Penneo dokumentnøgle: ZH0LC-E3V3D-JODLA-7NY3A-5EPS6-2GOM9

Revisorerklæring

IT Forum Gruppen A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller relateret til
drift af hosting platform i perioden fra 1. januar 2024 til 31. december 2024

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

April 2025

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' ydelser i forbindelse med drift af hosting platform samt generelle it-kontroller relateret hertil, 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.

IT Forum Gruppen A/S anvender underleverandørerne GlobalConnect A/S og Digital Realty Trust Inc. Denne erklæring er udarbejdet efter partielmetoden, og IT Forum Gruppen A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandørerne. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og 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 hensigtsmæssigt designet og er operationelt effektive sammen med kontrollerne hos IT Forum Gruppen A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og implementeringen 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 i perioden fra 1. januar 2024 til 31. december 2024.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet 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 udformet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes udformning 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.
- Ydelser udført af underleverandører, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.
- 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 2024 til 31. december 2024.

(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 2024 til 31. december 2024, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunderne har udført de komplementerende kontroller, som forudsættes i designet af IT Forum Gruppen A/S' kontroller i perioden fra 1. januar 2024 til 31. december 2024.

Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar 2024 til 31. december 2024.

Aarhus, den 10. april 2025
IT Forum Gruppen A/S

Mikael Elling
Administrerende direktør

Sektion 2: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

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 fra 1. januar 2024 til 31. december 2024 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 underleverandørerne GlobalConnect A/S og Digital Realty Trust Inc. Denne erklæring er udarbejdet efter partielmetoden, og IT Forum Gruppen A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandørerne. 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 udformningen, implementeringen og effektivt fungerende 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 udformningen 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 og udformningen 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 implementeringen 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 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 systemet, 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.

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:

a) at beskrivelsen af de generelle it-kontroller i relation til IT Forum Gruppen A/S' drift af hosting platform, således som de var designet og implementeret i perioden fra 1. januar 2024 til 31. december 2024, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret i perioden fra 1. januar 2024 til 31. december 2024, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra 1. januar 2024 til 31. december 2024.

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, som kunderne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber.

København, 10. april 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Partner, 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

Fra 1. januar 2024 til 31. december 2024 har virksomheden leveret serviceydelser i overensstemmelse med de systemer til styring af informationssikkerhed, der er dokumenteret i denne erklæring, og i overensstemmelse med ISO/IEC 27001:2022, hvilket understøtter en systematisk tilgang til risikostyring, databeskyttelse og compliance.

Introduktion

I det følgende afsnit 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.

IT Forum Gruppen A/S' ydelser
IT Forum Gruppen A/S leverer drift- og hostingydelser til kunder med høje krav til sikkerhed, stabilitet og compliance. Virksomheden administrerer, overvåger og vedligeholder hostingplatformen, herunder netværk, servere og systemer, med et stærkt fokus på informationssikkerhed, dataintegritet og tilgængelighed.

IT Forum Gruppen A/S' informationssikkerhedsstrategi
IT Forum Gruppen A/S har fastlagt en struktureret og ambitiøs tilgang til informationssikkerhed, der sikrer, at virksomhedens IT-serviceydelser lever op til de højeste standarder for sikkerhed og compliance. Direktionen og bestyrelsen prioriterer løbende sikkerhedsniveauet, og holder sig opdateret på de nyeste regulatoriske standarder.

IT Forum Gruppens transformation og sikkerhedsudvikling
For at styrke sin sikkerhedsstrategi har IT Forum Gruppen A/S det seneste år gennemgået en omfattende transformation og implementeret et sæt af sikkerhedspolitikker, der dækker samtlige kontrolmål og strategiske sikkerhedstiltag. Disse politikker har erstattet den tidligere informationssikkerhedshåndbog og sikrer en mere fleksibel og dynamisk styring af informationssikkerhed. Samtidig har virksomheden overgået til ISO/IEC 27001:2022, hvilket har medført:

- en forbedret kontrolstruktur, der sikrer en mere effektiv risikostyring og trusselsrespons
- en proaktiv tilgang til cybersikkerhed og compliance, hvor sikkerhed er en integreret del af driften
- en øget modenhed i sikkerhedsarbejdet, hvor kontroller og processer er blevet styrket.

Nøgleforbedringer siden sidste år
Siden sidste års erklæring har IT Forum Gruppen A/S gennemgået en markant sikkerhedsmæssig transformation, hvilket har resulteret i følgende forbedringer:

- Implementering af et ISMS (Information Security Management System) softwareværktøj, der centraliserer dokumentation, håndtering af kontroller og sikkerhedsprocesser. ISMS-systemet sikrer en struktureret og automatiseret tilgang til compliance, hvor alle sikkerhedskontroller, politikker og risikovurderinger dokumenteres og vedligeholdes i realtid.
- Overgang fra ISO/IEC 27001:2013 til ISO/IEC 27001:2022, hvilket sikrer en mere tidssvarende og omfattende kontrolstruktur.
- Udvidelse af IT-kontrollerne, der styrker den generelle governancestruktur, driftssikkerhed, adgangsstyring og hændelseshåndtering.
- Forbedret risikovurdering og compliancestruktur, der sikrer en mere dynamisk tilgang til trusselsbilledet.

Denne transformation understøtter IT Forum Gruppen A/S' ambition om at levere en sikker, effektiv og compliant IT-drift, der matcher de stigende krav fra både kunder og regulatoriske myndigheder.

Ledelsens ansvar og revision
IT Forum Gruppens bestyrelse modtager årligt en strategisk redegørelse om virksomhedens IT-sikkerhedsniveau, herunder en gennemgang af risikoprofil, sikkerhedspolitikker og compliancestatus. Dette sikrer, at ledelsen har et opdateret grundlag for beslutningstagning.

For at understøtte en kontinuerlig forbedring af sikkerhedsforanstaltninger gennemføres der løbende uafhængige vurderinger af sikkerhedsniveauet samt en evaluering af effektiviteten af de implementerede kontroller.

Disse vurderinger udføres af en certificeret IT-revisor med specialisering i IT-revision og risikostyring, som sikrer, at IT Forum Gruppens sikkerhedsforanstaltninger overholder gældende standarder og regulatoriske krav.

Som en del af virksomhedens complianceramme får IT Forum Gruppen A/S årligt en ISAE 3402-erklæring, der dokumenterer virksomhedens informationssikkerhed, herunder kontrolmiljø, sikkerhedsforanstaltninger og driftssikkerhed, hvilket styrker kunderne transparens og tillid til de leverede ydelser.

Generelle IT-kontroller hos IT Forum Gruppen A/S

I det følgende beskrives de generelle IT-kontroller, der understøtter IT Forum Gruppen A/S' ydelser til kunder, jf. afsnit 1.1.

IT-kontroller i tilknytning til IT-hostingydelser
IT Forum Gruppen A/S har implementeret ISO/IEC 27001:2022 som grundlag for sine informationssikkerhedskontroller. Den nye standard introducerer forbedret risikostyring, øget modstandsdygtighed og en moderniseret tilgang til cybersikkerhed og compliance, hvilket sikrer en struktureret og effektiv styring af IT-risici.

