

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 2025 til 31. december 2025

Marts 2026

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

Indholdsfortegnelse

Sektion 1:	IT Forum Gruppen A/S' udtalelse.....	1
Sektion 2:	Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet.....	3
Sektion 3:	Beskrivelse af IT Forum Gruppen A/S' ydelser i forbindelse med drift af hosting platform samt generelle it-kontroller relateret hertil.....	5
Sektion 4:	Kontrolmål, udførte kontroller, test og resultater heraf.....	13

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 2025 til 31. december 2025.

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 2025 til 31. december 2025.
- (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 2025 til 31. december 2025, 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 2025 til 31. december 2025.

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 2025 til 31. december 2025.

Aarhus, den 30. marts 2026
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 2025 til 31. december 2025 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 kontrollerens 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 2025 til 31. december 2025, 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 2025 til 31. december 2025, 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 2025 til 31. december 2025.

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, 30. marts 2026

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

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 fortsat udviklingen af sin informationssikkerhed og har bevæget sig fra implementering til en mere moden og driftsforankret sikkerheds- og compliancemodel.

Virksomheden har i perioden arbejdet målrettet med at konsolidere og operationalisere sit ISMS (Information Security Management System), hvilket har resulteret i følgende væsentlige forbedringer:

- **Forankring af ISMS i driften**
ISMS-platformen anvendes nu som et centralt styringsværktøj til håndtering af kontroller, risikovurderinger og dokumentation, hvilket sikrer en systematisk og løbende opfølgning på informationssikkerheden.
- **Øget modenhed i kontrolmiljøet**
Kontrolstrukturen er videreudviklet og operationaliseret, hvilket har styrket governance, adgangsstyring, ændringshåndtering og hændeshåndtering.
- **Styrket risikostyring og løbende vurdering af trusselsbilledet**
Risikovurderingsprocessen er videreudviklet til at understøtte en mere dynamisk og kontinuerlig vurdering af risici, hvilket muliggør en mere proaktiv håndtering af sikkerhedstrusler.

- **Konsolidering af ISO/IEC 27001:2022-rammeverket**
Overgangen til ISO/IEC 27001:2022 er fuldt implementeret og forankret i organisationens processer, hvilket sikrer et tidssvarende og robust kontrolgrundlag.
- **Styrket compliance- og dokumentationsstruktur**
Dokumentation, politikker og kontroller vedligeholdes løbende og er samlet i én platform, hvilket øger transparens, sporbarhed og revisionsklarhed.

Samlet set understøtter udviklingen en højere grad af modenhed i IT Forum Gruppen A/S' kontrolmiljø og sikrer, at informationssikkerhed er en integreret og løbende del af virksomhedens drift og governance.”

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 fra 1. januar 2025 til 31. december 2025 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 awareness-træning.
- Adgangsstyring – Implementering af Zero Trust-principper, strammere adgangskontrol og multifaktor-autentificering (MFA).
- Fysisk sikring og miljøsikring – Forbedret sikring af datacentre.
- Driftssikkerhed – Forstærket monitorering og dokumenteret hændeshåndtering.
- Kommunikationssikkerhed – Krypterede forbindelser, sikre transmissionsprotokoller og avanceret netværksovervågning.
- Styring af informationssikkerhedshændelser – Struktureret hændeshåndtering 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 hændelsehåndtering.

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.

Ansvar 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 hændelsehåndteringsprocesser.

