Revisorerklæring

IT Forum Gruppen A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller for perioden
1. januar 2023 til 31. december 2023 relateret til drift af hosting platform

April 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Indholdsfortegnelse

Sektion 1: IT Forum Gruppen A/S' udtalelse

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

IT Forum Gruppen A/S anvender serviceunderleverandørerne Interxion Danmark ApS og GlobalConnect A/S. Denne erklæring er udarbejdet efter partielmetoden, og IT Forum Gruppen A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Interxion Danmark ApS og GlobalConnect A/S. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i IT Forum Gruppen A/S' beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og er operationelt effektive sammen med kontrollerne hos IT Forum Gruppen A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

IT Forum Gruppen A/S bekræfter, at:

(a) Den medfølgende beskrivelse i Sektion 3, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for IT Forum Gruppen A/S' drift af hosting platform der har behandlet kunders transaktioner i perioden fra 1. januar 2023 til 31. december 2023. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været designet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller designet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes design har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 1. januar 2023 til 31. december 2023.

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

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af IT Forum Gruppen A/S' kontroller i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetencer og beføjelser i perioden fra 1. januar 2023 til 31. december 2023.

Århus, den 10. april 2024
IT Forum Gruppen A/S

Mikael Elling
CEO

Sektion 2: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres design og operationelle effektivitet

Til IT Forum Gruppen A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om IT Forum Gruppen A/S' beskrivelse i Sektion 3 af generelle it-kontroller for drift af brugersystemer til behandling af IT Forum Gruppen A/S' drift af hosting platform i perioden og om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IT Forum Gruppen A/S anvender serviceunderleverandøren Interxion Danmark ApS og GlobalConnect A/S. Denne erklæring er udarbejdet efter partielmetoden, og IT Forum Gruppen A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Interxion Danmark ApS og GlobalConnect A/S. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af IT Forum Gruppen A/S´ kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos IT Forum Gruppen A/S.

Enkelte af de kontrolmål, der er anført i IT Forum Gruppen A/S' beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt designet og operationelt effektive sammen med kontrollerne hos IT Forum Gruppen A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

IT Forum Gruppen A/S' ansvar

IT Forum Gruppen A/S er ansvarlig for udarbejdelsen af beskrivelsen i Sektion 3 og tilhørende udtalelse i Sektion 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 designet og implementeringen af operationelt effektive kontroller for at nå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton 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 IT Forum Gruppen A/S' beskrivelse (Sektion 3) og om designet og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at

beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet IT Forum Gruppen A/S' udtalelse i Sektion 1.

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

IT Forum Gruppen A/S' beskrivelse i Sektion 3 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 de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække 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 IT Forum Gruppen A/S' udtalelse i Sektion 1. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var designet og implementeret i perioden 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende

(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 1. januar 2023 til 31. december 2023, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis kunderne har designet og implementeret de komplementerende kontroller, der forudsættes i designet af IT Forum Gruppen A/S' kontroller i perioden fra 1. januar 2023 til 31. december 2023

(c) De testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har været operationelt effektive i perioden 1. januar 2023 til 31. december 2023

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i den efterfølgende Sektion 4 om kontrolmål, udførte kontroller, test og resultater heraf.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i Sektion 4 er udelukkende tiltænkt kunder, der har anvendt IT Forum Gruppen A/S' drift af hosting platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 10. april 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Director, CISA, CISM

Sektion 3: Beskrivelse af IT Forum Gruppen A/S' ydelser i forbindelse med drift af hosting platform samt generelle it-kontroller relateret hertil

I det følgende beskrives IT Forum Gruppen A/S' ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos IT Forum Gruppen A/S. Processer og systemopsætninger m.v., der er individuelt aftalt med IT Forum Gruppen A/S' kunder er ikke omfattet af erklæringen. Vurdering af eventuelle kundespecifikke processer og systemopsætninger m.v. vil fremgå af specifikke erklæringer til kunder, der har bestilt sådanne.

Kontroller i applikationssystemerne er ikke omfattet af denne erklæring.

Generelle it-kontroller hos IT Forum Gruppen A/S

Indledning
I det følgende beskrives de generelle it-kontroller relateret til IT Forum Gruppen A/S' ydelser til kunder, jf. beskrivelsen ovenfor i afsnit 1.1.

Anvendelse af underleverandører
IT Forum Gruppen A/S anvender flere væsentlige leverandører i forbindelse med leverancen af hosting platform.