Beskrivelsen dækker perioden 1. januar 2024 til 31. december 2024 og er udelukkende beregnet for IT Forum Gruppen A/S, virksomhedens kunder og deres respektive revisorer

De væsentligste sikkerhedsforanstaltninger omfatter:

- Sikkerhedspolitikker - Regelmæssig opdatering og revision af sikkerhedspolitikker baseret på risikobaseret tilgang.
- Organisering af informationssikkerhed – Tydeligere roller, ansvar og ledelsesinvolvering.
- Medarbejdersikkerhed – Stærkere procedurer for sikkerhedsgodkendelse af ansatte og øget awarenesstræning.
- Adgangsstyring – Implementering af Zero Trust-principper, strammere adgangskontrol og multifaktorautentificering (MFA).
- Fysisk sikring og miljøsikring – Forbedret sikring af datacentre.
- Driftssikkerhed – Forstærket monitorering og dokumenteret hændelseshåndtering.
- Kommunikationssikkerhed – Krypterede forbindelser, sikre transmissionsprotokoller og avanceret netværksovervågning.
- Styring af informationssikkerhedshændelser – Struktureret hændelseshåndtering og automatiserede alarmsystemer.
- Beredskabsstyring og kontinuitet – Regelmæssig test af beredskabsplan og nødprocedurer.

IT Forum Gruppen A/S varetager en række kerneopgaver for sine kunder, herunder:

- IT-driften af kundernes løsninger foregår fra et eller flere af IT Forum Gruppen A/S' driftscentre i Danmark.
- Overvågning af IT-driften.
- Brugerunderstøttelse og support, herunder fejlfinding og hændelseshåndtering.

Udstyret ejes af IT Forum Gruppen A/S medmindre andet er aftalt.

IT Forum Gruppen A/S er ansvarlig for at implementere og opretholde de nødvendige sikkerhedsforanstaltninger med henblik på at forebygge og opdage fejl samt sikre overholdelse af de krav, der er fastsat i kundeaftalerne.

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.

Risikostyring

IT Forum Gruppen A/S foretager vurderinger af sikkerhedsrisici med udgangspunkt i det aktuelle trusselsbillede relateret til virksomhedens forretningsområde – drift og hosting af IT-løsninger.

Formålet er at sikre, at kundedata er tilstrækkeligt beskyttet mod afbrydelser, datatab og uautoriseret adgang – både fysisk (bygninger og forsyningsforhold) og teknisk (hardware og software) – samt mod interne og eksterne trusler, uanset om disse er forsætlige eller utilsigtede.

Virksomheden vurderer løbende sikkerhedsniveauet – minimum én gang årligt og i forbindelse med større systemændringer – og prioriterer nødvendige tiltag for at opretholde et højt og tidssvarende sikkerhedsniveau, i overensstemmelse med kundernes krav og forventninger.

Der er etableret beredskabsforanstaltninger, som dækker både mindre og større driftsforstyrrelser, med henblik på hurtigst muligt at genetablere kundernes adgang til deres systemer i driftscentret.

Sammenhængen mellem den overordnede informationssikkerhedsstrategi og de tilknyttede sikkerhedspolitikker sikres i tæt samarbejde mellem direktionen og den IT-infrastrukturansvarlige.

Risikohåndtering

IT Forum Gruppen A/S har integreret risikohåndtering i virksomhedens sikkerhedspolitikker og forretningsprocesser, således at identificering og håndtering af risici er en naturlig del af den daglige drift.

Direktionen og den IT-infrastrukturansvarlige gennemfører regelmæssigt overordnede risiko- og konsekvensvurderinger, der omfatter bygninger, teknisk infrastruktur, applikationer, forretningsprocesser og andre kritiske elementer.

Formålet er at sikre, at sikkerhedsniveauet løbende tilpasses ændrede forretningsbehov og trusselsbilledet – og samtidig bevare et skarpt fokus på virksomhedens mest forretningskritiske systemer.

Som en del af risikohåndteringen har IT Forum Gruppen A/S defineret og implementeret en række sikkerhedsforanstaltninger, der understøtter en stabil og sikker IT- og hostingdrift over for kunderne.

Organisering af informationssikkerhed

IT Forum Gruppen A/S har etableret klare roller og ansvarsfordelinger for informationssikkerhed, hvilket sikrer en struktureret initiering, styring og kontrol af sikkerhedsprocesser i virksomheden. Disse kontroller understøtter en effektiv governancestruktur, hvor ansvaret for informationssikkerhed er tydeligt defineret, fordelt og overvåget for at sikre overholdelse af gældende standarder og regulatoriske krav.

Ansvaret for informationssikkerhed er forankret i ledelsen og understøttes af et opdateret sæt sikkerhedspolitikker, som giver alle medarbejdere klare retningslinjer for adfærd og ansvar. Politikkerne er udarbejdet i overensstemmelse med ISO/IEC 27001:2022 og revideres løbende.

Alle medarbejdere er ansvarlige for at beskytte informationsaktiver og overholde sikkerhedspolitikkerne, som er opdateret i henhold til ISO/IEC 27001:2022.

Alle medarbejdere er forpligtede til at beskytte virksomhedens informationsaktiver og efterleve gældende sikkerhedspolitikker. Ved konstaterede sikkerhedsbrud eller identificerede trusler har medarbejderne pligt til straks at eskalere hændelsen. Alle hændelser dokumenteres, vurderes og håndteres i henhold til de etablerede hændelseshåndteringsprocesser.

Medarbejdersikkerhed

IT Forum Gruppen A/S har implementeret strukturerede kontroller, der sikrer, at alle medarbejdere er bevidste om deres ansvar for informationssikkerhed og handler i overensstemmelse med virksomhedens sikkerhedspolitikker. Dette reducerer risikoen for menneskelige fejl, svindel og misbrug af informationsaktiver.

Som led i sikkerhedsforankringen gennemføres en grundig baggrundsvurdering af alle kandidater inden ansættelse. Denne vurdering foretages i overensstemmelse med gældende lovgivning og etiske standarder og tilpasses IT Forum Gruppen A/S' sikkerhedsniveau og risikoprofil.

Derudover gennemgår medarbejdere løbende sikkerhedstræning, herunder årlige awareness-sessioner, for at sikre, at de er opdaterede på de nyeste trusler, risici og sikkerhedsprocedurer.

Adgangsstyring

IT Forum Gruppen A/S har etableret betryggende kontroller til sikring af, at adgang til systemer, data og netværk styres i overensstemmelse med forretningsmæssige og lovgivningsbetingede krav. Kontrollerne er designet til at beskytte virksomhedens IT-miljø mod uautoriseret adgang og potentielle sikkerhedsrisici.

IT Forum Gruppen A/S 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 Forum Gruppen A/S' 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 Gruppen A/S 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 virksomhedens ansatte.

Standard adgangskoder 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.