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 kølevekslere 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-strømbakop, 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.
- Dokumentation 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 udviklingsammenhænge 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. Niveaue 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 ISAE 3402-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 revisions perioden 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.
Genduførelse 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	<p><i>Politikker for informationssikkerhed</i></p> <p>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.</p>	<p>Vi har inspiceret, at der foreligger en formel, skriftlig og identificerbar informationssikkerhedspolitik, som er godkendt af virksomhedens ledelse.</p> <p>Vi har inspiceret, at informationssikkerhedspolitikken er offentliggjort og kommunikeret til medarbejderne, og at den er opdateret inden for revisionsperioden.</p>	Ingen afvigelser konstateret.
5.2	<p><i>Roller og ansvar for informationssikkerhed</i></p> <p>Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov.</p>	<p>Vi har inspiceret, at roller og ansvar for informationssikkerhed er formelt defineret og dokumenteret i organisationen, samt at disse er opdateret og gældende for revisionsperioden.</p> <p>Vi har inspiceret, at roller og ansvar er allokeret til navngivne personer eller funktioner i organisationen.</p> <p>Vi har inspiceret organisationsdiagrammet for at verificere, at ansvar for informationssikkerhed fremgår tydeligt og kan identificeres i organisationens struktur.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.3	<p><i>Funktionsadskillelse</i></p> <p>Konfliktende opgaver og konfliktende ansvarsområder skal adskilles.</p>	<p>Vi har inspiceret, at funktionsadskillelse er dokumenteret og formaliseret gennem organisationsdiagrammet med tydelige roller, navne og rapporteringslinjer.</p> <p>Vi har inspiceret dokumentation, der beskriver tildeling af specifikke roller og rettigheder samt adskillelse af konfliktende opgaver og ansvarsområder.</p> <p>Vi har inspiceret, at organisationsdiagrammet er opdateret inden for revisionsperioden, samt at funktionsadskillelse er implementeret og dokumenteret gennem adskilte roller i organisationen.</p>	Ingen afvigelser konstateret.
5.4	<p><i>Ledelsens ansvar</i></p> <p>Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.</p>	<p>Vi har inspiceret, at ledelsen har fastlagt og formelt godkendt en informationssikkerhedspolitik for organisationen.</p> <p>Vi har inspiceret, at organisationens procedurer kræver, at medarbejdere efterlever informationssikkerhedspolitikker og -procedurer.</p> <p>Vi har inspiceret, at ansættelseskontrakter indeholder krav om efterlevelse af organisationens informationssikkerhedspolitikker og -procedurer.</p> <p>Vi har stikprøvevis inspiceret at kravene for efterlevelse af informationssikkerhedsforanstaltninger er inkluderet i medarbejdernes ansættelseskontrakt.</p>	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	<p><i>Kontakt med myndigheder</i></p> <p>Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.</p>	<p>Vi har inspiceret, at der er udarbejdet en procedure for kontakt med relevante myndigheder, og at organisationen har identificeret relevante myndigheder, herunder relevante tilsyn og styrelser.</p> <p>Vi har inspiceret dokumentation for vedligeholdelse og opdatering af proceduren for kontakt med myndigheder i revisionsperioden.</p>	Ingen afvigelser konstateret.
5.6	<p><i>Kontakt med særlige interessegrupper</i></p> <p>Organisationen skal etablere og vedligeholde passende kontakt med særlige interessegrupper eller andre specialistfora omkring sikkerhed og faglige organisationer.</p>	<p>Vi har inspiceret dokumentation for, at der eksisterer en dokumenteret procedure for kontakt med særlige interessegrupper, og at denne procedure er blevet fulgt i revisionsperioden.</p> <p>Vi har inspiceret dokumentation for at der har været kontakt med interessegrupper i løbet af revisionsperioden.</p>	Ingen afvigelser konstateret.
5.7	<p><i>Underretning om trusler</i></p> <p>Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretning om trusler.</p>	<p>Vi har inspiceret, at procedurer for håndtering og analyse af trusler er dokumenteret, godkendt og fordeler ansvar og metoder.</p> <p>Vi har inspiceret, at indsamling og analyse af trusler er udført og dokumenteret i perioden</p>	Ingen afvigelser konstateret.
5.8	<p><i>Informationssikkerhed i projekter</i></p> <p>Informationssikkerhed skal integreres i projektstyringen.</p>	<p>Vi har inspiceret, at der er dokumentation for integration af informationssikkerhedsprincipper i projektstyringsprocessen, herunder risikovurderinger og involvering af informationssikkerhedschefen.</p> <p>Vi har inspiceret en oversigt over udførte projekter i perioden med relevante oplysninger.</p> <p>Vi har stikprøvevis inspiceret, at informationssikkerhedskrav er blevet integreret i konkrete projekter.</p>	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	<p><i>Fortegnelse over information og understøttende aktiviteter</i></p> <p>Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.</p>	<p>Vi har inspiceret, at der er udarbejdet en fortegnelse over information og understøttende aktiver, herunder ejere og klassifikation, med løbende vedligeholdelse og dokumenteret ansvar.</p> <p>Vi har inspiceret, at fortegnelse over information og understøttende aktiver er opdateret i revisionsperioden.</p> <p>Vi har inspiceret, at ejerskab fremgår for aktiver i fortegnelsen i praksis.</p>	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	<p><i>Acceptabel brug af information og understøttende aktiviteter</i></p> <p>Regler for acceptabel brug og procedurer til håndtering af information og understøttende aktiver skal identificeres, dokumenteres og implementeres.</p>	<p>Vi har inspiceret at der er udarbejdet en procedure for acceptabel brug af information og aktiver.</p> <p>Vi har inspiceret at reglerne for acceptabel brug af information og aktiver er blevet implementeret.</p>	Ingen afvigelser konstateret.
5.11	<p><i>Returnering af aktiver</i></p> <p>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.</p>	<p>Vi har inspiceret en dokumenteret procedure for returnering af aktiver ved ansættelsesophør, hvor ansvarsområder er klart fordelt til nærmeste leder og IT-afdelingen.</p> <p>Vi har inspiceret liste over fratrådte medarbejdere i perioden.</p> <p>Vi har stikprøvevis inspiceret dokumentation for, at fratrådte medarbejdere har returneret organisationens aktiver.</p>	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	<p><i>Klassifikation af information</i></p> <p>Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.</p>	<p>Vi har inspiceret procedure for klassificering af information og aktiver.</p> <p>Vi har inspiceret eksempler på klassificeret information, hvor klassificeringen er udført i overensstemmelse med den dokumenterede procedure, med angivelse af klassifikationsniveauer og tydelig ansvarsplacering.</p>	Ingen afvigelser konstateret.
