Revisorerklæring

Softværket a.m.b.a.

ISAE 3402 type 1 erklæring om generelle it-kontroller relateret til drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF pr. 30. september 2024

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

November 2024

Indholdsfortegnelse

Sektion 1: Softværkets udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Softværkets ydelser i forbindelse med drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF 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.

Softværket anvender underleverandørerne team.blue Denmark A/S og Microsoft. Denne erklæring er udarbejdet efter partielmetoden, og Softværkets kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandørerne. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og fungerer effektivt. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Softværkets beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos Softværket. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og implementeringen af disses komplementerende kontroller.

Softværket bekræfter, at:

(a) Den medfølgende beskrivelse i sektion 3, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Softværkets drift af drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF pr. 30. september 2024.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

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

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

(ii) 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 udformet pr. 30. september 2024, hvis relevante kontroller hos underleverandøren var operationelt effektive, og kunderne har udført de komplementerende kontroller, som forudsættes i designet af Softværkets kontroller pr. 30. september 2024. Kriterierne for denne udtalelse var, at:

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

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

Kolding, den 1. november 2024
Softværket a.m.b.a.

Jan Elmstrøm Blaabjerg
Direktør

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

Til Softværket, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Softværkets beskrivelse i Sektion 3 af generelle it-kontroller for drift af brugersystemer til behandling af Softværkets drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, pr. 30. september 2024 og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Softværket anvender underleverandørerne team.blue Denmark A/S og Microsoft. Denne erklæring er udarbejdet efter partielmetoden, og Softværkets kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandørerne. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af Softværkets kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Softværket.

Enkelte af de kontrolmål, der er anført i Softværkets beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos Softværket. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og implementeringen af disses komplementerende kontroller.

Softværkets ansvar

Softværket 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 Softværkets 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 udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes udformning.

De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller implementeret. 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

Softværkets 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 Softværkets udtalelse i Sektion 1. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret pr. 30. september 2024, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 30. september 2024, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis kunderne har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Softværkets kontroller pr. 30. september 2024.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i Sektion 4 er udelukkende tiltænkt kunder, der har anvendt Softværket drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, 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, 1. november 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Director, CISA, CISM

Sektion 3: Beskrivelse af Softværkets ydelser i forbindelse med drift af it-hosting løsningen Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF og generelle it-kontroller relateret hertil

Formål

Hensigten med denne kontrolbeskrivelse er at tilkendegive over for alle, som har en relation til Softværket, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Softværket ønsker at opretholde og løbende udbygge et IT-sikkerhedsniveau på højde med de krav, som skitseres i ISO 27002. Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Softværket fremstår troværdigt. For at fastholde Softværkets troværdighed skal det sikres, at information behandles med fornøden fortrolighed, og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer og data betragtes, næst efter medarbejderne, som Softværkets mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, sikkerhed, høj kvalitet, overholdelse af lovgivningskrav, og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Softværkets image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Alle personer betragtes som værende potentiel årsag til et muligt brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

På de efterfølgende sider behandles de enkelte punkter, der læner sig op ad rækkefølgen i ISO 27002.

Bemærk at dokumentation i ISO 27002 starter med punkt 4, da punkt 1 til 3 er indledende bemærkninger.

4 - Risikovurdering og -håndtering

Softværket har en procedure for løbende risikovurdering af udvikling og vedligeholdelse af hostingmiljøet og Forsyning|FOF. Dermed kan Softværket sikre, at de risici, som er forbundet med hostingmiljøet samt udvikling og vedligeholdelsen af Forsyning|FOF, er minimeret til et acceptabelt niveau.

Risikovurdering opdateres en gang årligt, samt når der foretages større ændringer i udviklingen eller vedligeholdelsen, som vurderes relevante i forhold til at revurdere den generelle risikovurdering. Alle risici bliver inddelt i kategorierne Grøn, Gul og Rød. Ledelsen i Softværket forholder sig til alle risici i alle kategorier.

