

revi-it

et trygt samfund med it og data

v

Revisorerklæring

Emento A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller relateret til drift af online platform for forløbsguides for perioden 1. april 2021 til 31. marts 2022.

REVI-IT A/S | www.revi-it.dk

Højbro Plads 10, 1200 København K

CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk

www.dpo-danmark.dk | www.revi-cert.dk

Maj 2022

Indholdsfortegnelse

Afsnit 1:	Beskrivelse af Emento A/S' ydelser i forbindelse med drift af online platform for forløbsguides samt generelle it-kontroller relateret hertil	1
Afsnit 2:	Emento A/S' udtalelse.....	7
Afsnit 3:	Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet.....	9
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf.....	12

Afsnit 1: Beskrivelse af Emento A/S' ydelser i forbindelse med drift af online platform for forløbsguides samt generelle it-kontroller relateret hertil

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

Kontroller i applikationssystemerne er ikke omfattet af denne erklæring.

Formål

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

Emento A/S ønsker at opretholde og løbende udbygge et IT-sikkerhedsniveau på højde med de krav, som skitseres i ISO 27001. Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretlige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Emento A/S fremstår troværdigt. For at fastholde Emento A/S' 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 Emento A/S' 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 Emento A/S' image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Alle medarbejdere og andre, der udfører arbejde for Emento A/S, er omfattet af sikkerhedsbestemmelserne.

På de efterfølgende sider behandles de enkelte punkter i ISO 27002:2013. Bemærk at dokumentation i ISO 27002 starter med punkt 4, da punkt 1 til 3 er indledende bemærkninger.

Risikovurdering og -håndtering

Risikovurdering og -håndtering sker som en løbende aktivitet i Emento A/S. Her tages stilling til hvorvidt nye aktiver, ændringer i udviklingen eller vedligeholdelse eller ændringer i omverdenen giver anledning til re-vurdering af de nuværende sikkerhedsforanstaltninger.

Risici vurderes ud fra en sammenholdelse af sandsynlighed og konsekvens. Relevante procedurer og dokumenter gennemgås årligt.

Informationssikkerhedspolitik

Informationssikkerhedspolitikken gennemgås en gang årligt og godkendes af ledelsen.

Organisering af informationssikkerhed

Kunder har altid kun adgang til egne data. Kontrol af adgang til data gennemgås periodisk af CTO.

Det er kun ansatte med fornødne roller og rettigheder, der har adgang til kildekode, der desuden opbevares i eksternt depot. Opsætning og administration af testmaskiner, build-servere, bastion-servere, m.m. administreres via fornødne roller og rettigheder.

Funktioner i Emento A/S er delt op i 3 niveau: Strategisk, taktisk og operationelt. I tillæg har Emento A/S udpeget en DPO. I diverse procedurer og i nærværende dokument henvises også til rollen, generalsekretær, som er samme person som DPO.

En gang om måneden afholdes et årshjulsmøde, hvor det strategiske, taktiske og operationelle niveau samt DPO'en/generalsekretæren mødes og gennemgår relevante kontroller og laver en løbende vurdering af behov for korrektioner eller iværksættelse af nye tiltag.

Alt kommunikation med myndigheder eller interessegrupper varetages af det strategiske niveau.

Korrekt funktionsadskillelse kontrolleres en gang årligt af generalsekretæren og bestyrelsen.

Sikkerhed i forhold til HR

Inden ansættelse: Der skal som minimum altid deltage mindst 2 fra Emento A/S i samtaler med kandidater, ligesom der potentielt kan gennemføres check af kandidater omfattende referencer, CV, uddannelsesmæssige kvalifikationer samt straffeattest. Straffeattest skal altid tjekkes.

Det er kun ledelsen, der kan verificere kandidaters straffeattest og straffeattester opbevares ikke. Emento A/S indhenter alle kandidaters samtykke til at indhente referencer.

Under ansættelse: Alle medarbejdere i Emento A/S og leverandører, som udfører arbejde på vegne af Emento A/S, har underskrevet en fortrolighedserklæring og er instrueret i håndtering af informationssikkerhed og fortrolige oplysninger.