5.14	<p><i>Overførsel af information</i></p> <p>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.</p>	<p>Vi har inspiceret procedure for overførsel af information.</p> <p>Vi har inspiceret, at sikkerhedsprotokoller er implementeret, herunder brug af krypterede tjenester, TLS-kryptering, adgangskontrol, overvågning og logning.</p> <p>Vi har inspiceret, at der anvendes krypterede eller godkendte overførselstjenester ved overførsel af følsom information, og at dette kan dokumenteres gennem konkrete eksempler samt årlige kontroller af procedurer og fortrolighedskrav.</p>	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	<p><i>Administration af adgang</i></p> <p>Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til information og understøttende aktiver på grundlag af forretnings- og informationssikkerhedskrav.</p>	<p>Vi har inspiceret, at der foreligger en procedure for administration af adgang.</p> <p>Vi har inspiceret, at proceduren for administration af adgang indeholder dokumenteret opdateringsdato.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.16	<p><i>Styring af identifikation</i></p> <p>Identiteters samlede livscyklus skal styres.</p>	<p>Vi har inspiceret dokumentation for procedurer for styring af identiteters livscyklus.</p> <p>Vi har inspiceret, at brugere tildeles et unikt bruger-ID ved oprettelse, og at brugerrettigheder tildeles på baggrund af jobfunktion og definerede roller.</p> <p>Vi har stikprøvevis inspiceret, at tildeling af brugerrettigheder er godkendt af nærmeste leder, og at brugere er oprettet med unikke bruger-ID'er og rettigheder i overensstemmelse med jobfunktion.</p>	Ingen afvigelser konstateret.
5.17	<p><i>Autentifikationsoplysninger</i></p> <p>Tildeling og styring af autentifikationsoplysninger skal ske i form af en ledelsesproces, herunder rådgivning af medarbejdere om passende håndtering af autentifikationsoplysninger.</p>	<p>Vi har inspiceret, at der foreligger en skriftlig procedure for styring af autentifikationsoplysninger.</p> <p>Vi har inspiceret dokumentation, der viser at passwordkonfigurationen i systemet opfylder kravene om minimumslængde, kompleksitet, historik og udløb i overensstemmelse med den dokumenterede procedure for adgangsstyring.</p>	Ingen afvigelser konstateret.
5.18	<p><i>Adgangsrettigheder</i></p> <p>Adgangsrettigheder til information og understøttende aktiver skal tilvejebringes, vurderes, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for administration af adgang.</p>	<p>Vi har inspiceret procedurer for tildeling, ændring og fjernelse af adgangsrettigheder.</p> <p>Vi har inspiceret, at der er etableret en proces for rettidig fjernelse af adgangsrettigheder ved ansættelsesophør.</p> <p>Vi har stikprøvevis inspiceret dokumentation for, at tildeling af brugerrettigheder er godkendt af nærmeste leder, at brugere er oprettet med unikke bruger-ID'er, og at rettigheder er tildelt i overensstemmelse med jobfunktion.</p>	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	<p><i>Informationssikkerhed i leverandørforhold</i></p> <p>Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.</p>	<p>Vi har inspiceret procedure for styring af leverandørforhold og serviceaftaler.</p> <p>Vi har inspiceret, dokumentation for at der er etableret løbende kontrol, risikovurdering og monitorering, og at der ikke er konstateret undtagelser ved gennemgang.</p>	Ingen afvigelser konstateret.
5.21	<p><i>Styring af informationssikkerhed i IKT forsyningskæden</i></p> <p>Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med forsyningskæden for IKT-produkter og -tjenester.</p>	<p>Vi har inspiceret procedure for styring af informationssikkerhedsrisici i forsyningskæden for IKT-produkter og -tjenester.</p> <p>Vi har inspiceret, at proceduren beskriver identifikation og håndtering af informationssikkerhedsrisici i forsyningskæden.</p> <p>Vi har inspiceret, at proceduren er opdateret inden for revisionsperioden og godkendt af relevante ansvarlige med dokumenteret godkendelsesdato.</p>	Ingen afvigelser konstateret.
5.22	<p><i>Overvågning, vurdering og ændringsstyring af leverandørydelser</i></p> <p>Organisationen skal regelmæssigt overvåge, vurdere, evaluere og styre ændringer i leverandørers informationssikkerhedspraksis og levering af ydelser.</p>	<p>Vi har inspiceret, at der er etableret og dokumenteret processer for overvågning, vurdering og ændringsstyring af leverandørydelser.</p> <p>Vi har inspiceret, at overvågning, risikovurdering og opfølgning på signifikante risici er gennemført i revisionsperioden for alle vigtige leverandører.</p>	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	<p><i>Planlægning og forberedelse af incidenthåndtering ved sikkerhedshændelser</i></p> <p>Organisationen skal planlægge og forberede sig på at håndtere informationssikkerhedshændelser ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedshændelser.</p>	<p>Vi har inspiceret, at der foreligger en formel procedure for planlægning og forberedelse af incidenthåndtering ved sikkerhedshændelser.</p> <p>Vi har inspiceret, at information om roller og ansvar er gjort tilgængelig for relevante medarbejdere via organisationens intranet.</p>	Ingen afvigelser konstateret.
5.25	<p><i>Vurdering af om beslutning om informationssikkerhedshændelser</i></p> <p>Organisationen skal vurdere informationssikkerhedshændelser og beslutte, om de skal kategoriseres som informationssikkerhedshændelser.</p>	<p>Vi har inspiceret, at der foreligger en formel, skriftlig og ledelsesgodkendt procedure for vurdering og beslutning om informationssikkerhedshændelser, som er kommunikeret til relevante medarbejdere.</p> <p>Vi har stikprøvevis inspiceret at informationssikkerhedshændelser er blevet kategoriseret i henhold til proceduren.</p>	Ingen afvigelser konstateret.
5.26	<p><i>Håndtering af informationssikkerhedshændelser</i></p> <p>Informationssikkerhedshændelser skal håndteres i overensstemmelse med de dokumenterede procedurer.</p>	<p>Vi har inspiceret, at der foreligger en dokumenteret, formel og godkendt procedure for håndtering af informationssikkerhedshændelser.</p> <p>Vi har stikprøvevis inspiceret at informationssikkerhedshændelser er blevet håndteret i overensstemmelse med proceduren.</p>	Ingen afvigelser konstateret.
5.27	<p><i>Læring fra informationssikkerhedshændelser</i></p> <p>Den viden, der opnås i forbindelse med informationssikkerhedsincidents, skal anvendes til at styrke og forbedre foranstaltningerne for informationssikkerhed.</p>	<p>Vi har inspiceret, at der foreligger en dokumenteret procedure for læring fra informationssikkerhedshændelser.</p> <p>Vi har stikprøvevis inspiceret at sikkerhedshændelser er blevet registreret, for at reducere risikoen for gentagelser.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.28	<p><i>Indsamling af bevismateriale</i></p> <p>Organisationen skal definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af bevismateriale i relation til informationssikkerhedshændelser.</p>	<p>Vi har inspiceret, at der foreligger en skriftlig og versionsstyret procedure for indsamling af bevismateriale ved informationssikkerhedshændelser.</p> <p>Vi har stikprøvevis inspiceret, at bevismateriale er blevet identificeret, indsamlet og opbevaret i overensstemmelse med proceduren.</p>	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	<p><i>Informationssikkerhed under driftsforstyrrelse</i></p> <p>Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.