IT-sikkerhedsudvalget og den samlede ledergruppe har det overordnede ansvar for implementering af korrigerende handlinger for at minimere de identificerede risici.

5 - Sikkerhedspolitik

IT-sikkerhedspolitikken gennemgås en gang årligt. Denne gennemgang ligger som en fast opgave i årshjulet for IT-sikkerhedsudvalget.

6 - Organisering af informationssikkerhed

Der er skarp funktionsadskillelse, hvilket betyder, at det kun er udviklere, der kan tilgå og ændre i kildekode og programmers funktionalitet. Ligeledes er det kun ansatte hos vores hosting partnere, Teknisk Support, Infrastruktur, GIS- og udviklingsafdelingen, der i samarbejde har adgang til at ændre i hostingmiljøet, der kan påvirke driftsstabiliteten.

Kunder har kun adgang til egne data. Brugerne er oprettet som navngivne brugere og anvender personligt brugernavn og password. Adgang til produktionsdata, sker via en krypteret forbindelse.

Den enkelte medarbejder har ikke direkte adgang til produktionsserverne fra egen PC. Er det nødvendigt at tilgå produktionsdata for at yde support eller fejlfinde, sker dette igennem RDS, Microsofts Partner Portal eller TeamViewer, hvor der er sporbarhed af, hvem der logger på.

7 - Sikkerhed i forhold til HR

Eksterne konsulenter skal underskrive en fortrolighedserklæring inden de får adgang til hosting- eller udviklingsmiljøet. Softværket anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne it-sikkerhedsprocedurer er en del af standardaftalen.

Alle medarbejdere i Softværket har underskrevet en fortrolighedserklæring i forbindelse med ansættelseskontrakten, og er instrueret i håndtering af fortrolige oplysninger. Denne fortrolighed er også gældende ved ophør af ansættelsen. Brud på sikkerhedspolitikken kan medføre en opsigelse af ansættelsesforholdet.

8 - Styring af aktiver

Alle data i hostingmiljøet er håndteret som fortrolige kundedata. Alle medier indeholdende kundedata skal behandles med største omhu. Det bliver registreret, hvilket databærende udstyr en medarbejder får udleveret, og ved ophør af ansættelsesforholdet bliver alt udstyr inddraget.

Ligesom med systemdata, opererer Softværket med systemejere, der er ansvarlig for forskellige aktiver. Herigennem sikrer vi individuel fokus på sikkerheden i alle delelementer.

Alt databærende udstyr destrueres og bortskaffes på ansvarlig vis.

Al kildekode og programmer, der udvikles, er Softværkets ejendom, og må ikke kopieres eller overdrages til tredjepart.

9 – Adgangskontrol

Det er Teknisk Support og Infrastruktur, der har adgang til at oprette nye brugere, og alle medarbejderne her er instrueret i håndtering af kundernes brugernavn og kodeord.

Det er kun Teknisk Support og Infrastruktur, der har adgang til at oprette nye brugere og roller i databaserne samt ændre passwords.

Oprettelse og lukning af brugere sker udelukkende via skriftlig henvendelse, og efter at identitet er blevet bekræftet. Alle brugere oprettes med et stærkt kodeord, der for hostingbrugere skal skiftes mindst en gang årligt og 2 gange årligt for medarbejdere i Softværket. Softværket tilstræber at følge anbefalingerne fra Center For Cybersikkerhed omkring kodeord.

Der er yderligere sikring af kunders data ved, at en konto automatisk bliver spærret ved 5 på hinanden følgende fejl i indtastning af kodeord. Dette er for at forhindre, at man kan gætte sig frem til et kodeord. Der er også sat flere interne kontroller op til at registrere eventuelt misbrug af rettigheder i hostingmiljøet. Forsyning|Hosting benytter 2-faktor login.

