhedshændelser

Alle sikkerhedshændelser håndteres i overensstemmelse med den fastlagte Security Incident Management Policy og tilhørende procedurer. Hvis en medarbejder bliver opmærksom på en sikkerhedshændelse, skal vedkommende informere den udpegede security incident manager, som har ansvaret for at sikre en hurtig, effektiv og rettidig håndtering af informationssikkerhedshændelsen.

I tilfælde af en sikkerhedshændelse underrettes de berørte kunder så hurtigt som muligt, og der iværksættes tiltag for at sikre data og systemer. Hvis det er aftalt med kunden, udarbejdes en "root cause analysis"-rapport, for så vidt muligt at sikre at hændelsen ikke kan optræde igen.

Alle væsentlige sikkerhedshændelser rapporteres til ledelsen.

Eksterne parter og leverandørforhold

EG har formelle procedurer for indgåelse af aftaler og kontrakter med leverandører og konsulenter, der sikrer, at leverandøren lever op til de forpligtigelser og krav til sikkerhed, som EG er underlagt via kontrakter og lovgivning. Alle nye leverandører skal godkendes af et Vendor Approval Board, der foretager vurdering af leverandørens evne til at leve op til gældende sikkerheds- og compliance krav.

Aftaler vedligeholdes gennem en tæt dialog samt jævnlige møder med vores leverandører. Leverandøraftalerne optimeres jævnligt i forhold til vores situation og vores kunder.

3.2.3. Fysisk sikkerhed (kontrolmål C)

Der er etableret en sikker fysisk afgrænsning, som sikrer beskyttelse af områder med informationsbehandlingsudstyr samt lagringsmedier.

Sikring af kontorer, lokaler og faciliteter

Alle EG's bygninger er sikret efter anerkendt standard i meget høj sikringsklasse, som bruges på steder, hvor der håndteres store værdier eller følsomme person-/kundeoplysninger.

Både alarmsystemerne og adgangskontrolsystemerne er døgnovervågede af EG Facility og vagtens kontrolcentral.

Adgang til virksomhedens lokaler styres af adgangskort. Adgangsrettighederne afstemmes med HR-oplysningerne. Hvis en ansat eller en leverandør mister sit adgangskort, lukkes adgangen, så snart det kommer til vores kendskab, eller misbrug konstateres.

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.

Datacentre

Datacentre driftes af tredjeparter. EG har gennem indgåelse af kontrakter og aftaler sikret, at beskyttelse af datacentre lever op til ISO 27001-standarden, herunder er beskyttet mod interne og eksterne trusler (miljøkatastrofer og strømafbrydelser), og at der sker jævnligt vedligehold og test af sikkerheden. Adgang til serverrum kan kun gives til personer med autoriseret adgang godkendt af hosting-leverandøren eller af EG.

3.2.4. Styring af kommunikation og drift (kontrolmål D)

Driftsprocedurer

Der er etableret procedurer, der sikrer, at tilgængeligheden af systemer og data kan opretholdes, og driften kan fortsætte 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, monitorering, backup og beredskabsplaner.

Der foretages løbende patching af operativsystemet.

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.

Overvågning og logning

Effektiv monitorering af processer giver vigtige oplysninger til både proaktivt og reaktivt at kunne undgå events, der ellers ville have påvirket overholdelsen af den garanterede tilgængelighed af systemerne. Målet er at minimere den tid, det tager at genetablere normal drift. Derudover er et centralt sikkerhedsmål at identificere og reagere hurtigt på sikkerhedstrusler eller hændelser gennem løbende overvågning, hvilket sikrer, at systemers og datas integritet og tilgængelighed opretholdes.

For at imødekomme dette arbejder virksomheden med forebyggende monitorering og dertilhørende korrigerende handlinger. Ved denne metode sker der ingen eller minimal påvirkning af overholdelsen af den med kunderne aftalte tilgængelighed af systemerne.

Der, hvor det ikke er muligt at forudse events, benyttes detekterende monitorering med dertilhørende korrigerende handlinger.

EG bruger værktøjer til endpoint-detektion og -respons på alle servere og arbejdsstationer samt cloud-beskyttelsesværktøjer for løbende at overvåge enhver mistænkelig aktivitet og blokere angreb i realtid. Eksterne udbydere af administrerede detektions- og responstjenester overvåger EG's endpoints og cloud-arbejdsbelastninger kontinuerligt døgnet rundt, reagerer på advarsler og eskalerer problemer til relevante teams.