Beskrivelse af generelle IT-kontroller i tilknytning til IT Hosting ydelser hos IT Forum Gruppen
Denne beskrivelse vedrører generelle IT-kontroller i tilknytning til ovenstående aktiviteter. IT Forum Gruppens arbejde i relation til de generelle IT-kontroller er tilrettelagt med udgangspunkt i Informationssikkerhedshåndbogen og aftale mellem IT Forum Gruppen og den enkelte kunde, som beskrevet i Hostingaftale ver. 3.1 med evt. tillægsaftale. Derudover har IT Forum Gruppen valgt, med udgangspunkt i ISO27002:2013, at implementere relevante sikringsforanstaltninger indenfor følgende områder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Adgangsstyring
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandører
- Styring af informationssikkerhedshændelser
- Beredskabsstyring

Områderne er udvalgt med udgangspunkt i de opgaver, IT Forum Gruppen har ansvaret for og varetager på vegne af kunder, og som er beskrevet i Hostingaftale ver. 3.1 eller Driftsaftale ver. 3.0 og evt. tillægsaftale samt Informationssikkerhedshåndbogen. De implementerede sikringsforanstaltninger hos IT Forum Gruppen fremgår af bilag 1 til denne beskrivelse.

Beskrivelsen dækker perioden 1. januar 2023 til 31. december 2023 og er udelukkende beregnet for IT Forum Gruppen, IT Forum Gruppens kunder og deres respektive revisorer.

IT Forum Gruppen varetager overordnet set følgende IT-opgaver for sine kunder:

- IT-driften af kundernes løsninger foregår fra et eller flere af IT Forum Gruppens driftscentre i Danmark
- Overvågning af IT-driften.
- Support af brugere hos kunderne, herunder diverse fejlretning.

Udstyret ejes af IT Forum Gruppen medmindre andet er aftalt.

IT Forum Gruppen er ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af de i aftalerne stillede krav.

Underleverandører
Denne erklæring er udarbejdet efter partielmetoden og omfatter således kun kontrolmål og tilknyttede kontroller hos IT Forum Gruppen, men ikke kontrolmål og kontroller hos vores underleverandører og deres underleverandører.

IT Forum Gruppens informationssikkerhedsstrategi
Direktionen og bestyrelsen har fastlagt IT Forum Gruppens ønskede niveau for informationssikkerhed. IT Forum Gruppen har fokus på at tilbyde IT-serviceydelser tilpasset kundernes nødvendige sikkerhedsniveau. Således arbejdes der efter den internationale informationssikkerhedsstandard "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements".

IT Forum Gruppen har valgt at implementere relevante sikkerhedsforanstaltninger fra "ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security management". Således er politikker udarbejdet efter strukturen og relevante sikkerhedsforanstaltninger fra standarden.

Direktionen giver bestyrelsen en årlig redegørelse om IT-sikkerhedsniveauet. Under redegørelsen tager bestyrelsen stilling til IT Forum Gruppens IT risikoprofil og IT sikkerhedsniveau med tilhørende relevante politikker.

IT Forum Gruppen får udført en uafhængig vurdering af Informationssikkerhedsniveauet og af effektiviteten af de implementerede sikkerhedsforanstaltninger. Denne vurdering udføres af en uafhængig godkendt og certificeret revisor specialiseret inden for IT revision og risikostyring. Vurderingen afsluttes med afgivelse af en udtalelse fra ledelsen, samt at den uafhængige revisor afgiver en erklæring. Denne erklæring er baseret på den internationale revisionsstandard ISAE 3402. Derudover afgives der en erklæring fra revisor til BFIH om IT Forum Gruppens overholdelse af BFIH certificeringskrav til Hostingcertifikatet (nu Cloudcertifikatet).

IT Forum Gruppen A/S' Informationssikkerhedshåndbog har til formål at:

- tilbyde et stabilt og sikkert driftsmiljø med et højt serviceniveau.
- IT Forum Gruppens medarbejdere kun har adgang til følsomme data, hvis der er brug for informationen ved arbejdets udførelse, eller hvis den pågældende medarbejder har fået tilladelse til at tilgå disse informationer af kunden.
- forhindre uvedkommende personer i at få adgang til IT-systemer, hvor der er adgang til følsomme data.
- system og data er beskyttet mod forsyningssvigt.
- system og data kan gendannes hurtigst muligt ved force majeure lignende situationer.