Brugerrettigheder gennemgås en gang årligt. Denne gennemgang ligger som en fast opgave i årshjulet for IT-sikkerhedsudvalget.

10 - Kryptografi

Al adgang til Hostingmiljøet sker via en krypteret forbindelse.

Softværket anvender et krypteret system til opbevaring af administrative kodeord.

Kommunikation af følsomt og fortroligt data sker via sikker mail.

Softværket holder sig løbende opdateret på krypterings-teknologier/protokoller.

11 - Fysiske og miljømæssige sikringer

Fysisk adgang til bygningen via hovedindgang er overvåget af en reception. Alle andre indgange er låst med en elektronisk lås uden for normal åbningstid.

Adgang til serverrum er også sikret med elektronisk lås, og serverne er yderligere beskyttet af et metalgitter med elektronisk lås. Eksterne konsulenter har kun ledsaget adgang til serverrum. Alle lokaler er monteret med tyverialarm, og der er brandslukningsudstyr i serverrummet. Derudover er der UPS-anlæg i serverrummet, som sikrer mod kortvarigt strømudfald.

For Forsyning|Hostings og Forsyning|FOFs vedkommende sikres den fysiske og organisatoriske sikkerhed via de indgåede aftaler med underleverandørerne.

Der tages daglig backup af alle data i hostingmiljøet, og hver nat føres en kopi af data fra Softværket Hosting til en sikret sekundær lokation. For den del af Forsyning|FOF, der er placeret hos Microsoft, er backup-proceduren jf. Microsofts standard. Samme procedure er gældende for Softværkets interne miljø.

12 - Sikkerhed i forbindelse med drift

Softværket opererer med dobbeltroller på udvalgte systemer, som sikrer personuafhængighed. Desuden er der en fyldestgørende systemdokumentation, som løbende opdateres.

Aktiv overvågning sikrer kapacitetsstyring i hostingmiljøet, af både hosting-partner og Softværket.

Sikkerhed i hostingmiljøet sker primært ved at brugerne har begrænsede rettigheder. Det er ikke muligt selv at installere programmer. Hele systemet er desuden sikret via firewall og ved begrundet mistanke overvåges netværkstrafik.

Logning i forbindelse med Forsyning|Hosting sker via logningsbokse fra SektorCert. Herfra overvåges ind- og udgående trafik til et samlet nationalt overvågningsbillede.

13 - Kommunikationssikkerhed

Sikkerhed af vores netværk er af højeste prioritet. Alt er sikret via firewall, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværket. Disse opbevares sammen med systemdokumentationen.

Der er opsat overvågning og logning af netværkstrafik. Alene godkendt netværkstrafik kommer gennem vores firewall. Dette gælder både indgående og udgående trafik.

Der er en segmentering af netværket, afhængigt af funktionsbehov.

Softværket overfører ikke, medmindre det konkret er aftalt, kunders data eller dele deraf til tredjepart. Der er etableret fortrolighedsaftaler for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.

14 - Anskaffelse, udvikling og vedligeholdelse

Der er fastsatte procedurer ifm. egen udvikling og indkøb/implementering af software. Disse dækker over procedurer, før-, under og efter idriftsættelse.

Udvikling af Forsyning|FOF forestås primært af Softværkets udviklingsafdeling samt Microsofts Business Central Cloud-løsning.

Der foreligger en procesbeskrivelse for brug af testdata, så data bliver anonymiseret og ikke er personhenførbare.

15 - Leverandørforhold

Der er fortrolighedserklæringer med alle konsulenter der får adgang til systemet. Som udgangspunkt arbejder de udelukkende med hard- og softwareproblemstillinger, stillet af Softværket.

Softværket anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne it-sikkerhedsprocedurer er en del af standardaftalen.

Softværket har delvist uddelegeret driften for hostingmiljøet til hosting-partnere. Softværket har selv driftsansvaret for eget servermiljø hos Softværket.