EG anvender et 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 som aftalt for applikationen.

EG anvender et security information management-system, der giver mulighed for logning. 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.

Vores kommunikation til kunder i forbindelse med drifts- og datasikkerhed sker efter den aftalte procedure med den enkelte kunde i henhold til kontrakten.

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

Funktionsadskillelse

Der er etableret politikker og procedurer til sikring af funktionsadskillelse, der bl.a. omfatter krav til, at ansvar for udvikling og opdateringer til produktionsmiljø er adskilt, og at udvikling og driftsaktiviteter er adskilt.

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.

Backupdata opbevares separat fra produktionsdata i overensstemmelse med principperne om funktionsadskillelse og isoleret på både netværks- og identitetslaget.

Kryptering

Der er udarbejdet politik og procedurer i forhold til sikring af relevant og nødvendig kryptering af data.

Der anvendes som udgangspunkt kryptering på ekstern kommunikation til og fra virksomheden og til og fra datacentre. Der anvendes enten IPsec VPN eller SSL/TLS.

Kryptering i hviletilstand anvendes på filsystem- eller databaseniveau, hvor dette er anmodet om og aftalt med kunderne.

Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.

TLS-kryptering i forbindelse med afsendelse af e-mails opfylder de gældende krav på området.

Backup og restore

EG sikrer, at backup og restore følger gældende EG-standard og er i overensstemmelse med indgået aftale med kunden. De detaljerede principper og procedurer for backup og restore fremgår af den enkelte aftale med kunden.

Sikkerhedskopier konfigureres til at opfylde målsætninger for gendannelsespunkter og gendannelsestid. Sikkerhedskopier krypteres, beskyttes mod manipulation gennem uforanderlighed eller isolering og testes regelmæssigt for at bekræfte, at de kan gendannes inden for den krævede gendannelsestid.

Fejlrettelser og support

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.

Incident management er forankret i EG's supportsystem, hvor det er muligt at åbne kontakt igennem den tilhørende kundeportal, via mail eller via callcenter. I supportsystemet bliver alle incidents registreret og prioriteret i henhold til de gældende retningslinjer.

Afrapportering til kunder sker kun der, hvor dette er inkluderet i aftalen med kunden.

3.2.5. Adgangsstyring (kontrolmål E)

For at styre adgangen til virksomhedens systemer, informationer og netværk er der etableret regler for tildeling, ændring og nedlæggelse af adgange og rettigheder til alle EG-systemer.

Der er indarbejdet adgangsstyring for håndtering og godkendelse af såvel interne som eksterne brugeradgange.

Medarbejderadgang til virksomhedens systemer udefra sker ved hjælp af multifaktorgodkendelse (MFA), hvor det er teknisk muligt. Kun medarbejdere med et arbejdsbetinget behov har adgang til systemer ud fra princip om rolle- og rettighedsstyring. Den tekniske administration af autorisationer til EG's interne systemer og data styres af EG IT.

Der foretages periodisk gennemgang af brugerrettigheder, og alle adgange skal godkendes af nærmeste leder for at sikre, at kun personer med et arbejdsbetinget behov har adgang til systemer. Proceduren sikrer, at brugere, der ikke længere har et arbejdsbetinget behov for adgang, slettes i forbindelse med gennemgangen.

Alle medarbejdere og eksterne brugeres adgange inddrages, når ansættelsesforholdet ophører.

3.2.6. Anskaffelse, udvikling og vedligeholdelse af styresystemer (kontrolmål F)

EG er ansvarlig for håndtering af sårbarheder og patches på systemer i datacentrene. Formålet er at sikre, at sårbarheder i systemerne identificeres og afhjælpes rettidigt, at patches installeres rettidigt, og at sikkerhedsopdateringer installeres på kritiske systemer. Dette gælder både systemer, der anvendes internt, og systemer, der anvendes af eksterne kunder (kundesystemer).

Eksterne sårbarhedsscanninger på alle internetvendte systemer og interne sårbarhedsscanninger på al intern it-infrastruktur udføres regelmæssigt. 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 sårbarheds- og patch management-politikken og efter anbefaling fra netværksproducenten. Tilsvarende opdateres eller erstattes netværksenheder, hvis ikke firmware eller hardware længere supporteres af netværksproducenten.