Informationssikkerhedshåndbog
Den nærværende informationssikkerhedshåndbogs områder og afsnit henfører til inddelingen og nummereringen i DS/ISO/IEC 27002. Ud fra en risiko- og cost-beneflt vurdering er ikke alle punkter og underpunkter nævnt.

Risikostyring

Vurdering af sikkerhedsrisici
En vurdering af sikkerhedsrisici er lavet ud fra det trusselsbillede der knytter sig til IT Forum Gruppens forretningsområde, IT drift/hosting. Her skal sikres, at kundens data er beskyttet tilstrækkeligt mod afbrydelser, datatab og uønsket adgang. Dette både fysisk (bygninger og forsyning) og teknisk (hardware og software), samt mod både interne og eksterne faktorer der forsætligt eller uforsætligt kan true IT-driften.

IT Forum Gruppen vil løbende, men mindst en gang i året og ved større systemændringer, vurdere sikkerhedsniveauet og prioritere nødvendige tiltag for at sikre den fortsat høje sikkerhed, så den overholder kundernes krav.

Der er lavet et beredskab der både retter sig mod mindre og større nedbrud, således at kunden hurtigst muligt kan få adgang til deres systemer i driftscentret.

Sammenhængen i Informationssikkerhedshåndbogen sikres gennem samarbejde mellem direktionen og den IT-infrastrukturansvarlige.

Risikohåndtering

Risikohåndteringen tager udgangspunkt i det stående trusselsbillede med opgørelse af konsekvenser og sandsynligheder for at hændelser indtræffer.

IT Forum Gruppen indbygger risikohåndtering i forretningsgange og processer i organisationen, så emnet behandles hvor og når det er relevant. Direktionen og den IT- infrastrukturansvarlige skal periodisk gennemføre overordnede risiko- og konsekvensvurderinger af bygning, teknik, applikationer, processer med mere.

Formålet er dels at sikre at det nødvendige sikkerhedsniveau justeres i takt med ændrede behov, og dels at holde sig de mest forretningskritiske systemer for øje.

Som led i risikohåndteringen har IT Forum Gruppen blandt andet beskrevet en lang række sikkerhedsforanstaltninger i informationssikkerhedshåndbogen, samt etableret en lang række foranstaltninger. Disse foranstaltninger skal være med til at sikre en stabil og sikker hostingdrift og –service overfor kunderne.

Der er således etableret:

- Køling af det primære hostingcenter og backupfacilitet. Dette indbefatter løbende temperaturmåling med alarmer
- Automatisk Inergen brandslukning, hvor der er indgået servicekontrakt med leverandør

Sikkerhedskopier opbevares på en sekundær lokation i Danmark.

Nødstrømsanlæg i tilfælde af længerevarende strømudfald. Nødstrømsanlægget består af UPS og dieselgenerator. Der er indgået serviceaftaler med leverandører for begge dele. Hostingcenteret har redundant datakommunikation, der således er redundante telekommunikationslinjer.

Organisering af informationssikkerhed

Kontrolmål: Der er etableret betryggende kontroller som sikrer initiering og kontrol af informationssikkerhed i virksomheden.

Opgaver og ansvar for informationssikkerhed er fastlagt for medarbejderne. Medarbejderne er gjort bekendt med informationssikkerhedshåndbogens krav og ansvar.

Medarbejderne er ansvarlige for at beskytte informationsaktiver samt at betjene det IT-udstyr, der stilles til rådighed ifølge de retningslinjer, regler og forskrifter der er nævnt i IT Forum Gruppens politikker.

Ved sikkerhedsbrud/trusler skal IT Forum Gruppens medarbejdere rette henvendelse til IT-driftsansvarlig.

Medarbejdersikkerhed

Kontrolmål: Der er etableret betryggende kontroller til sikring af, at alle medarbejdere er opmærksomme på deres særlige ansvar i forhold til virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, svindel og misbrug af informationsaktiver.

En ansøger efterprøves før en aftale indgås. Denne efterprøvning foregår efter gældende love og etik, og vurderes ud fra IT Forums krav til informationssikkerhed og de relevante risici.

Adgangsstyring

Kontrolmål: Der er etableret betryggende kontroller til sikring af, at adgang til systemer, data og netværk styres i overensstemmelse med forretningsmæssige og lovgivningsbetingede krav.

IT Forum har etableret retningslinjer for adgangsstyring, der fastlægger adgangsregler og –rettigheder for bruger eller grupper af brugere. Denne adgangsstyring omfatter både logisk og fysiske adgang, der tildeles ud fra et arbejdsbetinget behov.