Det sker løbende tildeling af roller og rettigheder i forbindelse med ansættelser samt fjernelse heraf ved opsigelser. CTO udfører mindst en gang årligt stikprøver for at sikre at retningslinjer omkring roller og rettigheder følges.

Brud på informationssikkerhedspolitikken kan medføre en sanktion overfor den ansatte.

Ved ophør af ansættelsesforhold er fortrolighed også gældende.

Kontrol af at proces for ansættelse er fulgt sker løbende af ledelsen.

Styring af aktiver

Information skal håndteres i henhold til Information Classification policy.

Alle databærende aktiver er registreret med ejer og unik ID. Ligeledes er alle forretningskritiske funktioner og processer identificeret, og der er udpeget systemejere herfor. CTO vedligeholder liste over samtlige informationssystemer.

Bærbare enheder må ikke efterlades synligt i biler og skal medbringes som håndbagage på flyrejser.

Al information klassificeres på 4 forskellige niveauer. Det strategiske niveau har ansvar for klassificeringen.

Såfremt fortrolige data opbevares på mobile enheder, beskyttes data med passende sikkerhedsprodukter godkendt af de operationelle niveauer.

Netværksforbindelse til IT administrative formål krypteres altid.

Ved bortskaffelse af datamedier bliver disse sikkerhedslettet inden bortskaffelse.

Korrekt håndtering af aktiver verificeres minimum en gang årligt af Generalsekretæren.

Adgangskontrol

Adgangen til at udføre handlinger på Emento A/S' IT-systemer beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, fejl og svindel. CTO har ansvaret for at sikre informationssikkerheden i forbindelse med adgang til Emento A/S' systemer.

Der er etableret procedurer for tildeling og inddragelse af rettigheder.

Adgang til interne netværk fra et eksternt netværk går igennem Emento A/S' VPN og benytter 2 faktor godkendelse.

Gæster hos Emento A/S har adgang til et gæstenetværk, som ikke giver adgang til Emento A/S' interne systemer. Kildekode til Emento A/S' systemer ligger i eksternt depot og kun autoriserede personer har adgang hertil.

Emento A/S anvender 1Password til opbevaring af alle adgangskoder, og disse er inddelt i vaults iht. definerede roller med tilhørende adgange. 1Password anvendes ligeledes til generering af passwords, således at minimumskrav til udformning af passwords altid overholdes.

Det er kun udvalgte medarbejdere, der har adgang til at oprette nye brugere samt tildele og ændre passwords i Emento A/S' systemer. Alle medarbejderne er instrueret i håndtering af adgange.

Emento A/S' kunder er selv ansvarlige for egen brugeradministration enten via eget AD eller ved brug af Emento A/S' brugeradministrationssystem.

Udvalgte medarbejdere hos Emento A/S har rettigheder til at logge på alle systemer ifm. support. Det er ikke muligt for kunderne selv at lave ændringer i driftsmiljøerne.

Generalsekretæren verificerer en gang årligt at procedurer for adgangskontrol er fulgt.

Kryptografi

Det operationelle niveau skal løbende tage stilling til behov og regler for brug af kryptografiske kontroller og kryptografiske nøgler med henblik på at sikre fortrolighed, integritet og uafviselighed af informationer.

Al adgang til Emento A/S' produktionsmiljøer sker via TLS 1.2. Adgang til driftsmiljøer sker via HTTPS over en bastion-server med personlige certifikater. Alle data i databaser opbevares på krypterede og fragmenterede SAN diske.

Emento A/S anvender en krypteret ekstern service til password opbevaring til sikring af sikre kodeord, filer, certifikater m.m. Alle medarbejdere er instrueret i brugen af og vigtighed af anvendelse af denne service.

Er der behov for mailkommunikation med personfølsomme data, fx. i forbindelse med ansættelser, anvendes S/MIME krypteret service fra Permido til dette.

Generalsekretæren kontrollerer krypteringen en gang årligt.