</p>	<p>Vi har inspiceret, at informationssikkerhedskontinuitet er indlejret i organisationens beredskabsplaner gennem dokumentation for udarbejdelse, godkendelse og tilgængelighed af planerne for relevante medarbejdere.</p> <p>Vi har inspiceret, at beredskabsøvelser med inddragelse af krisestyring og relevante roller er gennemført, og at testaktiviteter er dokumenteret og evalueret.</p>	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	<p><i>IKT-parathed til understøttelse af business continuity</i></p> <p>IKT-parathed skal planlægges, implementeres, vedligeholdes og testes på grundlag af mål for business continuity og IKT-kontinuitetskrav.</p>	<p>Vi har inspiceret, at Business Impact Analysis (BIA) er dokumenteret, dateret og godkendt.</p> <p>Vi har inspiceret, at RTO og RPO er fastlagt.</p> <p>Vi har inspiceret, at beredskabsplaner og tilhørende politikker er testet og evalueret gennem beredskabsøvelser, hvor både tekniske og organisatoriske forhold samt overholdelse af RTO og RPO er dokumenteret.</p>	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	<p><i>Juridiske, lovmæssige, regulatoriske og kontraktlige krav</i></p> <p>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.</p>	<p>Vi har inspiceret, at der er udarbejdet et register over juridiske, lovmæssige, regulatoriske og kontraktlige krav, der er relevante for informationssikkerhed, og at organisationens tilgang til håndtering af disse krav er dokumenteret.</p> <p>Vi har inspiceret, at organisationens tilgang til håndtering af relevante krav løbende opdateres gennem årlig revision.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.32	<p><i>Intellektuelle ejendomsrettigheder</i></p> <p>Organisationen skal implementere passende procedurer til beskyttelse af intellektuelle ejendomsrettigheder.</p>	<p>Vi har inspiceret dokumenterede procedurer for beskyttelse af intellektuelle ejendomsrettigheder.</p> <p>Vi har inspiceret at adgang til kritiske ophavsrettigheder (fx kildekoder) er blevet begrænset til medarbejdere med et arbejdsrelateret behov.</p>	Ingen afvigelser konstateret.
5.33	<p><i>Beskyttelse af optegnelser</i></p> <p>Optegnelser skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse.</p>	<p>Vi har inspiceret, at der er defineret procedurer for beskyttelse af optegnelser mod tab, ødelæggelse, forfalskning, uautoriseret adgang og offentliggørelse.</p> <p>Vi har inspiceret dokumentation for implementering af immutable backup af logs.</p>	Ingen afvigelser konstateret.
5.34	<p><i>Privatlivsbeskyttelse og beskyttelse af personoplysninger</i></p> <p>Organisationen skal identificere og opfylde kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav</p>	<p>Vi har inspiceret, at der eksisterer interne kontroller for opbevaring og sletning af personoplysninger samt overordnede politikker og rammer for beskyttelse af PII, og at interne kontroller relateret til beskyttelse af personoplysninger er dokumenteret.</p>	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	<p>Overensstemmelse med organisationens informationssikkerhedspolitik, emnespecifikke politikker, regler og standarder skal vurderes regelmæssigt.</p>	<p>Vi har inspiceret, at informationssikkerhed er implementeret og operationel i overensstemmelse med de organisatoriske foranstaltninger og procedurer.</p> <p>Vi har inspiceret en detaljeret oversigt over interne kontroller relateret til informationssikkerhed.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
5.37	Driftsprocedurer for informationsbehandlingsfaciliteter skal dokumenteres og gøres tilgængelige for medarbejdere, der har brug for dem.	Vi har inspiceret, at driftsprocedurerne er versionsstyrede, daterede og godkendt. Vi har inspiceret dokumentation for formelle og godkendte driftsprocedurer for informationsbehandlingsfaciliteter.	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 jobansøgere 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 foreligger en dokumenteret og godkendt 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 medarbejderens 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	<p><i>Awareness, uddannelse og træning vedrørende informationssikkerhed</i></p> <p>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.</p>	<p>Vi har inspiceret, at der er etableret et formelt awareness-program for informationssikkerhed, som er risikobaseret, rolle-specifikt og omfatter årlig træning.</p> <p>Vi har inspiceret, at awareness-programmet omfatter relevante emner om organisationens informationssikkerhedspolitikker og procedurer.</p> <p>Vi har inspiceret, at opdateringer i informationssikkerhedspolitikker og procedurer kommunikerer til medarbejderne via e-mailbaserede træningsmoduler og awareness-kampagner.</p> <p>Vi har inspiceret dokumentation for gennemførelse af informationssikkerhedstræning, herunder registreringer af medarbejderes deltagelse.</p>	Ingen afvigelser konstateret.
6.4	<p><i>Sanktioner</i></p> <p>Der skal formaliseres og kommunikeres en sanktionsproces, så der iværksættes handlinger mod medarbejdere og andre relevante interessenter, som har overtrådt informationssikkerhedspolitikken.</p>	<p>Vi har inspiceret, at der foreligger en formel og dokumenteret sanktionsproces for overtrædelse af informationssikkerhedspolitikken.</p> <p>Vi har stikprøvevis inspiceret at underskrevne ansættelseskontrakter indeholder sanktionsprocessen.</p>	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	<p><i>Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold</i></p> <p>Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.</p>	<p>Vi har inspiceret, at informationssikkerhedsansvar og -forpligtelser efter ophør eller ændring af ansættelsesforhold er tydeligt defineret, og at dokumentationen angiver, hvilke medarbejdere og roller der er omfattet af disse forpligtelser.</p> <p>Vi har stikprøvevis inspiceret at fratrådte medarbejdere er blevet informeret om at informationssikkerhedsansvar og forpligtelser stadig er gældende efter ansættelsens ophør.</p>	Ingen afvigelser konstateret.
6.6	<p><i>Hemmeligholdelses- og fortrolighedsaftaler</i></p> <p>Hemmeligholdelses- og fortrolighedsaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejdere og andre interessenter.</p>	<p>Vi har inspiceret, at der foreligger en formel og dokumenteret fortrolighedsaftale.</p> <p>Vi har stikprøvevis inspiceret underskrevne fortrolighedsaftaler for eksterne parter.</p> <p>Vi har stikprøvevis inspiceret at fortrolighedsaftaler er underskrevet af medarbejderne.</p>	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	<p><i>Distancearbejde</i></p> <p>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 lokalteter.</p>	<p>Vi har inspiceret, at der foreligger dokumenterede sikkerhedskrav for fjernarbejde, herunder krav til firewall-regler, VPN og tekniske krav til udstyr.</p> <p>Vi har inspiceret dokumentation for, at multifaktor autentifikation er implementeret.</p> <p>Vi har inspiceret dokumentation for, at VPN anvendes til sikker kommunikation ved fjernarbejde, herunder firewallregler, logs og VPN-konfigurationer.</p>	Ingen afvigelser konstateret.