Alle kunder, der skal have adgang til systemer på primær drift, skal have eksplicit definerede logins, der bliver valideret fra centralt hold. Ved login sker automatisk logning af brugeren.

IT Forums medarbejdere defineres centralt, hvorfra login til servere valideres. Ved login på en server, skal der føres audit/logning. Servere og andet centralt udstyr, hvor det ikke er muligt at overholde ovenstående, skal beskrivelse i driftsdokumentationen angive adgangskontrollen til systemet.

Alle brugere hos IT Forum tildeles en unik identitet til personlig brug. Medarbejdere skriver ved ansættelsen under på, at deres personlige koder er fortrolige og at eventuelle gruppeadgangskoder kun må kendes af ITF's ansatte.

Standardadgangskoder fra systemleverandører ændres efter installation af systemet.

I de tilfælde, hvor der er brug for udvidede adgangsrettigheder, tildeles det i det omfang det skønnes nødvendigt for udførelse af en given opgave. Efter endt opgave skal de udvidede adgangsrettigheder fratages igen.

Alle teknikere hos IT Forum har tilladelse til at administrere udvidede adgangsrettigheder ud fra devisen; Har du givet adgangsrettigheden, er du ansvarlig for at den ikke bliver misbrugt og du er også ansvarlig for at den bliver frataget igen. Hvis der tillades udvidede adgangsrettigheder over længere perioder (længere end til arbejdsdagens slutning), skal den driftsansvarlige adviseres skriftligt.

Adgangsrettigheder for ITF's ansatte gennemgås en gang om året og revurderes i forbindelse med ændringer i den ansattes arbejdsmæssige forhold. Godkendelser til udvidede adgangsrettigheder skal jævnligt gennemgås for at sikre at adgangsrettigheder modsvarer den enkeltes reelle behov.

I tilfælde af opsigelse vurderer medarbejderens leder medarbejderens rettigheder til informationssystemet og inddrager om nødvendigt disse. Medarbejderens datafiler og mails gennemgås snarest muligt og relevant indhold overdrages til andre medarbejdere. Logon proceduren skal minimere mulighederne for uautoriseret adgang ved at afsløre så lidt som muligt om systemet.

Fysisk sikring og miljøsikring

Kontrolmål: Der er etableret betryggende kontroller til sikring af,

- at væsentlige informationsaktiver er beskyttet mod uautoriseret fysisk adgang, fysisk skade og forstyrrelser
- at kritisk informationsbehandlingsudstyr og lagringsmedier huses i sikre områder beskyttet af nødvendige barrierer og adgangskontroller
- at undgå tab af, skader på, eller kompromittering af informationsaktiver
- at udstyr beskyttes mod fysiske trusler
- at nødvendige forsyninger af el og ventilation samt kabelinstallationer er tilstrækkelige.

Driftscenter på primær lokation har et fysisk sikringsniveau, der kan modstå civile sabotageforsøg; herunder uretmæssig indtrængen, tyveri, hærværk og lignende. Sikringen sker blandt andet ved afskærmede vinduer, dobbelte ståldøre og alarm. Ved indbrudsforsøg på primær drift reagerer alarmcentral straks og virksomhedens beredskab alarmeres. Adgang til primære driftscentre begrænses til virksomhedens godkendte driftsteknikere. Al adgang logges.

Eksterne konsulenter, håndværkere og rengøring tillades kun adgang ifølge med en godkendt driftstekniker. I perioder med længerevarende arbejde kan eksterne personer tildeles adgang uden eskorte af driftstekniker. Dette sker ved underskrivning af tillidsaftale.

Der tages ugentlig backup af kunders forretningskritiske data. Disse gemmes i krypteret form på sekundære driftscentre.

Kølesystem er redundant efter N+1 princippet så en vilkårlig komponent i et vilkårligt køleanlæg kan blive defekt uden at det har betydning for driften. Fancoils med blæser og køleveksler sikrer stabil temperatur i de enkelte celler i driftsområdet.

Brandsikring med beskyttelse fra både udefrakommende og indefrakommende brand. Farlige og brandbare materialer forefindes ikke i samme lokale som driftscentret. Brandsikre døre har automatisk lukning. Der er etableret automatisk, Inergen baseret brandslukning i driftsområdet.

Primære driftscentre forsynes med et nedgravet strømkabel, samt UPS-strømbackup der beskytter mod transienter og sikrer tilstrækkelig tid til nedlukning i tilfælde af strømsvigt. Nødstrømsanlægget testes en gang om året. Dieselgeneratoren startes op en gang i kvartalet.