Fysisk og miljømæssig sikring

Alle indgange til Emento A/S' kontor og netværksrum er beskyttet med fysisk adgangskontrol. Adgang til netværk er yderligere beskyttet af et aflåst skab. Generalsekretæren verificerer en gang årligt, hvem der har fysisk adgang til Emento A/S' kontorer.

Alle servere er placeret hos en ekstern hostingleverandør med krav om passende tekniske og organisatoriske sikkerhedsforanstaltninger. Herunder brandslukningsudstyr, nødstrømsanlæg og backupserver på en sikret ekstern lokation, hvor der dagligt bliver overført en kopi af Emento A/S' data til. Generalsekretæren indhenter enten revisor erklæring fra hosting leverandør eller foretager eget tilsyn en gang årligt. Emento A/S har en politik for destruktion af databærende udstyr.

Sikkerhed i forbindelse med drift

Det operationelle niveau har ansvaret for at sikre løbende drift og vedligehold af systemer via etablerede driftsprocedurer. Det taktiske niveau har ansvaret for registrering af forstyrrelser og uregelmæssigheder i driften af systemer.

Endvidere er der etableret procedurer for ændringsstyring, kapacitetsstyring, incident- og problemhåndtering, test og overvågning, backup, hændelseslog og beskyttelse heraf, beskyttelse mod malware, styring af softwareinstallationer på driftssystemer samt sårbarhedsstyring.

Der er etableret procedurer for håndtering af audit af systemer, herunder både for revision samt for tilsyn fra relevante parter.

Det kontrolleres minimum en gang årligt af Generalsekretæren, at Procedure og risici for sikker udvikling er fulgt samt at Drift- og Vedligeholdelsesplan er opdateret.

Kommunikationssikkerhed

Sikkerhed på 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.

Adgang til Hosting-miljøet sker altid via SSL. Der er opsat overvågning og logning af netværkstrafik. Alene godkendt netværkstrafik kommer gennem Emento A/S' firewall. Dette gælder både indgående og udgående trafik.

Alle systemgrupper kører på deres eget VLAN. Opdelingen er beskrevet i systemdokumentationen.

Emento A/S overfører ikke, medmindre andet er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler for parter der er involveret i kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.

Anskaffelse, udvikling og vedligeholdelse

Ved anskaffelse af nye systemer eller ved væsentlige udvidelser til eksisterende systemer, foretages en vurdering af systemet. I denne vurdering er der særligt fokus på risici i relation til data og de registreredes rettigheder.

Udvikling af applikationer til produktionsmiljøet sker udelukkende i udviklingsafdeling af ansatte medarbejdere og/eller konsulenter med særlig forståelse for Emento A/S' kultur og sikkerhed.

Den enkelte udvikler har ikke direkte adgang til produktionsserverne fra en udvikler PC, men kan koble op igennem en bastion-server. Er det nødvendigt at tilgå kundernes miljø for yde support eller fejlfinde, sker dette igennem en kundens AD eller via en særlig systemadgang med ekstra sikkerhed og logning. CTO gennemgår log heraf periodisk.

Generalsekretæren kontrollerer periodisk, at der udarbejdes en DPIA i forbindelse med udvikling af nye features som vurderes at kunne udgøre en risiko.

Leverandørforhold

Der indgås fortrolighedserklæringer med alle konsulenter, der får adgang til Emento A/S' systemer. Som udgangspunkt arbejder de udelukkende med hardware og software problemstillinger og har ikke adgang til data.

Emento A/S anvender så vidt muligt faste konsulenter med kontrakter af en længere varighed. Alle konsulenter er instrueret i håndtering af fortrolige oplysninger på lige fod med Emento A/S' øvrige medarbejdere.

Der indhentes revisorerklæring fra hosting leverandøren senest et år efter kontraktindgåelse eller indhentning af sidste revisorerklæring. Erklæringen gennemgås og eventuelle observationer noteres i risikoen og meddeles leverandøren.

Der føres tilsyn med eksterne leverandøren i det omfang som det vurderes at være nødvendigt ift. leverandørens opgave og databehandling.

Styring af sikkerhedshændelser

Emento A/S har procedurer for styring af sikkerhedshændelser.