Softværket fører tilsyn med underleverandører ud fra en risikobaseret vurdering af de enkelte underleverandører. Tilsynet kan foretages ved gennemlæsning af revisionserklæringer, ISO-standard-certifikater, fysiske besøg eller i kombination.

16 - Styring af sikkerhedshændelser

Softværket har klare procedurer for alle sikkerhedshændelser, herunder som beskrevet i interne beredskabsplaner.

Alle hændelser bliver registret og løst uden ophold. Det er IT sikkerhedsudvalget, der har det overordnede ansvar for processen.

17 - Informationssikkerhedsaspekter ved beredskabsstyring

Katastrofer forsøges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici holdt op imod sikringsomkostninger. Softværket har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.

Softværket beredskabsplan omfatter:

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

Softværket har implementeret formelle nødplaner, og procedurer til beredskab for alle punkter. Både Softværket og hosting partner har redundans i alle kritiske netværkskomponenter. Derudover refereres der til hosting-partnerens IT-revisionserklæring.

18 - Overensstemmelse

Hverken Softværket eller vores kunder, er underlagt særlig lovgivning i forhold til vores ydelse. Softværket er dog opmærksom på, at lovændringer kan medføre behov for at revurdere nogle af selskabets procedurer og retningslinjer for opbevaring af data.

En gang årligt gennemgås den gældende sikkerhedspolitik af IT-sikkerhedsudvalget. Yderligere gennemgange foretages i forbindelse med større ændringer i organisationen eller hostingmiljøet.

Det er IT-sikkerhedsudvalget, der har det overordnede ansvar for IT-sikkerhedspolitikken.

Der foretages evalueringen af en ekstern it-revisor samt i forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer.

Kvalitetssikring af Forsyning|FOF

I Softværket er fundamentet for test og kvalitetssikring af Forsyning|FOF, at alle udviklingsopgaver gennemgår både manuelle og automatiserede tests, inden de frigives i en ny release.

Der kan dog være opgaver, der falder under vores klart definerede "bagatelgrænse." Disse omfatter mindre ændringer, såsom UI-justeringer eller opdateringer, der ikke påvirker kernefunktionaliteten, samt funktioner frigivet af Microsoft, hvor vi antager, at Microsoft allerede har gennemført omfattende intern test i overensstemmelse med deres officielle dokumentation. Sådanne opgaver kan undtages fra yderligere testning baseret på en risikovurdering.

Der anvendes en risikobaseret teststrategi for at sikre, at vores testindsats fokuserer på de mest kritiske områder af systemet. Risikoen for hver opgave vurderes løbende, og disse vurderinger gennemgås regelmæssigt for at sikre, at de forbliver præcise og relevante.

Processen for risikovurdering og ansvarsfordeling er klart defineret for at opretholde transparens og ensartethed.

Komplementerende kontroller

De forhold som Softværkets kunder antages at være ansvarlige for, både de indlysende og jf. Softværkets forretningsvilkår/SLA.

Softværkets kunder er, medmindre andet er aftalt, ansvarlige for selv at etablere en tilstrækkelig forbindelse til Softværkets hostingmiljø.

Herudover er Softværkets kunder, medmindre andet er aftalt, ansvarlige for:

- At det aftalte niveau for backup dækker kundens behov
- Eget sikkerhedsniveau, beredskab, backup, løbende opdateringer, drift osv., såfremt de ikke benytter Forsyning|Hosting

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 Softværkets kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Softværkets underleverandører.