Hvis der tillades udvidede adgangsrettigheder over længere perioder (længere end til arbejdsdagens slutning), skal den driftsansvarlige adviseres skriftligt.

Adgangsrettigheder for virksomhedens 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 indrager 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

IT Forum Gruppen A/S har implementeret robuste kontroller for at sikre, at væsentlige informationsaktiver er beskyttet mod fysiske trusler, uautoriseret adgang og miljømæssige risici. Der er etableret betryggende kontroller til sikring af,

- Kritiske informationsaktiver er beskyttet mod uautoriseret fysisk adgang, skader og forstyrrelser.
- Informationsbehandlingsudstyr og lagringsmedier opbevares i sikre områder med nødvendige barrierer og adgangskontrol.
- Risikoen for tab, skader eller kompromittering af informationsaktiver minimeres gennem strenge sikkerhedsforanstaltninger.
- Udstyr beskyttes effektivt mod fysiske trusler, herunder tyveri, sabotage og miljømæssige påvirkninger.
- Strømforsyning, ventilation og kabelinstallationer er tilstrækkelige og sikret mod driftsforstyrrelser.

Fysisk sikkerhed i driftscentre
IT Forum Gruppen A/S' primære driftscentre har et højt sikringsniveau, der kan modstå civile sabotageforsøg, uretmæssig indtrængen, tyveri og hærværk. Herunder:

- Bygningsmæssige sikringsforanstaltninger der omfatter afskærmede vinduer, dobbelte ståldøre og alarmsystemer.
- I tilfælde af indbrud aktiveres alarmcentralen øjeblikkeligt, og virksomhedens beredskabsprocedure iværksættes.
- Adgang til primære driftscentre er begrænset til godkendte driftsteknikere, og al fysisk adgang logges for sporbarhed.

Eksterne konsulenter, håndværkere og rengøringspersonale må kun få adgang i følgeskab med en godkendt driftstekniker. Ved længerevarende arbejde kan eksterne personer få midlertidig adgang, forudsat at de har underskrevet en tillidsaftale.

Databeskyttelse og redundans

- Kundernes forretningskritiske data sikkerhedskopieres minimum dagligt og opbevares i krypteret form på sekundære driftscentre for at sikre gendannelsesmuligheder.
- Kølesystemer er redundante efter N+1-princippet, hvilket betyder, at en vilkårlig komponent kan svigte uden at påvirke driften. Fancoils med blæsere og køleveksler sikrer en stabil temperatur i driftsområdet.
- Brandsikring beskytter både mod interne og eksterne brande - Der opbevares ingen farlige eller brandbare materialer i samme lokaler som driftscentrene. Automatiske brandsikre døre sikrer inddæmning ved brand. Der er installeret et Inergen-baseret automatisk brandslukningssystem i driftsområdet.

Strømforsyning og netværkssikring

- Primære driftscentre er tilsluttet et nedgravet strømkabel, som sikrer en stabil forsyning.
- Der er UPS-strømbackup, der beskytter mod transienter og sikrer tilstrækkelig tid til nedlukning i tilfælde af strømsvigt.
- Nødstrømsanlæg testes årligt, og dieselgeneratoren startes op kvartalsvist for at sikre driftsberedskab.

Driftscentrene har desuden redundante telekommunikationsforbindelser, der forlader bygningen via forskellige indgange for at sikre fortsat tilgængelighed i tilfælde af udfald.

Kabelsikring og arbejdsstationer

- Kabler i driftscentre er beskyttet mod udrivning og brud via kabelbakker og -skakte.
- Kabler i corenetværket mærkes med relevant information, og gennemføringer i murværk og etageadskillelser er brandsikret med brandhæmmende materiale.
- Dokumentationen for netværksføringer opdateres løbende for at sikre overblik og vedligeholdelse.
- Arbejdsstationer og systemer i primære driftssystemer er konfigureret til automatisk at låse skærm og tastatur efter 15 minutters inaktivitet eller manuelt ved forladelse af arbejdspladsen.

Denne omfattende fysiske sikring og miljøsikring sikrer, at IT Forum Gruppen A/S' infrastruktur forbliver modstandsdygtig, stabil og sikker i alle scenarier.

Fysisk sikring og miljøsikring serviceunderleverandører

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

Driftssikkerhed

IT Forum Gruppen A/S har etableret betryggende kontroller til sikring af, at systemer og data sikkerhedskopieres korrekt og kan gendannes.

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

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.

Systemteknisk adskillelse mellem miljøer etableres, når det vurderes nødvendigt i konkrete kundesager. Hvor en sådan adskillelse er implementeret, vil alle relevante enheder være markeret. Det er kun udpeget medarbejdere der har adgang til dette miljø. Denne adskillelse anvendes ligeledes i udviklingssammenhænge for at sikre klar differentiering mellem test- og produktionsmiljøer.

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 28 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

IT Forum Gruppen A/S har etableret betryggende kontroller til sikring af en korrekt og betryggende datakommunikation mellem virksomhedens systemer, kunder og samarbejdspartnere. Der er beskrevet retningslinjer og procedurer for at beskytte informationsudveksling og kommunikation mod trusler og uautoriseret adgang.

Virksomhedens netværk er struktureret og segmenteret, så interne og eksterne systemer adskilles for at minimere risikoen for kompromittering. Netværkstrafik overvåges kontinuerligt, og avancerede sikkerhedsløsninger, herunder firewalls, Intrusion Prevention Systems (IPS) og webfiltrering, sikrer, at al dataudveksling kontrolleres og beskyttes.

IT Forum Gruppen A/S benytter kryptering og sikre kommunikationsprotokoller for at beskytte data under overførsel. Kritiske netværk og trådløse forbindelser er sikret gennem adgangskontrol og overvågning, mens eksterne netværksgrænseflader er konfigureret til at afvise al ukendt trafik som standard.

Samarbejdet med tredjepartsleverandører understøttes af kontraktuelle sikkerhedskrav, herunder krav om overholdelse af relevante standarder og certificeringer som ISAE 3402. IT-Security teamet har ansvar for at sikre, at netværksarkitekturen løbende evalueres og optimeres i overensstemmelse med bedste praksis og virksomhedens risikovurderinger.

Gennem denne proaktive tilgang til kommunikationssikkerhed sikrer IT Forum Gruppen A/S en robust og skalerbar netværksinfrastruktur, der beskytter forretningskritiske systemer og data mod moderne sikkerhedstrusler.

Styring af underleverandører

IT Forum Gruppen A/S har 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 ISAE3402-erklæring eller tilsvarende erklæring fra underleverandøren.

Styring af informationssikkerhedshændelser

IT Forum Gruppen A/S har etableret en struktureret og dokumenteret proces for håndtering af informationssikkerhedshændelser, der sikrer rettidig identifikation, rapportering og udbedring. Formålet er at minimere risici, reducere konsekvenserne af sikkerhedsbrud og kontinuerligt forbedre virksomhedens sikkerhedsforanstaltninger.