6.8	<p><i>Indrapportering af informationssikkerhedshændelser</i></p> <p>Organisationen skal sørge for, at medarbejdere kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt Via passende kanaler.</p>	<p>Vi har inspiceret, at der foreligger en formel og godkendt procedure for indrapportering af informationssikkerhedshændelser.</p> <p>Vi har inspiceret, at medarbejderne har adgang til procedure for indrapportering af informationssikkerhedshændelser og anvender relevante kanaler til rapportering af informationssikkerhedshændelser.</p>	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	<p><i>Fysisk områdesikring</i></p> <p>Der skal defineres og anvendes områdesikring til at beskytte områder, der indeholder information og understøttende aktiver.</p>	<p>Vi har inspiceret, at procedurer for fysisk områdesikring er dokumenteret og godkendt.</p> <p>Vi har inspiceret implementeringen af disse fysiske sikkerhedsforanstaltninger og adgangskontrol på relevante lokaliteter.</p>	Ingen afvigelser konstateret.
7.2	<p><i>Fysisk adgangskontrol</i></p> <p>Sikrede områder skal beskyttes ved hjælp af passende adgangsforsanstaltninger og adgangspunkter.</p>	<p>Vi har inspiceret procedure for tildeling og fjernelse af fysisk adgang til sikrede områder.</p> <p>Vi har inspiceret, at adgangsrettigheder til sikre områder gennemgås kvartalsvist, og at loggennemgang er udført i perioden.</p>	Ingen afvigelser konstateret.
7.3	<p><i>Sikring af kontorer, lokaler og faciliteter</i></p> <p>Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.</p>	Vi har inspiceret, at fysiske sikringsforanstaltninger er implementeret og dokumenteret.	Ingen afvigelser konstateret.
7.5	<p><i>Beskyttelse mod fysiske og miljømæssige trusler</i></p> <p>Beskyttelse mod fysiske og miljømæssige trusler, som fx naturkatastrofer og andre tilsigtede eller utilsigtede fysiske trusler mod infrastrukturen, skal tilrettelægges og implementeres.</p>	<p>Vi har inspiceret, at der er etableret skriftlige procedurer for beskyttelse mod fysiske og miljømæssige trusler, og at denne er godkendt af ledelsen.</p> <p>Vi har inspiceret, at der er installeret brandslukningsudstyr samt brand- og røgalarmer i kritiske områder, og at der er udført test af lækagealarm til detektering af fugt og vand.</p>	Ingen afvigelser konstateret.
7.6	<p><i>Arbejde i sikrede områder</i></p> <p>Sikkerhedsforhold for arbejde i sikrede områder skal tilrettelægges og implementeres.</p>	<p>Vi har inspiceret, procedurer for arbejde i sikrede områder.</p> <p>Vi har inspiceret, at adgangskontrol, adgangsløgs, overvågning og adgangsbegrænsning er implementeret i sikrede områder, herunder at fysiske sikkerhedsforanstaltninger kun er tilgængelige for godkendte medarbejdere.</p>	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	<i>Placering og beskyttelse af udstyr</i> Udstyr skal placeres på et sikkert og beskyttet sted.	Vi har inspiceret procedure for placering og beskyttelse af udstyr. Vi har inspiceret dokumentation for, at adgang til sikre områder styres via adgangskontrol, herunder nøglebrikker og låsesystemer.	Ingen afvigelser konstateret.
7.10	<i>Lagringsmedier</i> 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 procedure for styring af lagringsmedier. Vi har inspiceret dokumentation for håndtering af lagringsmedier i overensstemmelse med proceduren. Vi har inspiceret, dokumentation for bortskaffede lagringsmedier.	Ingen afvigelser konstateret.
7.11	<i>Forsyningsikkerhed</i> Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	Vi har inspiceret dokumenterede procedurer for beskyttelse af informationsbehandlingsudstyr mod strømsvigt og andre forstyrrelser. Vi har stikprøvevis inspiceret serviceinspektion af UPS og generator.	Ingen afvigelser konstateret.
7.12	<i>Sikring af kabler</i> Kabler, som bærer strøm, data eller understøtter informationstjenester, skal beskyttes mod aflytning, forstyrrelse og beskadigelse.	Vi har inspiceret dokumenterede procedurer og politikker for beskyttelse af kabler. Vi har inspiceret dokumentation, der viser, at kabler er beskyttet.	Ingen afvigelser konstateret.
7.13	<i>Vedligeholdelse af udstyr</i> Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.	Vi har inspiceret procedure for vedligeholdelse af udstyr. Vi har inspiceret dokumentation for udført vedligeholdelse af udstyr.	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
7.14	<p><i>Sikker bortskaffelse eller genbrug af udstyr</i></p> <p>Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software slettes eller overskrives på forsvarlig vis inden bortskaffelse eller genbrug.</p>	<p>Vi har inspiceret, at der foreligger en dokumenteret procedure for sletning og destruktion af data på lagringsmedier før bortskaffelse eller genbrug.</p> <p>Vi har inspiceret dokumentation for bortskaffet udstyr.</p>	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	<p><i>Brugerenheder</i></p> <p>Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, skal beskyttes.</p>	<p>Vi har inspiceret procedure for håndtering af mobile enheder.</p> <p>Vi har inspiceret, at politikken for brug af mobile enheder er gjort tilgængelig for relevante medarbejdere.</p> <p>Vi har inspiceret, at installation af software på brugerudstyr er teknisk begrænset.</p> <p>Vi har inspiceret, at anti-malware software er implementeret på laptops.</p>	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	<p><i>Privilegerede adgangsrettigheder</i></p> <p>Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.</p>	<p>Vi har inspiceret procedure for administration af privilegerede adgangsrettigheder.</p> <p>Vi har inspiceret, at privilegerede adgangsrettigheder kun tildeles ved arbejdsrelateret behov, og at behovet løbende valideres.</p>	Ingen afvigelser konstateret.
8.3	<p><i>Begrænset adgang til information</i></p> <p>Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.</p>	<p>Vi har inspiceret politik for administration af adgange.</p> <p>Vi har inspiceret, at tildelingen af brugerrettigheder sker på baggrund af dokumenterede brugergrupper og roller.</p> <p>Vi har inspiceret, at kriterier for adgang til følsomme data er fastlagt og dokumenteret med rolle, afdeling og arbejdsopgaver samt godkendelse.</p> <p>Vi har inspiceret dokumentation for godkendelse af adgangsrettigheder.</p>	Ingen afvigelser konstateret.
8.4	<p><i>Adgang til kildekode</i></p> <p>Adgang til at læse og skrive kildekode, udviklingsværktøjer og softwarebiblioteker skal håndteres på en hensigtsmæssig måde.</p>	<p>Vi har inspiceret, at tildeling og anvendelse af privilegerede adgangsrettigheder til kildekode er kontrolleret og begrænset.</p> <p>Vi har inspiceret, at adgang til kildekode er begrænset til autoriserede personer via adgangskontrolmekanismer.</p>	Ingen afvigelser konstateret.
8.5	<p><i>Sikker autentifikation</i></p> <p>Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.</p>	<p>Vi har inspiceret at der er etableret en procedure til styring af passwords.</p> <p>Vi har inspiceret dokumentation for passwordkonfigurationer, herunder minimumslængde, kompleksitetskrav, hukommelse af adgangskoder, maksimal levetid, lockout-funktionalitet og krav til mobile enheder.</p> <p>Vi har inspiceret dokumentation for implementering og anvendelse af multifaktor autentifikation på relevante systemer.</p>	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	<p><i>Kapacitetsstyring</i></p> <p>Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.</p>	<p>Vi har inspiceret, at der er specificeret procedurer for overvågning af informationsbehandlingsressourcer.</p> <p>Vi har inspiceret dokumentation for implementering af tekniske løsninger til overvågning, der understøtter løbende monitorering af ressourcer og kapacitet.</p>	Ingen afvigelser konstateret.