Primære driftscentre har redundante telekommunikationsforbindelser der forlader bygningen to forskellige steder. Kabler i driftscentre er sikret mod udrivning og brud ved, at kabelføringen samles i kabelbakker og –skakte. Kabler i corenetværket mærkes med relevant information. Kabelgennemføringer i murværk og etageadskillelser er tilstoppet med brandhæmmende materiale. Netværksføring dokumenteres, der opdateres.

Hvor der er adgang til primære driftssystemer skal det sikres at skærm og tastatur låses automatisk efter 10 min inaktivitet eller at brugeren låser skærm og tastatur når brugeren forlader sin arbejdsplads.

Fysisk sikring og miljøsikring serviceunderleverandører

Denne erklæring er udarbejdet efter partielmetoden og omfatter således kun kontrolmål og tilknyttede kontroller hos IT Forum Gruppen, men ikke kontrolmål og kontroller hos vores underleverandører og deres underleverandører.

Driftssikkerhed

Kontrolmål: Der er etableret betryggende kontroller til sikring af, at systemer og data sikkerhedskopieres, at sikkerhedskopier opbevares betryggende og at sikkerhedskopier er læsbare.

Der foreligger driftsdokumentation, der sikrer at en vilkårlig driftstekniker er i stand til at løse problemer op til et totalt nedbrud. Drifts-dokumentationen opdateres ved ændringer. I fejlsituationer udpeges kontaktpersoner til at håndtere telefoni med kunder, mens driftsteknikere får udbedret fejlene.

Driftsvagt er døgnet rundt tilgængelig inden for de aftalte svartider.

Større ændringer i software og hardware skal planlægges og dokumenteres i en vis detaljeringsgrad med vurdering af ændringens konsekvenser. Dertil kommer dokumentation af nødprocedurer i tilfælde af fejlslagne ændringer. Hvis det vurderes nødvendigt skal ændringer testes før det sættes i produktion.

Kapacitet på servere og services måles og overvåges regelmæssigt for at sikre tilstrækkelig kapacitet. Alarmer aktiveres, når grænser for kapacitet overskrides.

Grundet IT Forums størrelse og driftscentrenes sammensætning er der etableret en systemteknisk adskillelse mellem de forskellige miljøer. Det tilstræbes at holde testmiljø og driftsmiljø så identiske som muligt. Alle enheder i testmiljøet er markeret med, eller indeholder ordet ”TEST”.

Servere er installeret med opdateret antivirus.

Der tages dagligt sikkerhedskopi af den grundlæggende IT infrastruktur. Sikkerhedskopien opbevares i krypteret form på sekundær lokation. For at kunne honorere kundens ønske om datasikkerhed og gendannelse af data i driftscentret, laves der daglig backup af både kundens forretningskritiske data samt backup af de servere som kunden har placeret i driftscentret. Backup gemmes som standard i minimum 7 versioner tilbage. Gendannelsesprocedurer afprøves regelmæssigt på sikkerhedskopier ved at indlæse udvalgte filer for kunder.

Brugeraktiviteter, afvigelser og sikkerhedshændelser logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug. Brugen af IT Forums primære driftssystemer overvåges og følges løbende op på. Niveauet for overvågning fastlægges ud fra en risikovurdering og lovgivningens krav. Fejl på primære driftssystemer logges og analyseres, og nødvendige udbedringer og modforholdsregler gennemføres. Log-faciliteter og log-oplysninger beskyttes mod manipulation. Aktiviteter udført af systemadministratorer og -operatører samt andre med særlige rettigheder logges.

Der er forretningsgange for installation af systemer i driftsmiljøer.

Kommunikationssikkerhed

Kontrolmål: Der er etableret betryggende kontroller til sikring af en korrekt og betryggende datakommunikation. Informationssikkerhedshåndbogen indeholder regler og procedurer for informationsudveksling for IT Forum.

Styring af underleverandører

Kontrolmål: Der er etableret betryggende kontroller som sikrer, at der er udfærdiget skriftlige samarbejdsaftaler med relevante leverandører

Aftaler om samarbejde med relevante leverandører indgås efter at ledelsen har foretaget en sikkerhedsmæssig vurdering.

IT Forum Gruppen er i tæt dialog med underleverandøren og modtager en ISAE 3402 erklæring eller tilsvarende erklæring fra underleverandøren.