Virksomheden har en dedikeret politik og interne retningslinjer, der fastlægger procedurer for opfølgning på IT-sikkerhedshændelser. Disse hændelser registreres og dokumenteres i relevante systemer, hvor de følges op og evalueres for at sikre en struktureret og transparent håndtering.

Hændelser håndteres af den driftsansvarlige i samarbejde med IT-Security teamet, hvor der foretages en vurdering af hændelsens alvorlighed. Nødvendige korrigerende handlinger iværksættes straks, og der udarbejdes retningslinjer for forebyggende tiltag.

Efter håndtering evalueres hændelsen, hvor erfaringer dokumenteres, og forbedringer af processer og kontroller implementeres for at reducere sandsynligheden for gentagelse.

Denne systematiske tilgang til sikkerhedshændelser sikrer, at IT Forum Gruppen A/S kan reagere hurtigt og effektivt på trusler, samtidig med at der sikres kontinuerlig forbedring af informationssikkerheden.

Beredskabsstyring

IT Forum Gruppen A/S har etableret strukturerede og veldefinerede kontroller, der sikrer fortsat drift og hurtig genopretning i tilfælde af systemnedbrud eller katastrofer. Formålet er at minimere forretningsforstyrrelser, beskytte kritiske processer og sikre en rettidig retablering af virksomhedens operationer.

Som en del af virksomhedens forretningskontinuitetsstrategi gennemføres løbende risikovurderinger af kritiske systemer og processer. Identificerede risici prioriteres og dokumenteres, hvilket giver et dynamisk overblik over virksomhedens sikkerhedsmodel og mulige sårbarheder.

For at sikre en hurtig og effektiv genoprettelse er der udarbejdet beredskabs- og retableringsplaner, som fastsætter procedurer for vedligeholdelse og genoprettelse af drift inden for en defineret tidsramme efter en afbrydelse.

Disse planer afprøves mindst én gang årligt, hvor der foretages en evaluering af relevans og effektivitet. Resultaterne dokumenteres i en evalueringsrapport, der danner grundlag for eventuelle forbedringer og optimeringer af beredskabsstrategien.

Denne systematiske tilgang til beredskabsstyring sikrer, at IT Forum Gruppen A/S kan reagere hurtigt og effektivt på hændelser, samtidig med at virksomhedens kritiske funktioner opretholdes og forbliver beskyttede mod større forstyrrelser.

Væsentlige ændringer i generelle IT-kontroller

Der har ikke i årets løb været væsentlige ændringer i de generelle it-kontroller.

Komplementerende kontroller hos kunderne

Kunderne er ansvarlige for datatransmission mellem IT Forum Gruppen A/S 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 implementering 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' underleverandører.

Kontroller udført hos 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 effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover inspiceres dokumentation for at kontrollen er implementeret.
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 Organisatoriske foranstaltninger