Standardpatching:

Såfremt der er undtagelser fra standardpatchniveau, bliver det valgte patchniveau beskrevet. Som udgangspunkt leveres der standardpatchning.

Forudsætningen er, at leverandøren kan vælge servicevindue til patching.

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

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.

- Alle sikkerhedsopdateringer. Disse installeres grundet sikkerheden hurtigst muligt.
- Alle update rollups til operativsystemet. Det anbefales, at disse opdateringer installeres, efter at de er blevet vurderet og testet.
- Alle servicepacks til operativsystemet. De har generelt gennemgående ændringer og forbedringer til systemerne og skal testes nøje i miljøet, før de installeres.

Proces for godkendelse af servicepacks

Løbende 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.

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

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.

Test af ændringer til operativsystemer og netværk godkendes før flytning til produktion.

Nødændringer af operativsystemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende.

3.2.7. Anskaffelse, udvikling og vedligeholdelse af applikationer (kontrolmål F)

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. Softwareudviklingslivscykluspolitikken (SDLC) definerer minimumskrav til livscyklussen for EG-produkter.

Sikkerhedskontroller implementeres i softwareudviklingslivscyklussen. Al kode og alle softwarekomponenter, der bruges i EG's applikationer, testes eller scannes med sikkerhedssoftware for at identificere og afhjælpe sårbarheder.

Ved større og mere grundlæggende features følges følgende proces:

- Eventuel markedsvalidering gennem inddragelse af kunder efter behov og ønske
- Prototypeudvikling og relevant involvering fra kunder i dette
- Udvikling og løbende release til alle eller enkelte kunder
- Overvågning af brugen og eventuel tilretning
- Release af feature til alle eller enkelte kunder
- Uddannelse af brugere gennem gennemarbejdet grænseflade og tilhørende artikler på supportsite
- Support til brugeren efterfølgende pr. telefon eller e-mail til supportsystem
- Løbende overvågning af brugen samt eventuelle tilretninger.

Øvrige opgaver, mindre rettelser, opdatering og fejlrettelser udføres løbende under hensyntagen til omfang, prioritering og generelt strategisk fokus.

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

3.2.8. Katastrofeberedskabsplan (Kontrolmål G)

EG har udarbejdet et sæt af krisehåndterings- og beredskabsplaner med det formål at sikre, at EG kan holde kritiske forretningsprocesser kørende i tilfælde af en katastrofesituation.

EG har udarbejdet en beredskabsplan, der beskriver katastrofeorganisationen med de ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instruks for de nødvendige indsatsgrupper.

Beredskabsplanerne for EG omfatter bl.a.:

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

Beredskabsplanerne opdateres og testes én gang årligt for at sikre, at de er tilstrækkelige og effektive.

3.3. Komplementære kontroller hos kunderne

Forudsætninger vedrørende kundernes ansvar er beskrevet i individuelle kontrakter. 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.

3.4. Forbedringer

I 2025 har EG taget følgende initiativer for at forbedre niveauet af sikkerhed og databeskyttelse:

Måned	Forbedring
November 2025	**I 2025 styrkede vi i EG vores position inden for cybersikkerhed og databeskyttelse gennem en række strategiske og operationelle initiativer.** • Vores governance-struktur blev forstærket via vores rammeværk for cyber- og informationssikkerhed, der sikrer overensstemmelse med gældende krav såsom CIS-kontroller, NIS2, AI Act og GDPR-krav. • Implementering af centrale tekniske og organisatoriske forbedringer, herunder: o Udvidelse af testning af applikationssikkerhed og kapaciteter til sårbarhedsstyring o Forbedret styring af cloud-sikkerhed o Udvidet asset management gennem integrationer med central CMDB o Yderligere forbedret tredjepartsrisikostyring via nye klassifikations- og vurderingskriterier samt interne værktøjer. **Infrastruktur- og applikationssikkerhed blev styrket** gennem skærpede databeskyttelses- og sikkerhedsstandarder, automatiseret scanning for sårbarheder og udvidet penetrationstestprogram for applikationer og infrastruktur. Databeskyttelsesforanstaltninger blev opdateret og forbedret med omfattende dataklassifikation, krypteringsstandarder og opdateret test af processer for hændelsesrapportering for at understøtte ny lovgivning såsom NIS2. EG har yderligere investeret i awareness-træning for at højne sikkerhedsbevidsthed for EG-medarbejdere og løbende compliance-overvågning for at indlejre en kultur af robusthed og regulatorisk parathed i hele organisationen. EG har implementeret og distribueret retningslinjer for generativ/agentisk AI og MCP-serverstyring, herunder godkendelsesflow og integrationsmønstre. EG har: • etableret formel arbejdsprocedure til at definere og styre sikker AI-adoption på tværs af produkter og interne processer • introduceret AI-assisterede værktøjer, der forbinder sårbarhedsdata med udvikleres workflows, og lanceret et AI-baseret trusselsmodelleringsværktøj for at accelerere ensartet dokumentation og risikovurderinger. **Endelig har EG revideret systembeskrivelserne i revisionserklæringerne** for at afspejle ny gældende lovgivning og indarbejde de relevante organisatoriske ændringer som følge af disse juridiske opdateringer.