Erklæringen er afgivet efter partielmetoden, således indgår relevante kontroller hos serviceunderleverandører ikke.

Styring af informationssikkerhedshændelser

Kontrolmål: Der er etableret betryggende kontroller til sikring af, at informationssikkerhedshændelser og svagheder i forbindelse med informationssikkerhedssystemer kommunikeres på en sådan måde, at korrigerende handling iværksættes rettidigt.

Al håndtering af sikkerhedsbrud, forbedringer og udbedringer koordineres af den driftsansvarlige. Denne vurderer det kritiske niveau og udstikker retningslinjer. Ansvaret påhviler den driftsansvarlige at vægte tiltag mod omkostninger. Sikkerhedshændelser og-svagheder rapporteres til den driftsansvarlige så snart som muligt på en kort og præcis måde. Den driftsansvarlige vurderer hændelsen og udstikker retningslinjer for udbedring.

Beredskabsstyring

Kontrolmål: Der er etableret betryggende kontroller til modvirkning af afbrydelser af forretningsaktiviteter og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer og at sikre rettidig retablering.

Kritiske elementer risikovurderes. Identificerede risici prioriteres, hvilket giver et situationsbillede af den nuværende sikkerhedsmodel. Det sammenfattes i et dokument med vurderinger om de områder, der skal fokuseres på. Der udarbejdes planer for vedligeholdelse og retablering af virksomhedens forretningsaktiviteter inden for den fastsatte tidsramme efter en afbrydelse af eller fejl i virksomhedens kritiske forretningsprocesser. Beredskabsplanerne afprøves mindst en gang årligt samt vedligeholdes og revurderes løbende. I forbindelse med afprøvningen laves en rapport der skal give et overblik over relevans og effektivitet for beredskabsplanen.

Væsentlige ændringer i generelle IT kontroller

Der har ikke i årets løb været væsentlige ændringer i de generelle IT kontroller for Hosting miljøet.

Komplementerende kontroller hos kunderne

Kunderne er ansvarlige for datatransmission mellem IT Forum Gruppen og kunden. Det er således kundernes ansvar at sikre kontroller herom.

Endvidere er al brugeradministration, herunder tildeling af rettigheder samt beskyttelse af tilgang via udstyr placeret på kundernes lokationer kundens ansvar. Kunderne skal således kontrollere al brugeradministration.

Anskaffelse, udvikling og implementering af forretningssystemer og brugersystemer er kundernes ansvar. Kontroller omkring systemudvikling, anskaffelse og ændringsstyring er kundernes ansvar.

Adgang til forretningssystemer og brugersystemer er kundernes ansvar. Kontroller omkring adgang til disse systemer og data herfor er kundernes ansvar.

Den enkelte kunde skal som dataansvarlig indgå en kontrakt med IT Forum Gruppen som databehandler, der skal sikre, at IT Forum Gruppen alene handler efter instruks fra den enkelte kunde, og at IT Forum Gruppen træffer alle nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger til behandling af persondata.

Sektion 4: Kontrolmål, udførte kontroller, test og resultater heraf

Formål og omfang

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi ved vores test har konstateret afvigelser i design, implementering eller operationel effektivitet af de testede kontroller, har vi anført disse under resultat af test.

Denne erklæring er udarbejdet efter partielmetoden og IT Forum Gruppen A/S' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos IT Forum Gruppen A/S' underleverandør Interxion Danmark ApS og GlobalConnect A/S.

Kontroller, som er specifikke for de enkelte kundeløsninger, eller som er udført af IT Forum Gruppen A/S' kunder, er ikke omfattet af vores erklæring.

Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos IT Forum Gruppen A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring 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 blive operationelt effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover foretages der stikprøvevis test af kontrollernes operationelle effektivitet i revisionsperioden.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af Grant Thornton som grundlag for vurdering af de generelle it-kontroller hos IT Forum Gruppen A/S.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed

Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.1.1	*Politikker for informationssikkerhed* Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er kommunikeret til medarbejdere.	Vi har inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen, og kommunikeret til medarbejderne. Vi har inspiceret, at informationssikkerhedspolitikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
5.1.2	*Gennemgang af politikker for informationssikkerhed* Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

A.6.1 Intern organisering
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
6.1.1	*Roller og ansvarsområder for informationssikkerhed* Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret et organisationsdiagram for informationssikkerhedsorganisationen. Vi har inspiceret beskrivelse af ansvarsområder i informationssikkerhedsorganisationen.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser
Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
6.2.1	*Politik for mobilt udstyr* Der er etableret en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.	Vi har inspiceret politik for mobilt udstyr. Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobilt udstyr.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen
Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
7.1.1	*Screening* Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.	Vi har inspiceret politik for screening af nye medarbejdere. Vi har stikprøvevis inspiceret dokumentation for, at der bliver indhentet screeningsdokumentation på nye medarbejdere i perioden.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring
Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
9.1.1	*Politik for adgangsstyring* En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret politikken for adgangsstyring. Vi har inspiceret at politikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.