Kontrolmål: At sikre fortsat egnethed, tilstrækkelighed, effektivitet af retningslinjer og understøtning af informationssikkerhed i overensstemmelse med forretningsmæssige, juridiske, lovbestemte, regulerende og kontraktmæssige krav.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.1	*Politikker for informationssikkerhed* Informationssikkerhedspolitik og emnespecifikke politikker skal defineres, godkendes af ledelsen, offentliggøres, kommunikeres til og anerkendes af relevante medarbejdere og relevante interessenter og vurderes med planlagte mellemrum samt hvis der sker væsentlige ændringer.	Vi har inspiceret at informationssikkerhedspolitikken er godkendt af ledelsen samt offentliggjort og kommunikeret til medarbejderne. Vi har inspiceret at informationssikkerhedspolitikken er opdateret.	Ingen afvigelser konstateret.
5.2	*Roller og ansvar for informationssikkerhed* Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov.	Vi har inspiceret organisationsdiagram over informationssikkerhedsorganisationen. Vi har inspiceret beskrivelsen af roller og ansvar i informationssikkerhedsorganisationen.	Ingen afvigelser konstateret.
5.3	*Funktionsadskillelse* Konfliktende opgaver og konfliktende ansvarsområder skal adskilles.	Vi har inspiceret organisationsdiagrammer der viser at adskillelsen af opgaver er etableret på virksomhedsniveau.	Ingen afvigelser konstateret.
5.4	*Ledelsens ansvar* Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.	Vi har inspiceret at ledelsen i ansættelseskontrakter har krævet at medarbejderne efterlever informationssikkerhedspolitikker og procedurer. Vi har stikprøvevis inspiceret at kravene for efterlevelse af informationssikkerhedsforanstaltninger er inkluderet i medarbejdernes ansættelseskontrakt.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At etablere et ledelsesmæssigt grundlag der sikrer identifikation og afbødning af informationssikkerhedsrisici relateret til juridiske, regulerende, rådgivende myndigheder, trusler og projektstyring.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.5	*Kontakt med myndigheder* Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.	Vi har inspiceret at der er etableret en procedure for passende kontakt med relevante myndigheder. Vi har inspiceret at passende kontakt med relevante myndigheder er vedligeholdt.	Ingen afvigelser konstateret.
5.6	*Kontakt med særlige interessegrupper* Organisationen skal etablere og vedligeholde passende kontakt med særlige interessegrupper eller andre specialistfora omkring sikkerhed og faglige organisationer.	Vi har inspiceret at der er etableret en procedure for passende kontakt med særlige interessegrupper. Vi har inspiceret at passende kontakt med særlige interessegrupper er vedligeholdt.	Ingen afvigelser konstateret.
5.7	*Underretning om trusler* Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretning om trusler.	Vi har inspiceret at der er etableret en procedure for trusselsefterretninger. Vi har inspiceret at identificerede trusler er indsamlet og analyseret.	Ingen afvigelser konstateret.
5.8	*Informationssikkerhed i projekter* Informationssikkerhed skal integreres i projektstyringen.	Vi har inspiceret at der er etableret en projektstyringsprocedure inklusive at informationssikkerhedskrav er integreret i projektstyringen. Vi har stikprøvevis inspiceret at informationssikkerhedskrav er blevet integreret i projektstyringen.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At identificere organisatoriske aktiver og definere passende beskyttelsesansvar.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.9	*Fortegnelse over information og understøttende aktiviteter* Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.	Vi har inspiceret at en fortegnelse over aktiver, inklusive ejere, er udviklet og vedligeholdt.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At identificere organisatoriske aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.10	*Acceptabel brug af information og understøttende aktiviteter* Regler for acceptabel brug og procedurer til håndtering af information og understøttende aktiver skal identificeres, dokumenteres og implementeres.	Vi har inspiceret at der er udarbejdet en procedure for acceptabel brug af information og aktiver. Vi har inspiceret at reglerne for acceptabel brug af information og aktiver er blevet implementeret.	Ingen afvigelser konstateret.
5.11	*Returnering af aktiver* Medarbejdere og andre interessenter skal aflevere alle de af organisationens aktiver, de har i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører eller ændrer karakter.	Vi har inspiceret at der er udarbejdet en procedure for returneringen af aktiver. Vi har, stikprøvevis, inspiceret at medarbejdere, ved ansættelsesophør har returneret organisationens aktiver.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.12	*Klassifikation af information* Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.	Vi har inspiceret at der er udarbejdet en procedure for klassificering af information.	Ingen afvigelser konstateret.
5.14	*Overførsel af information* Der skal være etableret regler eller procedurer for, eller aftaler om, overførsel af information for alle former for overførselsfaciliteter i organisationen og mellem organisationen og andre parter.	Vi har inspiceret at der er udarbejdet en sikkerhedsprocedure i forbindelse med overførsel af information. Vi har inspiceret at meddelelser er sikret med passende sikkerhedsprotokoller og brugen af sikker mail.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre autoriseret adgang og forhindre uautoriseret adgang til systemer og tjenester.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.15	*Administration af adgang* Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til information og understøttende aktiver på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret at både politik og procedure for administration af adgang er etableret og opdateret.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.16	*Styring af identifikation* Identiteters samlede livscyklus skal styres.	Vi har stikprøvevis inspiceret at identiteter er tildelt unikke bruger-ID, der muliggør sporing af aktiviteter. Vi har stikprøvevis inspiceret at tildelingen af brugerrettigheder er baseret på jobfunktionen og godkendelse fra nærmeste leder. Vi har stikprøvevis inspiceret at sletning af brugerrettigheder bliver udført rettidigt efter ansættelsesophør.	Ingen afvigelser konstateret.
5.17	*Autentifikationsoplysninger* Tildeling og styring af autentifikationsoplysninger skal ske i form af en ledelsesproces, herunder rådgivning af medarbejdere om passende håndtering af autentifikationsoplysninger.	Vi har inspiceret at der er etableret en procedure for styring af passwords. Vi har inspiceret at konfiguration af passwords er i overensstemmelse med den etablerede procedure.	Ingen afvigelser konstateret.
5.18	*Adgangsrettigheder* Adgangsrettigheder til information og understøttende aktiver skal tilvejebringes, vurderes, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for administration af adgang.	Vi har stikprøvevis inspiceret at tildelingen af brugernes adgangsrettigheder er baseret på jobfunktionen og godkendelse fra nærmeste leder. Vi har stikprøvevis inspiceret at sletning af brugernes adgangsrettigheder bliver udført rettidigt efter ansættelsesophør. Vi har inspiceret at adgangsrettigheder bliver gennemgået regelmæssigt og mindst én gang om året.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre et aftalt niveau af informationssikkerhed i leverandørforhold og levering af serviceydelser i overensstemmelse med leverandøraftaler.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.19	*Informationssikkerhed i leverandørforhold* Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.	Vi har inspiceret at proceduren til styring af leverandørforhold og serviceaftaler indeholder krav til afhjælpning af de risici der er forbundet med leverandørens adgang til aktiver.	Ingen afvigelser konstateret.
5.21	*Styring af informationssikkerhed i IKT forsyningskæden* Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med forsyningskæden for IKT-produkter og -tjenester.	Vi har inspiceret at der er etableret en procedure for styring af forsyningskæden for IKT-produkter og tjenester.	Ingen afvigelser konstateret.
5.22	*Overvågning, vurdering og ændringsstyring af leverandørydelser* Organisationen skal regelmæssigt overvåge, vurdere, evaluere og styre ændringer i leverandørers informationssikkerhedspraksis og levering af ydelser.	Vi har inspiceret at alle der er foretaget overvågning af alle vigtige leverandører inklusive udliciterede services. Vi har inspiceret at der er blevet fulgt op på enhver signifikant risiko der er identificeret i overvågningen.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre en hurtig, effektiv, ensartet og metodisk tilgang til håndteringen af informationssikkerhedshændelser, inklusive kommunikation omkring sikkerhedshændelser og svagheder.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.24	*Planlægning og forberedelse af incidenthåndtering ved sikkerhedshændelser* Organisationen skal planlægge og forberede sig på at håndtere informationssikkerhedshændelser ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedshændelser.	Vi har inspiceret at der er etableret en procedure for styring af informationssikkerhedshændelser. Vi har inspiceret at roller og ansvar relateret til styring af informationssikkerhedshændelser er blevet defineret og gjort tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
5.25	*Vurdering af om beslutning om informationssikkerhedshændelser* Organisationen skal vurdere informationssikkerhedshændelser og beslutte, om de skal kategoriseres som informationssikkerhedshændelser.	Vi har inspiceret at der er etableret en procedure for vurdering og beslutning om informationssikkerhedshændelser. Vi har stikprøvevis inspiceret at informationssikkerhedshændelser er blevet kategoriseret i henhold til proceduren.	Ingen afvigelser konstateret.
5.26	*Håndtering af informationssikkerhedshændelser* Informationssikkerhedshændelser skal håndteres i overensstemmelse med de dokumenterede procedurer.	Vi har inspiceret proceduren for håndtering af informationssikkerhedshændelser. Vi har stikprøvevis inspiceret at informationssikkerhedshændelser er blevet håndteret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
5.27	*Læring fra informationssikkerhedshændelser* Den viden, der opnås i forbindelse med informationssikkerhedsincidents, skal anvendes til at styrke og forbedre foranstaltningerne for informationssikkerhed.	Vi har inspiceret at der er etableret en procedure for læring fra informationssikkerhedshændelser. Vi har stikprøvevis inspiceret at sikkerhedshændelser er blevet registreret for at reducere risikoen for gentagelser.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.28	*Indsamling af bevismateriale* Organisationen skal definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af bevismateriale i relation til informationssikkerhedshændelser.	Vi har inspiceret at der er etableret en procedure for håndtering af bevismateriale relateret til informationssikkerhedshændelser. Vi har stikprøvevis inspiceret at bevismateriale er blevet identificeret, indsamlet, anskaffet og opbevaret i henhold til proceduren.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: Informationssikkerhedskontinuitet skal være indlejret i organisationens beredskabsplaner.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.29	*Informationssikkerhed under driftsforstyrrelse* Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.	Vi har inspiceret at organisationens beredskabsplaner er udarbejdet og godkendt af ledelsen. Vi har inspiceret at beredskabsplaner er gjort tilgængelige for relevante medarbejdere. Vi har inspiceret at beredskabsplaner er blevet testet.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre beskyttelsen og tilgængelighed af information og andre tilknyttede aktiver under en afbrydelse.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.30	*IKT-parathed til understøttelse af business continuity* IKT-parathed skal planlægges, implementeres, vedligeholdes og testes på grundlag af mål for business continuity og IKT-kontinuitetskrav.	Vi har inspiceret at der er udarbejdet en Business Impact Analysis (BIA). Vi har inspiceret at Recovery Time Objective (RTO) og Recovery Point Objective (RPO) er blevet identificeret for relevante ressourcer. Vi har inspiceret at beredskabsplaner, inklusive Recovery Time Objective (RTO) og Recovery Point Objective (RPO) er blevet testet.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre overholdelse af og undgå brud på juridiske, lovmæssige, regulatoriske og kontraktlige krav, der er relevante for informationssikkerhed eller andre sikkerhedskrav.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.31	*Juridiske, lovmæssige, regulatoriske og kontraktlige krav* Juridiske, lovmæssige, regulatoriske og kontraktlige krav, der er relevante for informationssikkerhed, samt organisationens tilgang til overholdelse af disse krav, skal være identificeret, dokumenteret og opdateret.	Vi har inspiceret at der bliver vedligeholdt et register over juridiske, lovmæssige, regulatoriske og kontraktmæssige krav der er relevante for informationssikkerheden. Vi har inspiceret at organisationens tilgang til imødegåelse af relevante krav er identificeret, dokumenteret og opdateret.	Ingen afvigelser konstateret.
5.32	*Intellektuelle ejendomsrettigheder* Organisationen skal implementere passende procedurer til beskyttelse af intellektuelle ejendomsrettigheder.	Vi har inspiceret at adgang til kritiske ophavsrettigheder (fx kildekoder) er blevet begrænset til medarbejdere med et arbejdsrelateret behov.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.33	*Beskyttelse af optegnelser* Optegnelser skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse.	Vi har inspiceret at logs er beskyttede mod ødelæggelse eller sletning.	Ingen afvigelser konstateret.
5.34	*Privatlivsbeskyttelse og beskyttelse af personoplysninger* Organisationen skal identificere og opfylde kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav	Vi har stikprøvevis inspiceret at krav og risici til PII (Personlig Identificerbar Information) i forbindelse med projekter er identificeret.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål: At sikre at informationssikkerhed er implementeret og operationel i overensstemmelse med de organisatoriske foranstaltninger og procedurer.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.36	Overensstemmelse med organisationens informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder skal vurderes regelmæssigt.	Vi har inspiceret at organisationen har defineret en oversigt over kontroller til overholdelse af politikker og procedurer. Vi har inspiceret at interne kontroller til overholdelse af politikker og procedurer er blevet udarbejdet.	Ingen afvigelser konstateret.
5.37	Driftsprocedurer for informationsbehandlingsfaciliteter skal dokumenteres og gøres tilgængelige for medarbejdere, der har brug for dem.	Vi har inspiceret at driftsprocedurer er blevet udarbejdet og dokumenteret. Vi har inspiceret at driftsprocedurer er gjort tilgængelige for relevante medarbejdere.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger

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*
6.1	*Screening* Der skal udføres baggrundsverifikation af alle jobansøgeres baggrund. Verifikationen skal foretages, inden de tiltræder i organisationen og løbende, under hensyntagen til love, forskrifter og etiske regler, og skal vurderes i forhold til organisationens krav, klassifikationen af den information, der skal gives adgang til, og de relevante risici.	Vi har inspiceret at der er udarbejdet en procedure for screening af nye medarbejdere. Vi har stikprøvevis inspiceret at baggrundschecks af nye medarbejdere er blevet udført i henhold til proceduren.	Ingen afvigelser konstateret.
6.2	*Ansættelsesvilkår og -betingelser* Ansættelseskontrakter skal beskrive medarbejdernes og organisationens ansvar for informationssikkerhed.	Vi har stikprøvevis inspiceret at underskrevne ansættelseskontrakter beskriver medarbejderens og organisationens ansvar for informationssikkerhed.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger

Kontrolmål: At sikre at medarbejdere og relevante interessenter er bevidste om og lever op til deres informationssikkerhedsansvar, og forstår konsekvenserne af manglende overholdelse af informationssikkerhedspolitikkerne.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
6.3	*Awareness, uddannelse og træning vedrørende informationssikkerhed* Organisationens medarbejdere og relevante interessenter skal modtage passende awareness, uddannelse og træning vedrørende informationssikkerhed samt regelmæssige opdateringer om organisationens informationssikkerhedspolitik, emnespecifikke politikker og procedurer, hvor det er relevant for deres jobfunktion.	Vi har inspiceret at der er etableret et program for informationssikkerheds awareness. Vi har inspiceret at organisationens medarbejdere har gennemført træning vedrørende informationssikkerhed. Vi har inspiceret at organisationen har etableret en kontrol for opfølgning på medarbejdere, der ikke har gennemført informationssikkerheds awarenesstræning.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
6.4	*Sanktioner* Der skal formaliseres og kommunikeres en sanktionsproces, så der iværksættes handlinger mod medarbejdere og andre relevante interessenter, som har overtrådt informationssikkerhedspolitikken.	Vi har inspiceret at der er etableret en sanktionsproces der er kommunikeret til medarbejderne. Vi har stikprøvevis inspiceret at underskrevne ansættelseskontrakter indeholder sanktionsprocessen.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger

Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
6.5	*Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold* Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.	Vi har inspiceret at der er defineret informationssikkerhedsansvar og forpligtelser der gælder efter ansættelsens ophør eller ændring. Vi har stikprøvevis inspiceret at fratrådte medarbejdere er blevet informeret om at informationssikkerhedsansvar og forpligtelser stadig er gældende efter ansættelsens ophør.	Ingen afvigelser konstateret.
6.6	*Hemmeligholdelses- og fortrolighedsaftaler* Hemmeligholdelses- og fortrolighedsaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejdere og andre interessenter.	Vi har inspiceret at der er etableret en hemmeligholdelses- og fortrolighedsaftale. Vi har stikprøvevis inspiceret at hemmeligholdelses- og fortrolighedsaftaler er underskrevet af medarbejderne og andre relevante interessenter.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger

Kontrolmål: At sikre et passende sikkerhedsniveau når medarbejdere arbejder Via fjernarbejdspladser, og en effektiv rapportering af informationssikkerhedshændelser.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
6.7	*Distancearbejde* Der skal være implementerede sikkerhedstiltag, når medarbejdere arbejder på afstand, for at beskytte information, der er adgang til, og som behandles eller lagres uden for organisationens lokaliteter.	Vi har inspiceret at multifaktor autentifikation er implementeret og aktiveret når medarbejderne arbejder på afstand. Vi har inspiceret at virtuelle private netværk (VPN) bliver anvendt for sikker kommunikation, når medarbejderne arbejder på afstand.	Ingen afvigelser konstateret.
6.8	*Indrapportering af informationssikkerhedshændelser* Organisationen skal sørge for, at medarbejdere kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt Via passende kanaler.	Vi har inspiceret at der er etableret en procedure for indrapportering af informationssikkerhedshændelser. Vi har inspiceret at medarbejderne har mulighed for at indrapportere informationssikkerhedshændelser og at kvalificeret personale følger op på disse.	Ingen afvigelser konstateret.