Kontroller udført hos Softværkets 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 Softværket. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover inspiceres dokumentation for at kontrollen er implementeret.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af Grant Thornton som grundlag for vurdering af de generelle it-kontroller hos Softværket

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed
Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
5.1.1	*Politikker for informationssikkerhed* Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Vi har inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter. Vi har inspiceret, at informationssikkerhedspolitikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
5.1.2	*Gennemgang af politikker for informationssikkerhed* Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken. Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

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

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
6.1.1	*Roller og ansvarsområder for informationssikkerhed* Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret et organisationsdiagram for informationssikkerhedsorganisationen. Vi har inspiceret, at strukturen er tilstrækkelig til at styre implementeringen og driften af informationssikkerhed. Vi har inspiceret beskrivelse af roller og ansvarsområder i informationssikkerhedsorganisationen.	Ingen afvigelser konstateret.
6.1.2	*Funktionsadskillelse* Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har inspiceret dokumentation for adskillelse af funktioner. Vi har inspiceret overordnet organisationsdiagram for organisationen.	Ingen afvigelser konstateret.
6.1.3	*Kontakt med myndigheder* Der opretholdes passende kontakt med relevante myndigheder.	Vi har inspiceret dokumentation for, at der er retningslinjer for passende kontakt med myndigheder. Vi har inspiceret dokumentation for, at der er opretholdt passende kontakt med relevante myndigheder.	Ingen afvigelser konstateret.
6.1.4	*Kontakt med særlige interessegrupper* Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Vi har inspiceret proceduren vedrørende vedligeholdelse af reglerne for passende kontakt med særlige interessegrupper, faglige sikkerhedsfora og faglige organisationer. Vi har inspiceret dokumentation for, at der er opretholdt passende kontakt med særlige interessegrupper.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
6.2.2	*Fjernarbejdspladser* Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.	Vi har inspiceret politik for sikring af fjernarbejdspladser. Vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har inspiceret proceduren for ansættelse af nye medarbejdere. Vi har inspiceret dokumentation for at seneste tiltrådte medarbejder er blevet orienteret omkring rolle samt ansvar ved informationssikkerhed.	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
7.2.1	*Ledelsesansvar* Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har inspiceret informationssikkerhedspolitikken vedrørende fastsættelse af krav til medarbejdere og kontrahenter. Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde informationssikkerhedspolitikken i ansættelseskontrakterne med medarbejderne.	Ingen afvigelser konstateret.
7.2.2	*Bevidsthed om, uddannelse og træning i informationssikkerhed* Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter vil ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, idet omfang det er relevant for deres jobfunktion.	Vi har inspiceret procedurer til sikring af tilstrækkelig uddannelse og træning i informationssikkerhed (awarenesstræning). Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejderne. Vi har inspiceret, at alle medarbejdere har deltaget i awarenesstræning.	Ingen afvigelser konstateret.
7.2.3	*Sanktioner* Der er etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret til medarbejdere og kontrahenter. Vi har inspiceret, at sanktionsprocessen er en del af ansættelseskontrakten, for den seneste tiltrådte medarbejder.	Ingen afvigelser konstateret.

A.7.3 Ansættelsesforholdets ophør eller ændring Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
7.3.1	*Ansættelsesforholdets ophør eller ændring* Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har forespurgt til medarbejderes og kontrahenters forpligtelser til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse eller kontrakt. Vi har inspiceret dokumentation for at informationssikkerhedsansvar og -forpligtelser ved ansættelsens ophør eller ændring er defineret og kommunikeret. Vi har inspiceret, at seneste fratrådte medarbejder er informeres om stadigt gældende tavshedspligt ved fratrædelse.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

A.8.1 Ansvar for aktiver Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
8.1.1	*Fortegnelse over aktiver* Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har inspiceret fortegnelser over aktiver.	Ingen afvigelser konstateret.
8.1.2	*Ejerskab af aktiver* Der udpeges en ejer i organisationen for hvert aktiv.	Vi har inspiceret oversigt over ejerskab til aktiver.	Ingen afvigelser konstateret.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
8.1.3	*Accepteret brug af aktiver* Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres.	Vi har inspiceret reglerne for accepteret brug af aktiver.	Ingen afvigelser konstateret.
8.1.4	*Tilbagelevering af aktiver* Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	Vi har inspiceret proceduren til sikring af tilbagelevering af udleverede aktiver. Vi har inspiceret, at aktiver er inddraget for seneste fratrådte medarbejder.	Ingen afvigelser konstateret.