8.7	<p><i>Beskyttelse mod malware</i></p> <p>Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.</p>	<p>Vi har inspiceret procedure for beskyttelse mod malware.</p> <p>Vi har inspiceret systemrapporter og dokumentation, der viser, at anti-malware software er installeret, aktiv og opdateret.</p>	Ingen afvigelser konstateret.
8.8	<p><i>Styring af tekniske sårbarheder</i></p> <p>Der skal indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende tiltag.</p>	<p>Vi har inspiceret procedure for styring af tekniske sårbarheder.</p> <p>Vi har inspiceret dokumentation for daglige og ugentlige sårbarhedsskanninger, reaktion på identificerede sårbarheder og håndtering af afvigelser i overensstemmelse med proceduren.</p>	Ingen afvigelser konstateret.
8.9	<p><i>Konfigurationsstyring</i></p> <p>Konfigurationer, herunder sikkerhedskonfigurationer, af hardware, software, tjenester og netværk skal etableres, dokumenteres, implementeres, overvåges og vurderes.</p>	<p>Vi har inspiceret, at der foreligger dokumenterede og versionsstyrede baseline-sikkerhedskonfigurationer.</p> <p>Vi har inspiceret, at der er etableret processer for konfigurationsstyring.</p> <p>Vi har inspiceret, at der er etableret procedurer og værktøjer til overvågning og vurdering af sikkerhedskonfigurationer.</p> <p>Vi har inspiceret dokumentation for implementeret konfigurationsstyring, herunder patching, sikkerhedskonfigurationer, kryptering, compliance-kontroller, endpoint politikker og registrering og overvågning af hardware og software.</p>	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At forhindre unødigt 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	<p><i>Sletning af information</i></p> <p>Information lagret i informationssystemer, enheder eller i andre lagringsmedier skal slettes, når der ikke længere er brug for den.</p>	<p>Vi har inspiceret procedure for sletning af information.</p> <p>Vi har inspiceret dokumentation for, at informationssystemer er konfigureret til automatisk sletning af information.</p> <p>Vi har inspiceret dokumentation for, at automatiske sletningsfunktioner har været anvendt i perioden.</p>	Ingen afvigelser konstateret.
8.12	<p><i>Forebyggelse af datalækage</i></p> <p>Der skal benyttes tiltag til at forebygge datalækage i systemer, netværk og andre enheder, der behandler, lagrer eller transmitterer følsom information.</p>	<p>Vi har inspiceret procedure for forebyggelse af datalækage.</p> <p>Vi har inspiceret dokumentation for, at teknologiske foranstaltninger til forebyggelse af datalækage er implementeret.</p>	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	<p><i>Backup af information</i></p> <p>Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.</p>	<p>Vi har inspiceret procedure for backup.</p> <p>Vi har inspiceret, at backup proceduren er opdateret og godkendt.</p> <p>Vi har stikprøvevis inspiceret dokumentation for, at backup gennemføres i henhold til proceduren, herunder rapporter og systemudtræk med status for backup-jobs.</p> <p>Vi har stikprøvevis inspiceret dokumentation for gennemførte restoretests, herunder at backup-data er genskabt succesfuldt, og at den seneste test er gennemført inden for revisionsperioden.</p>	Ingen afvigelser konstateret.
8.14	<p><i>Redundans i faciliteter til informationsbehandling</i></p> <p>Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.</p>	<p>Vi har inspiceret, at der foreligger dokumenterede krav til redundans i systemarkitektur og it-landskab, herunder alternativ lokation for opbevaring af data og backup.</p> <p>Vi har inspiceret dokumentation for implementerede kontroller, der understøtter redundans i komponenter og behandlingsaktiviteter.</p> <p>Vi har inspiceret dokumentation for implementerede redundans foranstaltninger.</p>	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	<p><i>Overvågning af aktiviteter</i></p> <p>Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerhedshændelser.</p>	<p>Vi har inspiceret proceduren for overvågning af aktiviteter.</p> <p>Vi har inspiceret dokumentation for at overvågning er implementeret.</p>	Ingen afvigelser konstateret.
8.17	<p><i>Synkronisering af ure</i></p> <p>Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.</p>	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	<p><i>Brugen af privilegerede understøttende programmer</i></p> <p>Brugen af understøttende programmer, der kan omgå system- og applikationsforanstaltninger, skal begrænses og styres effektivt.</p>	<p>Vi har inspiceret procedure for adgang til privilegerede understøttende programmer.</p> <p>Vi har inspiceret, at adgangen til privilegerede understøttende programmer er begrænset teknisk og at procedurer er etableret.</p> <p>Vi har inspiceret, at krav til logning af ændringer og forsøg på anvendelse af understøttende programmer er fastlagt, og at ekstraordinære handlinger bliver logget.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
8.19	<p><i>Softwareinstallation i test- og produktionssystemer</i></p> <p>Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallationer i test- og produktionssystemer.</p>	<p>Vi har inspiceret procedure for softwareinstallationer på operativsystemer.</p> <p>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.</p>	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	<p><i>Netværkssikkerhed</i></p> <p>Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.</p>	<p>Vi har inspiceret politikken for netværk og netværksenheder.</p> <p>Vi har inspiceret, dokumentation for at implementering og konkrete sikkerhedsforanstaltninger er dokumenteret gennem tekniske konfigurationer.</p>	Ingen afvigelser konstateret.
8.22	<p><i>Segmentering af netværk</i></p> <p>Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.</p>	<p>Vi har inspiceret netværkssikkerhedspolitikken.</p> <p>Vi har inspiceret, at netværket er segmenteret i flere zoner, herunder DMZ, gæstenetværk og interne netværk.</p>	Ingen afvigelser konstateret.
8.23	<p><i>Webfiltrering</i></p> <p>Adgang til eksterne websites skal styres for at reducere eksponering for skadeligt indhold.</p>	<p>Vi har inspiceret, at webfiltreringsmekanismer er etableret og at tekniske begrænsninger forhindrer adgang til forbudte websider.</p> <p>Vi har inspiceret, at opdateret liste over blokerede eksterne websider.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
8.24	<p><i>Brug af kryptografi</i></p> <p>Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.</p>	<p>Vi har inspiceret politik for brug af kryptografi</p> <p>Vi har inspiceret, at information beskyttes i henhold til politikken for kryptografi, og at konfigurationsrapporter samt compliance-rapporter bekræfter opfyldelse af politikken.</p> <p>Vi har inspiceret VPN-konfigurationer, som dokumenterer brugen af stærke krypteringsalgoritmer til beskyttelse af data-trafik.</p>	Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger

Kontrolmål: At sikre at informationssikkerhed er udviklet og implementeret indenfor rammerne af den sikre udviklingslivscyklus.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
8.25	<p><i>Sikker udviklingslivscyklus</i></p> <p>Der skal fastlægges og anvendes regler for sikker udvikling af software og systemer.</p>	<p>Vi har inspiceret procedure for sikker udvikling.</p> <p>Vi har inspiceret, at proceduren er opdateret og godkendt af ledelsen i revisionsperioden.</p>	Ingen afvigelser konstateret.
8.26	<p><i>Krav til applikationssikkerhed</i></p> <p>Informationssikkerhedskrav skal identificeres, specificeres og godkendes ved udvikling eller anskaffelse af applikationer.</p>	<p>Vi har inspiceret procedure for sikker udvikling.</p> <p>Vi har forespurgt, hvorvidt der har været udviklingsprojekter i revisionsperioden.</p>	<p>Vi er blevet informeret om at der ikke har været nogen udviklingsprojekter i revisionsperioden.</p> <p>Ingen afvigelser konstateret.</p>
8.27	<p><i>Sikker systemarkitektur og udviklingsprincipper</i></p> <p>Principper for udvikling af sikre systemer skal fastlægges, dokumenteres, vedligeholdes og anvendes i forbindelse med udvikling af informationssystemer.</p>	<p>Vi har inspiceret principper for udvikling af informationssystemer.</p> <p>Vi har inspiceret, at principperne for udvikling af informationssystemer er godkendt.</p> <p>Vi har inspiceret, at principperne er opdateret og vedligeholdt.</p>	Ingen afvigelser konstateret.