A.7 Fysiske foranstaltninger

Kontrolmål: At forhindre uautoriseret fysisk adgang, beskadigelse og indgriben i organisationens information og understøttende aktiver.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
7.1	*Fysisk områdesikring* Der skal defineres og anvendes områdesikring til at beskytte områder, der indeholder information og understøttende aktiver.	Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og sikkerhedsperimetre. VI har inspiceret relevante lokaliteter og deres sikkerhedsperimetre for at fastslå hvorvidt sikkerhedsforanstaltninger er implementeret for at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
7.2	*Fysisk adgangskontrol* Sikrede områder skal beskyttes ved hjælp af passende adgangsforanstaltninger og adgangspunkter.	Vi har inspiceret proceduren for tildeling af fysisk adgang. Vi har inspiceret access points og indgangsveje for at fastslå hvorvidt personlige adgangskort skal bruges for at opnå adgang til kontoret. Vi har inspiceret at der er installeret alarmer på fysisk adgangskontrol og at disse er aktiverede. Vi har inspiceret at der i løbet af perioden er udført gennemgang af fysiske adgangsrettigheder.	Ingen afvigelser konstateret.
7.3	*Sikring af kontorer, lokaler og faciliteter* Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.	Vi har inspiceret at der er fysisk sikring af kontorer, lokaler og faciliteter. Vi har forespurgt om informationsbehandlingsfaciliteterne kan ses eller høres udefra.	Ingen afvigelser konstateret.
7.5	*Beskyttelse mod fysiske og miljømæssige trusler* Beskyttelse mod fysiske og miljømæssige trusler, som fx naturkatastrofer og andre tilsigtede eller utilsigtede fysiske trusler mod infrastrukturen, skal tilrettelægges og implementeres.	Vi har inspiceret procedurer til beskyttelse mod fysiske og miljømæssige trusler. Vi har inspiceret at der er etableret sikkerhedsforanstaltninger til beskyttelse mod ild, varme og vand og vi har inspiceret relevante lokationer for at sikre at der er installeret ildslukningsudstyr, ild-og røgalarmer, blokering af vandrør, hævede gulve og alarmer til detektering af fugt, vand eller lignende.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
7.6	*Arbejde i sikrede områder* Sikkerhedsforhold for arbejde i sikrede områder skal tilrettelægges og implementeres.	Vi har inspiceret procedurer for arbejdet i sikrede områder. Vi har inspiceret at procedurerne er blevet implementerede.	Ingen afvigelser konstateret.