A.8.2 Klassifikation af information Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.			
Nr.	**Softværkets kontrol**	**Grant Thorntons test**	**Resultat af test**
8.2.3	*Håndtering af aktiver* Der udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Vi har inspiceret procedurer for håndtering af aktiver. Vi har inspiceret dokumentation for, at aktiver håndteres jf. proceduren.	Ingen afvigelser konstateret.

A.8.3 Mediehåndtering Kontrolmål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
8.3.1	*Styring af flytbare medier* Der er implementeret procedurer til styring af flytbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget.	Vi har inspiceret at procedurer for styring af bærbare medier stemmer overens med det vedtagne klassifikationssystem.	Ingen afvigelser konstateret.
8.3.2	*Bortskaffelse af medier* Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.	Vi har inspiceret procedurer for bortskaffelse af medier. Vi har inspiceret, at medier bortskaffes i overensstemmelse med procedurerne for den senest udførte bortskaffelse.	Ingen afvigelser konstateret.
8.3.3	*Transport af fysiske medier* Medier, der indeholder information beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.	Vi har inspiceret procedurer for beskyttelse af medier under transport.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

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

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
9.1.1	*Politik for adgangsstyring* En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret politikken for adgangsstyring. Vi har inspiceret at politikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
9.1.2	*Adgang til netværk og netværkstjenester* Brugere har kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret udtræk over brugere med adgang til netværk og netværkstjenester. Vi har inspiceret, at adgange er tildelt baseret på et arbejdsbetinget behov for medarbejdere.	Ingen afvigelser konstateret.

A.9.2 Administration af brugeradgang Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
9.2.1	*Brugerregistrering-og afmelding* Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder. Vi har inspiceret, at seneste bruger der er tildelt adgangsrettigheder, er godkendt jf. proceduren. Vi har inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har inspiceret, at seneste tildelte brugeradgange er blevet tildelt efter proceduren for adgangsstyring og kontrol.	Ingen afvigelser konstateret.
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder. Vi har inspiceret et udtræk af privilegerede brugere og vi har forespurgt om adgangsrettigheder er tildelt baseret på et arbejdsbetinget behov. Vi har inspiceret at privilegerede brugeradgange er personhenførbare. Vi har inspiceret, at der periodisk foretages gennemgang af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret procedure for regelmæssig gennemgang og evaluering af adgangsrettigheder. Vi har inspiceret, at der foretages gennemgang og evaluering af adgangsrettigheder med jævne mellemrum.	Ingen afvigelser konstateret.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
9.2.6	*Inddragelse eller justering af adgangsrettigheder* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder. Vi har inspiceret at fratrådte medarbejdere har fået deres adgangsrettigheder inddraget rettidigt.	Ingen afvigelser konstateret.

A.10 Kryptografi

A.10.1 Kryptografiske kontroller
Kontrolmål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
10.1.1	*Politik for anvendelse af kryptografi* Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har inspiceret politik for anvendelse af kryptering. Vi har inspiceret oversigt over opdatering og gennemgang af politikker samt proceduren, hvoraf politikken for kryptografi fremgår.	Ingen afvigelser konstateret.
10.1.2	*Administration af nøgler* Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at krypteringsnøgler er aktive samt at der følges op på, hvornår de skal fornyes.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

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

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til kontoret. Vi har inspiceret at der er opsat alarmsystemer til fysisk adgangskontrol.	Ingen afvigelser konstateret.
11.1.3	*Sikring af kontorer, lokaler og faciliteter* Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret.	Vi har stikprøvevis inspiceret, at der er etableret fysisk sikring af kontorer, lokaler og faciliteter. Vi har inspiceret, at der foretages inspektion af brandslukningsudstyr.	Ingen afvigelser konstateret.