A.9.2 Administration af brugeradgang Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
Nr.	***IT Forum Gruppen A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
9.2.2	*Tildeling af brugeradgang* Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har stikprøvevis inspiceret, at tildelte brugeradgange er blevet tildelt efter proceduren for adgangsstyring og kontrol.	Ingen afvigelser konstateret.
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder. Vi har inspiceret et udtræk af privilegerede brugere og vi har forespurgt om adgangsrettigheder er tildelt baseret på et arbejdsbetinget behov. Vi har inspiceret at privilegerede brugeradgange er personhenførbare. Vi har inspiceret, at der periodisk foretages gennemgang af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret proceduren for regelmæssig gennemgang og evaluering af adgangsrettigheder. Vi har inspiceret, at der foretages gennemgang og evaluering af adgangsrettigheder månedligt.	Ingen afvigelser konstateret.
9.2.6	*Inddragelse eller justering af adgangsrettigheder* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Vi har inspiceret politik for inddragelse og justering af adgangsrettigheder. Vi har stikprøvevis inspiceret at fratrådte medarbejdere har fået deres adgangsrettigheder inddraget rettidigt.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
11.1.1	*Fysisk perimetersikring* Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	Vi har inspiceret politikken for fysisk beskyttelse af faciliteter og perimetersikkerhed. Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til kontoret. Vi har inspiceret at der er opsat alarmsystemer til fysisk adgangskontrol.	Ingen afvigelser konstateret.
11.1.4	*Beskyttelse mod eksterne og miljømæssige trusler* Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret.	Vi har inspiceret proceduren vedrørende beskyttelse mod eksterne og miljømæssige trusler. Vi har inspiceret at der er implementeret sikkerhedsforanstaltninger til at forhindre trusler fra ild, varme og fugt og inspiceret relevante lokationer for at konstatere, om der er installeret brandslukningsudstyr, brand- og røgalarmer, blokering af vandførende rør, hævede gulve samt alarmer til test af fugt og vand m.v.	Ingen afvigelser konstateret.
11.1.5	*Arbejde i sikre områder* Procedurer for arbejde i sikre områder er tilrettelagt og etableret.	Vi har inspiceret politikken for arbejde i sikre områder.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
11.1.6	*Områder til af- og pålæsning* Adgangssteder som f.eks. områder til af- og pålæsning og andre steder, hvor uautoriserede personer kan komme ind på området, styres og adskilles så vidt muligt fra informationsbehandlingsfaciliteter for at undgå uautoriseret adgang.	Vi har inspiceret, at der skal anvendes adgangskort til områder til af- og pålæsning.	Ingen afvigelser konstateret.

A.11.2 Udstyr Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.			
Nr.	**IT Forum Gruppen A/S' kontrol**	**Grant Thorntons test**	**Resultat af test**
11.2.2	*Understøttende forsyninger (forsyningssikkerhed)* Udstyr skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	Vi har inspiceret backupstrøm, UPS-anlæg og dieselgeneratorer. Vi har inspiceret servicerapporter, der viser, at serviceinspektioner er udført og at udstyr testes regelmæssigt.	Ingen afvigelser konstateret.
11.2.3	*Sikring af kabler* Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, skal beskyttes mod indgreb, interferens og skader.	Vi har inspiceret, at der er udarbejdet en politik for sikring af kabler. Vi har inspiceret at der er gennemgang af faciliteter og anlægsenheder.	Ingen afvigelser konstateret.
11.2.8	*Brugerudstyr uden opsyn* Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har inspiceret politik for sikring af beskyttelse af udstyr, som er uden opsyn. Vi har inspiceret, at der er implementeret kontroller for brugerudstyr uden opsyn i form af automatisk screensaver.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