Sikkerhedshændelser bliver registreret og løst uden unødigt forsinkelse eller jfr. .kontrakt. Det strategiske niveau har det overordnede ansvar for processen.

Generalsekretæren kontrollerer mindst en gang årligt, at alle medarbejdere er bekendte med og i stand til at følge procedurer for informationssikkerhedsbrud samt at eventuelle sikkerhedshændelser er registreret i hændelsesloggen.

Informationssikkerhedsaspekter ved beredskabsstyring

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttet ud fra en afvejning af risici i forhold til sikringsomkostninger. Emento A/S har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.

Emento A/S har implementeret formelle nødplaner og procedurer til beredskab, herunder redundans i kernekomponenter.

Generalsekretæren kontrollerer en gang årligt at alle medarbejdere er bekendte med og i stand til at følge nødplaner og procedurer for beredskab.

Overensstemmelse

Både Emento A/S og vores kunder er underlagt GDPR og databeskyttelsesloven. Vores kunder kan desuden være underlagt anden særlig lovgivning som fx. Sundhedsloven eller Socialloven.

En gang årligt gennemgås den gældende sikkerhedspolitik af det strategiske niveau, samt ved større ændringer i organisationen eller driftsmiljøerne.

Det er det strategiske niveau, der har det overordnede ansvar for IT-sikkerhed.

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

Emento A/S' kunder er, medmindre andet er aftalt, ansvarlige for at implementere følgende komplementære kontroller:

- At det aftalte niveau for backup dækker kundens behov
- Periodisk gennemgang af kundens egne brugere og meddele lukning af brugere
- At kundes brugere ikke lagrer ulovligt materiale på Emento A/S' servere

Afsnit 2: Emento A/S' udtalelse

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

Emento A/S anvender serviceunderleverandøren team.blue Denmark A/S. Denne erklæring er udarbejdet efter partielmetoden, og Emento A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos team.blue Denmark A/S. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Emento A/S' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Emento A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Emento A/S bekræfter, at:

- (a) Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Emento A/S' online platform for forløbsguides, der har behandlet kunders transaktioner i perioden fra 1. april 2021 til 31. marts 2022.

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.
 - 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. april 2021 til 31. marts 2022
- (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 udformede og fungerede effektivt i perioden fra 1. april 2021 til 31. marts 2022, hvis relevante kontroller hos underleverandøren var operationelt effektive, og kunderne har udført de kompletterende kontroller, som forudsættes i designet af Emento A/S i hele perioden fra 1. april 2021 til 31. marts 2022.

Kriterierne for denne udtalelse var, at:

- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
- (ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
- (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. april 2021 til 31. marts 2022.

Aarhus, den 6. maj 2022
Emento A/S



Allan Juhl
Adm. direktør

Afsnit 3: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

Til Emento A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Emento A/S' beskrivelse i afsnit 1 af generelle it-kontroller for drift af online platform for forløbsguides i perioden 1. april 2021 til 31. marts 2022 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Enkelte af de kontrolmål, der er anført i Emento A/S' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Emento A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Emento A/S' ansvar

Emento A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 1) og tilhørende udtalelse (afsnit 2), 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 effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' 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.

REVI-IT anvender ISQC 11 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

¹ ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Emento A/S' beskrivelse (afsnit 1) og om udformningen og funktionen 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 udformede og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten 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 og funktionalitet. 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 ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet Emento A/S' udtalelse i afsnit 2.

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

Emento A/S' beskrivelse i afsnit 1 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Emento A/S' udtalelse i afsnit 2. Det er vores opfattelse, at:

- (a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret i perioden 1. april 2021 til 31. marts 2022, 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 i perioden fra 1. april 2021 til 31. marts 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandøren var operationelt effektive, og hvis kunderne har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Emento A/S' kontroller i perioden fra 1. april 2021 til 31. marts 2022.
- (c) De testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i perioden 1. april 2021 til 31. marts 2022.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

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

København, den 6. maj 2022

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Henrik Paaske

Statsautoriseret revisor



Christian H. Riis

Partner, CISA

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

4.1. Formål og omfang

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

Denne erklæring er udarbejdet efter partielmetoden og Emento A/S' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Emento A/S' underleverandør.