A.11.2 Udstyr
Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
11.2.5	*Fjernelse af aktiver* Udstyr, information og software bliver ikke fjernet fra organisationen uden forudgående tilladelse.	Vi har inspiceret retningslinjer for fjernelse af udstyr, information og software fra virksomheden.	Ingen afvigelser konstateret.
11.2.9	*Politik for ryddeligt skrivebord og blank skærm* Der er udarbejdet en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.	Vi har inspiceret politik for ryddeligt skrivebord og blank skærm.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

A.12.2 Malwarebeskyttelse
Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
12.2.1	*Kontroller mod malware* Det er implementeret kontroller til detektering, forhindring og gendannelse med henblik på at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har inspiceret retningslinjer for kontroller mod malware. Vi har inspiceret, at der er implementeret kontroller mod malware.	Ingen afvigelser konstateret.

A.12.3 Backup
Kontrolmål: At beskytte mod tab af data

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
12.3.1	*Backup af information* Der bliver taget backupkopier af information, software og systembilleder, og disse bliver testet regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har inspiceret dokumentation for at proceduren for backup er gennemgået og opdateret. Vi har inspiceret dokumentation for senest udførte backup. Vi har inspiceret dokumentation for at der er udført en restoretest.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware
Kontrolmål: At sikre integriteten af driftssystemer.

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
12.5.1	*Softwareinstallation i driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret retningslinjer for installation af software på driftssystemer. Vi har stikprøvevis inspiceret, at retningslinjerne efterleves.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
12.6.1	*Styring af tekniske sårbarheder* Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder evalueres og der er iværksat passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder. Vi har stikprøvevis inspiceret at servere, databasesystemer og netværkskomponenter er patchet rettidigt.	Ingen afvigelser konstateret.
12.6.2	*Begrænsninger på softwareinstallation* Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.	Vi har inspiceret dokumentation for at der er begrænsninger for almene brugere på installation af software. Vi har inspiceret dokumentation for at almene brugere bliver nægtet dette, ved forsøg på installation.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

A.13.1 Styring af netværkssikkerhed Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.			
Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
13.1.2	*Sikring af netværkstjenester* Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.	Vi har inspiceret at leverandøraftaler indeholder aftale omkring et passende niveau af sikring på netværket. Vi har inspiceret dokumentation for at der er implementeret sikkerhedsforanstaltninger når netværket tilgås udefra. Vi har inspiceret dokumentation for at der føres kontrol med hvilke adgange der er i netværket for leverandører og services.	Ingen afvigelser konstateret.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
13.1.3	*Opdeling af netværk* Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret netværksdiagrammer, hvoraf det fremgår at der er adskillelse af udviklings-, test- og driftsmiljøer.	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel
Kontrolmålet: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
13.2.4	*Fortroligheds- og hemmeligholdelsesaftaler* Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres.	Vi har inspiceret skabelon for fortrolighedsaftale med eksterne parter. Vi har inspiceret dokumentation for, at ved brug af ekstern part, er afsnit om tavshedspligt beskrevet i kontrakten. Vi har inspiceret dokumentation for, at skabelon til fortrolighedsaftaler gennemgås regelmæssigt.	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