Nr.	IT Forum Gruppen A/S' kontrol	Grant Thorntons test	Resultat af test
8.28	<p><i>Sikker programmering</i></p> <p>Principper for sikker programmering skal anvendes ved softwareudvikling.</p>	<p>Vi har inspiceret procedure for softwareudvikling.</p> <p>Vi har forespurgt, hvorvidt der har været udviklingsprojekter i revisionsperioden.</p>	<p>Vi er blevet informeret om at der ikke har været nogen udviklingsprojekter i revisionsperioden.</p> <p>Ingen afvigelser konstateret.</p>

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
8.29	<p><i>Sikkerhedstest under udvikling og godkendelse</i></p> <p>Processer til sikkerhedstest skal defineres og implementeres i udviklingslivscyklussen.</p>	<p>Vi har inspiceret procedurer for sikkerhedstest i udviklingslivscyklussen.</p> <p>Vi har inspiceret dokumentation for at automatiske og manuelle sikkerhedstest er defineret og implementeret.</p> <p>Vi har forespurgt, hvorvidt der har været udviklingsprojekter i revisionsperioden.</p>	<p>Vi er blevet informeret om at der ikke har været nogen udviklingsprojekter i revisionsperioden.</p> <p>Ingen afvigelser konstateret.</p>
8.31	<p><i>Adskillelse af udviklings- test- og produktionsmiljøer</i></p> <p>Udviklings-, test- og produktionsmiljøer skal adskilles og sikres.</p>	<p>Vi har inspiceret proceduren for adskillelse af udviklings-, test- og produktionsmiljøer.</p> <p>Vi har inspiceret at der er etableret adskillelse af pligter mellem medarbejdere med adgang til udviklings-, test- og produktionsmiljøer.</p>	<p>Ingen afvigelser konstateret.</p>
8.32	<p><i>Ændringsstyring</i></p> <p>Ændringer til informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.</p>	<p>Vi har inspiceret proceduren for ændringsstyring.</p> <p>Vi har stikprøvevis inspiceret at ændringer til systemer er blevet implementeret efter proceduren, herunder at de er planlagt, godkendt og testet.</p>	<p>Ingen afvigelser konstateret.</p>

PENNEO

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

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

Mikael Elling

Underskriver 1

Serienummer: c3427568-ee5d-430b-8da2-80dac2bcd7bb7

IP: 185.108.xxx.xxx

2026-03-30 12:36:11 UTC



Andreas Moos

Grant Thornton, Godkendt Revisionspartnerselskab CVR:
34209936

Underskriver 2

Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035

IP: 62.243.xxx.xxx

2026-03-30 13:20:52 UTC



Kristian Randløv Lydolph

Underskriver 3

Serienummer: 7b9e0bc5-648f-4c07-87a8-debb5e403de6

IP: 80.71.xxx.xxx

2026-03-30 16:38:47 UTC



Penneo dokumentnøgle: VHGNE-TV5X8-S4UEQ-RYL95-039XV-5DRBV

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.