Kontroller udført hos Emento A/S' kunder, er ikke omfattet af vores erklæring.

4.2. Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Emento A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
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.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3. Resultater af test

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

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
5.1.1	<p><i>Politikker for informationssikkerhed</i></p> <p>Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.</p>	<p>Vi har inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejderne og relevante eksterne parter.</p>	Ingen afvigelser konstateret.
5.1.2	<p><i>Gennemgang af politikker for informationssikkerhed</i></p> <p>Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.</p>	<p>Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken.</p> <p>Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.</p>	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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
6.1.1	<i>Roller og ansvarsområder for informationssikkerhed</i> Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret at organisationsdiagrammet viser, at ansvaret for informationssikkerhed er klart defineret og fordelt.	Ingen afvigelser konstateret.
6.1.2	<i>Funktionsadskillelse</i> Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har forespurgt til procedurer vedrørende tildeling og opretholdelse af adskillelse af ansvarsområder og funktioner. Vi har inspiceret dokumentation for adskillelse af funktioner i organisationen.	Ingen afvigelser konstateret.
6.1.3	<i>Kontakt med myndigheder</i> Der opretholdes passende kontakt med relevante myndigheder.	Vi har inspiceret dokumentation for, at der er opretholdt passende kontakt med myndigheder. Vi har inspiceret, at kontaktinformationen er vedligeholdt og opdateret.	Ingen afvigelser konstateret.
6.1.4	<i>Kontakt med særlige interessegrupper</i> Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Vi har inspiceret, at der er opretholdt passende kontakt med særlige interessegrupper, faglige sikkerhedsfora og faglige organisationer.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser
Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
6.2.1	<p><i>Politik for mobilt udstyr</i></p> <p>Der er etableret en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.</p>	<p>Vi har inspiceret politik for sikring af mobile enheder.</p> <p>Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobile enheder.</p> <p>Vi har stikprøvevis inspiceret, at tekniske kontroller er implementeret på mobile enheder.</p>	Ingen afvigelser konstateret.
6.2.2	<p><i>Fjernarbejdspladser</i></p> <p>Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.</p>	<p>Vi har inspiceret politik for sikring af fjernarbejdspladser.</p> <p>Vi har inspiceret dokumentation for, at der skal logges på via VPN, ved anvendelsen af fjernarbejdspladser.</p>	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen

Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er tiltænkt.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
7.1.1	<p><i>Screening</i></p> <p>Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.</p>	<p>Vi har inspiceret proceduren for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse.</p> <p>Vi har forespurgt til relevant lovgivning i forbindelse med screening af medarbejdere.</p> <p>Vi har stikprøvevis inspiceret dokumentation for, at screening er gennemført i forbindelse med ansættelser.</p>	Ingen afvigelser konstateret.
7.1.2	<p><i>Ansættelsesvilkår og -betingelser</i></p> <p>Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.</p>	<p>Vi har inspiceret, at en standardansættelseskontrakt indeholder pågældende og organisationens ansvar for informationssikkerhed.</p> <p>Vi har stikprøvevis inspiceret kontrakter med nyansatte medarbejdere er underskrevet.</p>	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen

Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
7.2.1	<p><i>Ledelsesansvar</i></p> <p>Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.</p>	<p>Vi har inspiceret proceduren vedrørende fastsættelse af krav til medarbejdere og kontrahenter.</p> <p>Vi har inspiceret, at ledelsen har stillet krav om, at medarbejderne og kontrahenter skal overholde informationssikkerhedspolitikken.</p>	Ingen afvigelser konstateret.
7.2.2	<p><i>Bevidsthed om, uddannelse og træning i informationssikkerhed</i></p> <p>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.</p>	<p>Vi har forespurgt til procedurer til sikring af tilstrækkelig uddannelse og træning i informationssikkerhed (awarenesstræning).</p> <p>Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejdere.</p>	Ingen afvigelser konstateret.
7.2.3	<p><i>Sanktioner</i></p> <p>Der er etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.</p>	<p>Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret til medarbejderne og kontrahenter.</p>	Ingen afvigelser konstateret.