A.7 Fysiske foranstaltninger

Kontrolmål: At forhindre tab, beskadigelse, tyveri eller kompromittering af aktiver og afbrydelse af organisationens drift.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
7.8	*Placering og beskyttelse af udstyr* Udstyr skal placeres på et sikkert og beskyttet sted.	Vi har inspiceret proceduren for placering og beskyttelse af udstyr. Vi har inspiceret at relevante lokationer er aflåste.	Ingen afvigelser konstateret.
7.10	*Lagringsmedier* Lagringsmedier skal styres i hele deres livscyklus i forbindelse med anskaffelse, brug, transport og bortskaffelse i overensstemmelse med organisationens klassifikationssystem og krav til håndtering.	Vi har inspiceret procedurerne for styring af media, gennem anskaffelse, brug, transport og bortskaffelse. Vi har inspiceret dokumentation for at aktiver bliver håndteret i henhold til proceduren. Vi har stikprøvevis inspiceret at data og software er blevet slettet før bortskaffelse.	Ingen afvigelser konstateret.
7.11	*Forsyningssikkerhed* Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	Vi har inspiceret procedurer til beskyttelse af udstyr mod strømsvigt og andre forstyrrelser som følge af svigt i understøttende forsyninger. Vi har inspiceret at der er etableret backup strøm, UPS installation og diesel generatorer med passende kapacitet. Vi har inspiceret servicerapporter der viser at serviceinspektioner er blevet udført i overensstemmelse med leverandørernes anbefalinger og at udstyret bliver testet regelmæssigt.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
7.12	*Sikring af kabler* Kabler, som bærer strøm, data eller understøtter informationstjenester, skal beskyttes mod aflytning, forstyrrelse og beskadigelse.	Vi har inspiceret at strøm- og datakommunikationskabler er beskyttede mod forstyrrelse og beskadigelse.	Ingen afvigelser konstateret.
7.13	*Vedligeholdelse af udstyr* Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.	Vi har inspiceret politikken for vedligeholdelse af udstyr Vi har inspiceret at servicerapporter vedrørende vedligeholdelse af udstyr, indeholder leverandørernes anbefalinger.	Ingen afvigelser konstateret.
7.14	*Sikker bortskaffelse eller genbrug af udstyr* Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software slettes eller overskrives på forsvarlig vis inden bortskaffelse eller genbrug.	Vi har forespurgt til proceduren for sletning af data og software på lagringsmedier, før bortskaffelse af samme. Vi har stikprøvevis inspiceret at data er blevet slettet eller sikkert overskrevet inden bortskaffelse eller genbrug.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At beskytte information mod de risici der er forbundet med brugerenheder.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
8.1	*Brugerenheder* Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, skal beskyttes.	Vi har inspiceret at der er etableret en procedure for mobile enheder. Vi har inspiceret at politikken for brug af mobile enheder er gjort tilgængelig for relevante medarbejdere. Vi har inspiceret at installation af software på brugerudstyr er begrænset. Vi har stikprøvevis inspiceret at anti-malware er implementeret på laptops.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre at tildelingen og anvendelsen af privilegerede adgangsrettigheder er kontrolleret og begrænset, for at reducere risikoen for uautoriseret adgang, systemændringer eller forkert autentifikation.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.2	*Privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.	Vi har inspiceret at der er etableret en procedure til administration af privilegerede adgangsrettigheder. Vi har stikprøvevis inspiceret at tildeling af privilegerede adgangsrettigheder bliver udført efter godkendelse af nærmeste leder. Vi har stikprøvevis inspiceret at privilegerede adgangsrettigheder er begrænset til et arbejdsrelateret behov.	Ingen afvigelser konstateret.
8.3	*Begrænset adgang til information* Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.	Vi har inspiceret at der er etableret en politik for administration af adgange. Vi har stikprøvevis inspiceret at tildeling af brugerrettigheder er baseret på brugergrupper og roller, der indbefatter specifikke adgange, som fx læse, skrive, slette, og eksekvere. Vi har inspiceret at adgang til følsomme data er begrænset til et arbejdsbetinget behov. Vi har inspiceret at adgangsrettigheder er blevet gennemgået regelmæssigt og mindst én gang om året.	Ingen afvigelser konstateret.
8.5	*Sikker autentifikation* Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.	Vi har inspiceret at der er etableret en procedure til styring af passwords. Vi har inspiceret at password konfigurationer er baseret på den definerede procedure. Vi har inspiceret at multifaktor autentifikation er installeret og aktiv.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.6	*Kapacitetsstyring* Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.	Vi har inspiceret at der er etableret en procedure for overvågning af ressourcer og kapacitetsjusteringer. Vi har inspiceret at informationsbehandlingsressourcer bliver overvåget. Vi har inspiceret at der er implementeret overvågning til identificering af problemer.	Ingen afvigelser konstateret.
8.7	*Beskyttelse mod malware* Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.	Vi har inspiceret at der er etableret en procedure til beskyttelse mod malware. Vi har stikprøvevis inspiceret at der er installeret anti-malware på serverne. Vi har stikprøvevis inspiceret at der er installeret anti-malware på laptops.	Ingen afvigelser konstateret.
8.8	*Styring af tekniske sårbarheder* Der skal indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende tiltag.	Vi har inspiceret at der er etableret en procedure til styring af tekniske sårbarheder. Vi har inspiceret at der regelmæssigt udføres sårbarhedsskanninger. Vi har inspiceret at der er reageret på alle afvigelser eller svagheder.	Ingen afvigelser konstateret.
8.9	*Konfigurationsstyring* Konfigurationer, herunder sikkerhedskonfigurationer, af hardware, software, tjenester og netværk skal etableres, dokumenteres, implementeres, overvåges og vurderes.	Vi har inspiceret at organisationen har defineret grundlæggende sikkerhedskonfigurationer for hardware, software, services og netværk. Vi har stikprøvevis inspiceret at hardware, software, services og netværk er opsat i overensstemmelse med de grundlæggende sikkerhedskonfigurationer.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At forhindre unødig eksponering af følsomme data og at efterleve juridiske, lovmæssige, regulatoriske og kontraktlige krav.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.10	*Sletning af information* Information lagret i informationssystemer, enheder eller i andre lagringsmedier skal slettes, når der ikke længere er brug for den.	Vi har inspiceret at der er etableret en procedure for sletning af informationer. Vi har inspiceret at systemer er konfigurerede til automatisk at slette informationer i overensstemmelse med proceduren. Vi har stikprøvevis inspiceret at information bliver slettet før bortskaffelse af media.	Ingen afvigelser konstateret.
8.12	*Forebyggelse af datalækage* Der skal benyttes tiltag til at forebygge datalækage i systemer, netværk og andre enheder, der behandler, lagrer eller transmitterer følsom information.	Vi har inspiceret at der er etableret en procedure til forebyggelse af datalækage. Vi har inspiceret at foranstaltninger til forebyggelse af datalækager er implementeret i henhold til proceduren.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre kontinuerlig drift af informationsbehandlingsfaciliteter, inklusive genopretning efter tab af data eller systemer.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.13	*Backup af information* Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.	Vi har inspiceret at der er etableret en procedure for backup. Vi har stikprøvevis inspiceret at der løbende foretages backup i henhold til proceduren. Vi har stikprøvevis inspiceret at der dagligt modtages rapporter fra systemet med oplysning om, hvorvidt backuppen blev gennemført korrekt. Vi har stikprøvevis inspiceret at mislykkede eller fejlbehæftede backupkørsler er blevet rettet. Vi har inspiceret at der regelmæssigt udføres backup test for at fastslå at data kan genskabes fra backup filerne.	Ingen afvigelser konstateret.
8.14	*Redundans i faciliteter til informationsbehandling* Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har inspiceret at der er etableret tilgængelighedskrav for de relevante services og informationssystemer. Vi har inspiceret at system arkitektur og it-landskab er etableret med passende redundans. Vi har inspiceret at der er implementeret kontroller for redundans i komponent- og behandlingsaktiviteter i overensstemmelse med kravene.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At dokumentere hændelser, indsamle beviser, sikre loginformationer, forhindre uautoriseret adgang, opdage afvigelser og identificere informationssikkerheds-hændelser og brud.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.16	*Overvågning af aktiviteter* Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerhedshændelser.	Vi har inspiceret at der er etableret en procedure for overvågning af logaktiviteter. Vi har inspiceret at logaktiviteter bliver overvåget i henhold til proceduren.	Ingen afvigelser konstateret.
8.17	*Synkronisering af ure* Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.	Vi har inspiceret at ure, som organisationen anvender til informationsbehandling og supporterende informationsbehandlingssystemer, er synkroniserede med godkendte tidskilder.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre integriteten af driftssystemer og applikationsforanstaltninger så vel som at forebygge udnyttelse af tekniske sårbarheder.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.18	*Brugen af privilegerede understøttende programmer* Brugen af understøttende programmer, der kan omgå system- og applikationsforanstaltninger, skal begrænses og styres effektivt.	Vi har inspiceret at adgang til vedligeholdelse af understøttende programmer er begrænset til brugere med et arbejdsrelateret behov.	Ingen afvigelser konstateret.
8.19	*Softwareinstallation i test- og produktionssystemer* Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallationer i test- og produktionssystemer.	Vi har inspiceret at der er etableret en procedure for softwareinstallationer på operativsystemer. Vi har inspiceret dokumentation for at der er opsat et system til udrulning af patches, samt at der er opsat alarmering i forbindelse med fejlede patches.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre beskyttelsen af netværk, netværksenheder og understøttende behandlingsfaciliteter.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.20	*Netværkssikkerhed* Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.	Vi har inspiceret at der er etableret en sikkerhedspolitik for netværk og netværksenheder. Vi har inspiceret at der anvendes virtuelle private netværk (VPN) for at sikre krypteret forbindelse med netværk udenfor organisationen. Vi har inspiceret at netværket overvåges for afvigelser og at der bliver fulgt op på disse.	Ingen afvigelser konstateret.
8.22	*Segmentering af netværk* Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.	Vi har inspiceret at der er etableret en netværkssikkerhedspolitik. Vi har inspiceret at der er implementeret segmentering der opdeler netværk i flere zoner.	Ingen afvigelser konstateret.
8.23	*Webfiltrering* Adgang til eksterne websites skal styres for at reducere eksponering for skadeligt ind hold.	Vi har inspiceret at organisationen har vedligeholdt en liste over eksterne websider, som medarbejderne ikke har adgang til. Vi har inspiceret at der er implementeret en liste over begrænsede eksterne websider, og vi har inspiceret at brugerudstyr ikke kan få adgang til forbudte websider.	Ingen afvigelser konstateret.
8.24	*Brug af kryptografi* Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.	Vi har inspiceret at der er etableret en politik for definitionen af regler for brug af kryptografi. Vi har inspiceret at information er beskyttet i henhold til politikken for kryptografi.	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At godkende at informationssikkerhedskrav er overholdt ved implementering af applikationer eller kode i driftsmiljøet.

Nr.	*IT Forum Gruppen A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.31	*Adskillelse af udviklings- test- og produktionsmiljøer* Udviklings-, test- og produktionsmiljøer skal adskilles og sikres.	Vi har inspiceret at udviklings-, test- og produktionsmiljøer er adskilte. Vi har inspiceret at der er etableret adskillelse af pligter mellem medarbejdere med adgang til udviklings-, test- og produktionsmiljøer.	Ingen afvigelser konstateret.
8.32	*Ændringsstyring* Ændringer til informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.	Vi har inspiceret at der er etableret en procedure for ændringsstyring. Vi har stikprøvevis inspiceret at nøglepersoner har godkendt ændringer før disse bliver implementeret. Vi har stikprøvevis inspiceret at ændringer bliver testet, baseret på fastsatte kriterier, før de implementeres.	Ingen afvigelser konstateret.

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."

Mikael Elling
Underskriver 1
Serienummer: c3427568-ee5d-430b-8da2-80dac2bcdbb7
IP: 212.130.xxx.xxx
2025-04-10 13:22:00 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2025-04-10 13:25:45 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2025-04-10 13:44:00 UTC