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 operationelle effektivitet 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 den operationelle effektivitet 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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
A.1	**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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
B.1	**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 informations-sikkerheden er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at fortrolighedsaftaler, rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.	Ingen afvigelser noteret.
B.2	**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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
C.1	**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 en 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.	Ingen afvigelser noteret.
C.2	**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.	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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
	Der er udarbejdet en politik om, at skriveborde holdes ryddet for papir og flytbare lagringsmidler, samt at der skal være blank skærm på informationsbehandlingsfaciliteter.		
C.3	**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.	Ingen afvigelser noteret.
C.4	**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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
C.5	**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.	Ingen afvigelser noteret.

Kontrolmål D:

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
D.1	**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.	Ingen afvigelser noteret.
D.2	**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	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.	Ingen afvigelser noteret.

Kontrolmål D:

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
	gælder bl.a. udviklere, som har 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.		
D.3	**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.	Ingen afvigelser noteret.
D.4	**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.	Ingen afvigelser noteret.

Kontrolmål D:

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
		Vi har gennemgået proceduren for ekstern opbevaring af backupbånd, til bekræftelse af at backups opbevares på betryggende vis.	
D.5	**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.	Ingen afvigelser noteret.

Kontrolmål D:

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
D.6	**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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
E.1	**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.	Ingen afvigelser noteret.
E.2	**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 passwords, 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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
E.3	**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.	Ingen afvigelser noteret.
E.4	**Inddragelse af adgangsrettigheder** Der er implementeret en 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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
E.5	**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 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 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 ved inspektion konstateret, at netværket er segmenteret i mindre net ved hjælp af VLANs og DMZs for at reducere risikoen for uautoriseret adgang.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
E.6	**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.	Ingen afvigelser noteret.

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.

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
E.7	**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.	Ingen afvigelser noteret.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
F.1	**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 en 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.	Ingen afvigelser noteret.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
F.2	**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. 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 helpdesksystemet 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 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 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.	Vi har ved vores test konstateret, at der ikke er implementeret en tilstrækkeligt formaliseret procedure for ændringsstyring af infrastruktur, herunder en beskrivelse af processen, fastlagt ejerskab samt dokumenterede kriterier for klassifikation af ændringer som Standard Changes eller Normal Changes. Vi har dog observeret, at de testede Normal Changes er godkendt i overensstemmelse med det etablerede systemunderstøttede godkendelsesflow. Ingen yderligere afvigelser noteret.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
F.3	**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.	Ingen afvigelser noteret.
F.4	**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	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 ved vores test konstateret, at udviklingsopgaver ikke i alle tilfælde dokumenteres og godkendes i overensstemmelse med proceduren, herunder at code-review ikke er formaliseret tilstrækkeligt. Vi har dog observeret, at releases testes ud fra flere teststrategier, før de lægges i produktion. Ingen yderligere afvigelser noteret.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
	• 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.		

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
F.5	**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.	Ingen afvigelser noteret.

Kontrolmål G: Katastrofeplan

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

Nr.	EG's kontrolaktivitet	PwC's udførte testhandlinger	Resultat af PwC's tests
G.1	**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.	Ingen afvigelser noteret.

PENNEO

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

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

Rasmus Dalby Martinussen
Kunde
Serienummer: 090fee93-08c6-4523-bebf-64790bf8c6a1
IP: 185.128.xxx.xxx
2026-04-30 07:08:37 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-04-30 07:55:30 UTC

Mit ID