A.14.2 Sikkerhed i udviklings- og hjælpeprocesser
Kontrolmål: At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
14.2.2	*Procedurer for styring af systemændringer* Ændringer af systemer inden for udviklingslivscyklussen styres ved hjælp af formelle procedurer for ændringsstyring.	Vi har inspiceret at proceduren for Change Management indeholder krav om: • Risikovurdering • Test • Godkendelse Vi har inspiceret at seneste implementerede ændring følger ændringsprocessen.	Ingen afvigelser konstateret.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
14.2.3	*Teknisk gennemgang af applikationer efter ændringer af driftsplatforme* Ved ændring af driftsplatforme gennemgås forretningskritiske applikationer og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.	Vi har forespurgt til procedure for teknisk gennemgang af applikationer efter ændringer af driftsplatforme. Vi har inspiceret, at seneste ændring til operativsystemer og infrastruktur er blevet vurderet m.h.t. deres eventuelle konsekvenser for applikationssystemer inden de er blevet gennemført.	Ingen afvigelser konstateret.
14.2.4	*Begrænsning af ændringer af softwarepakker* Ændringer i softwarepakker er vanskeliggjort og begrænset til nødvendige ændringer, og alle ændringer styres effektivt.	Vi har forespurgt vedrørende procedure for begrænsning af ændringer af softwarepakker. Vi har inspiceret hvordan begrænsninger af ændringer i softwarepakker er implementeret.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

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

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
15.2.1	*Overvågning og gennemgang af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har inspiceret, at proceduren for styring af leverandører og serviceaftaler indeholder krav til årlig overvågning og gennemgang af serviceydelser leveret af underleverandører, er i overensstemmelse med det aftalte. Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører.	Ingen afvigelser konstateret.
15.2.2	*Styring af ændringer i leverandørydelser* Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, - procedurer og -kontroller, styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, - systemer og -processer er, og til en revurdering af risici.	Vi har forespurgt til styring af ændringer hos leverandører og inspiceret dokumentation for håndteringen.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

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

Nr.	*Softværkets kontrol*	*Grant Thorntons test*	*Resultat af test*
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har inspiceret proceduren for håndtering af sikkerheds-hændelser. Vi har inspiceret at proceduren er gennemgået og opdateret.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedshændelser. Vi har inspiceret, at seneste informationssikkerhedshæn-delse er rapporteret ad passende ledelseskanaler.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger orga-nisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observe-rede svagheder eller mistanke om svagheder i in-formationssystemer og -tjenester.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedssvagheder. Vi har stikprøvevis inspiceret, at medarbejdere har rapporte-ret svagheder eller mistanke om svagheder i informationssy-stemer og -tjenester.	Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informationssikker-hedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som infor-mationssikkerhedsbrud.	Vi har inspiceret procedure for vurdering af informationssik-kerhedshændelser. Vi har inspiceret, at seneste informationssikkerhedshæn-delse har været håndteret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overens-stemmelse se med de dokumenterede procedurer.	Vi har inspiceret proceduren for håndtering af informations-sikkerhedsbrud. Vi har inspiceret, at seneste informationssikkerhedsbrud har været håndteret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.

Nr.	Softværkets kontrol	Grant Thorntons test	Resultat af test
16.1.6	*Erfaring fra informationssikkerhedsbrud* Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	Vi har forespurgt til hvordan erfaringer fra informationssikkerhedsbrud håndteres. Vi har inspiceret, at erfaringer fra seneste informationssikkerhedsbrud er blevet håndteret.	Ingen afvigelser konstateret.

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

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

Nr.	***Softværkets kontrol***	***Grant Thorntons test***	***Resultat af test***
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	Vi har inspiceret at beredskabsplanen er godkendt af ledelsen.	Ingen afvigelser konstateret.
17.1.2	*Implementering af informationssikkerhedskontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har inspiceret at beredskabsplanen vedligeholdes og opdateres efter behov. Vi har inspiceret dokumentation for at beredskabsplanen er tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
17.1.3	*Verificér, gennemgå og evaluér informationssikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har inspiceret dokumentation for at der er udført tests af beredskabsplanens risikoområder.	Ingen afvigelser konstateret.

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

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

Jan Elmstrøm Blaabjerg
Underskriver 1
Serienummer: 5603c969-4ec3-4b24-a521-1b8723de8e31
IP: 93.165.xxx.xxx
2024-11-01 08:10:43 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2024-11-01 08:14:29 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
På vegne af: Kristian Randløv Lydolph
Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2024-11-01 08:15:57 UTC