A.7.3 Ansættelsesforholdets ophør eller ændring

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
7.3.1	<p><i>Ansættelsesforholdets ophør eller ændring</i></p> <p>Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikerer til medarbejderen eller kontrahenten og håndhæves.</p>	<p>Vi har inspiceret proceduren for medarbejdernes og kontrahenters forpligtelser til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse eller kontrakt.</p> <p>Vi har forespurgt om der har været nogle fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogle fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.8 Styring af aktiver

A.8.1 Ansvar for aktiver

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
8.1.1	<p><i>Fortegnelse over aktiver</i></p> <p>Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.</p>	<p>Vi har inspiceret fortegnelser over aktiver indeholder både hardware samt software.</p> <p>Vi har inspiceret at fortegnelser er vedligeholdt og opdateret.</p>	<p>Ingen afvigelser konstateret.</p>
8.1.2	<p><i>Ejerskab af aktiver</i></p> <p>Der udpeges en ejer i organisationen for hvert aktiv.</p>	<p>Vi har inspiceret dokumentation for at der er defineret ejerskab over de forskellige aktiver.</p>	<p>Ingen afvigelser konstateret.</p>
8.1.4	<p><i>Tilbagelevering af aktiver</i></p> <p>Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.</p>	<p>Vi har forespurgt til proceduren for sikring af tilbagelevering af udleverede aktiver.</p> <p>Vi har inspiceret, at der i standardtjeklisten for ansættelsesforhold fremgår, hvilke aktiver der skal inddrages ved fratrædelse.</p> <p>Vi har forespurgt om hvorvidt der har været fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogle fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.8.2 Klassifikation af information

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

Nr.	Emento A/S' kontrol I	REVI-IT's test	Resultat af test
8.2.1	<p><i>Klassifikation af information</i></p> <p>Information klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.</p>	<p>Vi har inspiceret politik for klassificering af information.</p> <p>Vi har inspiceret at information er klassificeret efter hvor følsom og kritisk informationen er.</p>	Ingen afvigelser konstateret.
8.2.2	<p><i>Mærkning af information</i></p> <p>Der er udarbejdet og implementeret et passende sæt procedurer til mærkning af information der er i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.</p>	<p>Vi har inspiceret proceduren for mærkning af data.</p> <p>Vi har stikprøvevis inspiceret, at information er mærket i overensstemmelse med klassifikationssystemet.</p>	Ingen afvigelser konstateret.
8.2.3	<p><i>Håndtering af aktiver</i></p> <p>Der er udarbejdet og implementeret procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.</p>	<p>Vi har inspiceret procedurer for håndtering af aktiver.</p> <p>Vi har stikprøvevis inspiceret, at aktiver håndteres i overensstemmelse med proceduren.</p>	Ingen afvigelser konstateret.

A.8.3 Mediehåndtering

Kontrolmål: at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
8.3.2	<p><i>Bortskaffelse af medier</i></p> <p>Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.</p>	<p>Vi har inspiceret procedurer for bortskaffelse af medier.</p> <p>Vi har forespurgt om der har været bortskaffede medier i erklæringsperioden, som indeholder lagret information.</p>	<p>Vi er blevet informeret om, at der ikke har været nogen bortskaffede medier i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring

Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.1.1	<p><i>Politik for adgangsstyring</i></p> <p>En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informations sikkerhedskrav.</p>	<p>Vi har inspiceret politikken for adgangsstyring.</p> <p>Vi har inspiceret at politikken er opdateret og gennemgået i erklæringsperioden.</p>	Ingen afvigelser konstateret.
9.1.2	<p><i>Adgang til netværk og netværkstjenester</i></p> <p>Brugere har kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.</p>	<p>Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester.</p> <p>Vi har inspiceret udtræk over brugere med henblik på at konstatere, at de kun har adgang til godkendte netværk og netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.</p>	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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.2.1	<p><i>Brugerregistrering-og afmelding</i></p> <p>Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgang adgangsrettigheder.</p> <p>Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt inden de får adgang.</p> <p>Vi har forespurgt om hvorvidt der har været nogle fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogen fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen herfor.</p> <p>Ingen afvigelser konstateret.</p>
9.2.2	<p><i>Tildeling af brugeradgang</i></p> <p>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.</p>	<p>Vi har inspiceret, at der er etableret en procedure for brugeradministration.</p> <p>Vi har stikprøvevis inspiceret, at brugerne tildeles adgangsrettigheder baseret på deres rolle og arbejdsbetinget behov.</p>	<p>Ingen afvigelser konstateret.</p>
9.2.3	<p><i>Styring af privilegerede adgangsrettigheder</i></p> <p>Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.</p>	<p>Vi har forespurgt til procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder.</p> <p>Vi har inspiceret udtrækket over de privilegerede brugere og forespurgt om disse har et arbejdsbetinget behov for adgangen.</p>	<p>Ingen afvigelser konstateret.</p>
9.2.4	<p><i>Styring af hemmelig autentifikationsinformation om brugere</i></p> <p>Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.</p>	<p>Vi har inspiceret proceduren vedrørende tildeling af passwords.</p> <p>Vi har inspiceret dokumentation for hvordan brugerne modtager password, og efterfølgende skal ændre dette.</p>	<p>Ingen afvigelser konstateret.</p>
9.2.5	<p><i>Gennemgang af brugeradgangsrettigheder</i></p> <p>Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.</p>	<p>Vi har forespurgt til proceduren for regelmæssig gennemgang og evaluering af adgangsrettigheder.</p> <p>Vi har stikprøvevis inspiceret at der foretages gennemgang og evalueringer af adgangsrettigheder.</p>	<p>Ingen afvigelser konstateret.</p>

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.2.6	<p><i>Inddragelse eller justering af adgangsrettigheder</i></p> <p>Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.</p>	<p>Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder.</p> <p>Vi har forespurgt om hvorvidt der har været fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.9.3 Brugernes ansvar

Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.3.1	<p><i>Brug af hemmelig autentifikationsinformation</i></p> <p>Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.</p>	<p>Vi har inspiceret skriftlige krav til kvaliteten af adgangskoder.</p> <p>Vi har inspiceret teknisk dokumentation for at kravene til adgangskoderne i systemerne som minimum stemmer overens med de skriftlige krav.</p>	<p>Ingen afvigelser konstateret.</p>

A.9.4 Styring af system- og applikationsadgang

Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.4.2	<p><i>Procedurer for sikker logon</i></p> <p>Adgang til systemer og applikationer styres af en procedure for sikker logon.</p>	<p>Vi har inspiceret proceduren for sikkert login.</p>	<p>Ingen afvigelser konstateret.</p>
9.4.3	<p><i>System for administration af passwords</i></p> <p>Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet.</p>	<p>Vi har inspiceret, at der i politikker og procedurer stilles krav til kvaliteten af passwords.</p> <p>Vi har inspiceret, at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav.</p>	<p>Ingen afvigelser konstateret.</p>

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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
10.1.1	<i>Politik for anvendelse af kryptografi</i> Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har inspiceret politikken for anvendelse af kryptering.	Ingen afvigelser konstateret.
10.1.2	<i>Administration af nøgler</i> 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 stikprøvevis inspiceret, at krypteringsnøglerne er aktive samt, at der er udført en gennemgang af nøglerne.	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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
11.1.2	<i>Fysisk adgangskontrol</i> Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har forespurgt til procedurerne for adgangskontrol til sikre områder. Vi har inspiceret adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til produktionsfaciliteterne.	Ingen afvigelser konstateret.
11.1.3	<i>Sikring af kontorer, lokaler og faciliteter</i> 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.	Ingen afvigelser konstateret.