A.12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
12.1.1	*Dokumenterede driftsprocedurer* Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret.	Ingen afvigelser konstateret.
12.1.2	*Ændringsstyring* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret politikken vedrørende ændringer til informationsbehandlingsudstyr og – systemer. Vi har stikprøvevis inspiceret dokumentation for at implementerede ændringer er håndteret i overensstemmelse med politikken herfor.	Vi har inspiceret, at der i 14 ud af 25 stikprøver for ændringer ikke er klassificering indenfor 'større ændringer' eller 'mindre ændringer' i overensstemmelse med politikken. Ingen yderligere afvigelser konstateret.
12.1.3	*Kapacitetsstyring* Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.	Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav. Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.	Ingen afvigelser konstateret.
12.1.4	*Adskillelse af udviklings-, test- og driftsmiljøer* Udviklings-, test- og driftsmiljøer adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.	Vi har inspiceret netværksdiagram, hvoraf det fremgår at der er adskillelse af udviklings-, test- og driftsmiljøer. Vi har inspiceret teknisk dokumentation for at der er adskillelse af anvendte miljøer i systemer.	Ingen afvigelser konstateret.

A 12.2 Malwarebeskyttelse Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
Nr.	***IT Forum Gruppen A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.2.1	*Kontroller mod malware* Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har inspiceret retningslinjer for kontroller mod malware. Vi har inspiceret, at der er implementeret kontroller mod malware.	Ingen afvigelser konstateret.

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	***IT Forum Gruppen A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.3.1	*Backup af information* Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har inspiceret, at der er udarbejdet en politik for backup af data, som er gennemgået og opdateret i erklæringsperioden. Vi har stikprøvevis inspiceret, at der tages succesfuld backup i overensstemmelse med politikken. Vi har inspiceret, at der er foretaget gendannelsestest af backup data på periodisk basis.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	***IT Forum Gruppen A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.4.2	*Beskyttelse af log-oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har inspiceret politik for sikring af logoplysninger. Vi har inspiceret at logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	*Administrator- og operatørlog* Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.	Vi har inspiceret politikken vedrørende logning af aktiviteter udført af systemadministratorer og -operatører. Vi har stikprøvevis inspiceret at systemadministratorers og operatørers handlinger logges på servere og databasesystemer.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	***IT Forum Gruppen A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret politik for patching og opgradering af systemer og at den er gennemgået og opdateret i perioden. Vi har inspiceret dokumentation for at relevante systemer er opdateret og patchet efter bestemte krav i politikken herfor.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

A.13.1 Styring af netværkssikkerhed
Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
13.1.1	*Netværksstyring* Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls, intrusion detection og andre relevante sikkerhedsforanstaltninger. Vi har inspiceret at der er opdateret firmware på SAN maskiner på udvalgte lokationer. Vi har inspiceret dokumentation for design af netværket.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

15.2 Styring af leverandørydelser
Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
15.2.1	*Overvågning og gennemgang af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører i perioden.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har inspiceret proceduren for håndtering af sikkerheds-hændelser. Vi har inspiceret at proceduren er gennemgået og opdateret i perioden.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedshændelser. Vi har stikprøvevis inspiceret, at informationssikkerhedshæn-delser er rapporteret ad passende ledelseskanaler.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger orga-nisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observe-rede svagheder eller mistanke om svagheder i in-formationssystemer og -tjenester.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedssvagheder. Vi har stikprøvevis inspiceret, at medarbejdere har rapporte-ret svagheder eller mistanke om svagheder i informationssy-stemer og -tjenester.	Ingen afvigelser konstateret.

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

A.17.1 Informationssikkerhedskontinuitet
Kontrolmål: At sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	Vi har inspiceret at beredskabsplanen er udarbejdet ud fra et scenarie.	Vi har inspiceret, at der foreligger en beredskabsplan, men at denne kun er udarbejdet efter ét enkelt scenarie af kritiske situationer. Vi har dog inspiceret, at der er påbegyndt arbejde på en beredskabsplan som dækker flere kritiske situationer med forventet implementering i 2024. Ingen yderligere afvigelser konstateret.
17.1.2	*Implementering af informationssikkerhedskontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har inspiceret at beredskabsplanen vedligeholdes og opdateres efter behov.	Ingen afvigelser konstateret.
17.1.3	*Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har inspiceret dokumentation for at der er udført tests af beredskabsplanens enkelte scenarier.	Ingen afvigelser konstateret.

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."

Mikael Elling
Underskriver 1
Serienummer: c3427568-ee5d-430b-8da2-80dac2bcdbb7
IP: 212.130.xxx.xxx
2024-04-11 08:44:51 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2024-04-11 10:19:03 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2024-04-11 12:57:27 UTC