A.11.2 Udstyr			
Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
11.2.1	<p><i>Placering og beskyttelse af udstyr</i></p> <p>Udstyr er placeret og beskyttet, så risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.</p>	<p>Vi har inspiceret proceduren vedrørende placering og beskyttelse af udstyr.</p> <p>Vi har inspiceret relevante lokationer for at vurdere, hvorvidt lokaler er sikkert aflåst og kontrolleret, at kun medarbejdere med et arbejdsbetinget behov har adgang hertil.</p>	Ingen afvigelser konstateret.
11.2.4	<p><i>Vedligeholdelse af udstyr</i></p> <p>Udstyr vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.</p>	<p>Vi har inspiceret politikken for vedligeholdelse af udstyr.</p> <p>Vi har forespurgt om hvorvidt der har været foretaget reparationer og vedligeholdelse af udstyr i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogen reparationer eller vedligeholdelse af udstyr i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
11.2.5	<p><i>Fjernelse af aktiver</i></p> <p>Udstyr, information og software må ikke fjernes fra organisationen uden forudgående tilladelse.</p>	Vi har inspiceret retningslinjer for fjernelse af udstyr, information og software fra virksomheden.	Ingen afvigelser konstateret.
11.2.6	<p><i>Sikring af udstyr og aktiver uden for organisationen</i></p> <p>Der er etableret sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen.</p>	Vi har inspiceret retningslinjer for sikring af udstyr og aktiver uden for organisationen.	Ingen afvigelser konstateret.
11.2.7	<p><i>Sikker bortskaffelse eller genbrug af udstyr</i></p> <p>Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.</p>	<p>Vi har inspiceret proceduren for sletning af data og software på lagringsmedier inden bortskaffelse af lagringsmediet.</p> <p>Vi har forespurgt om hvorvidt der har været bortskaffelse eller genbrug af udstyr i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været bortskaffelse eller genbrug af udstyr i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
11.2.8	<i>Brugerdstyr uden opsyn</i> Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har inspiceret proceduren for sikring af beskyttelse af udstyr, som er uden opsyn.	Ingen afvigelser konstateret.
11.2.9	<i>Politik for ryddeligt skrivebord og blank skærm</i> 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.12.1 Driftsprocedurer og ansvarsområder

Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.1.1	<i>Dokumenterede driftsprocedurer</i> Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt. Vi har stikprøvevis inspiceret, at driftsdokumentation er opdateret og tilgængelig for medarbejdere, som har behov for dem.	Ingen afvigelser konstateret.
12.1.2	<i>Ændringsstyring</i> Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren for ændringsstyring. Vi har stikprøvevis inspiceret, at ændringer er testet og godkendt samt at der er etableret funktionsadskillelse i processen. Vi har stikprøvevis inspiceret, at ændringer monitoreres og dokumenteres.	Ingen afvigelser konstateret.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.1.3	<p><i>Kapacitetsstyring</i></p> <p>Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.</p>	<p>Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav.</p> <p>Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.</p>	Ingen afvigelser konstateret.
12.1.4	<p><i>Adskillelse af udviklings-, test- og driftsmiljøer</i></p> <p>Udviklings-, test- og driftsmiljøer adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.</p>	<p>Vi har forespurgt til sikring af adskillelse af udviklings-, test- og driftsmiljøer.</p> <p>Vi har stikprøvevis inspiceret, at der enten er logisk eller fysisk adskillelse mellem udvikling, test og produktion.</p>	Ingen afvigelser konstateret.

A 12.2 Malwarebeskyttelse

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.2.1	<p><i>Kontroller mod malware</i></p> <p>Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.</p>	<p>Vi har forespurgt procedure til foranstaltninger mod malware.</p> <p>Vi har stikprøvevis inspiceret, at der er implementeret kontroller mod malware.</p> <p>Vi har forespurgt til proceduren for tilsyn med udstyr hvor der ikke er installeret malware kontrol.</p>	Ingen afvigelser konstateret.

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.3.1	<p><i>Backup af information</i></p> <p>Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.</p>	<p>Vi har forespurgt til krav til konfiguration af backup.</p> <p>Vi har inspiceret, at der gennemføres overvågning af afviklingen af backup.</p> <p>Vi har forespurgt til test af gendannelse fra backupfiler.</p>	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning
Kontrolmål: At registrere hændelser og tilvejebringe bevis.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.4.1	<p><i>Hændelseslogning</i></p> <p>Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.</p>	<p>Vi har forespurgt til logning af brugeraktivitet.</p> <p>Vi har inspiceret at der foreligger en hændelseslog samt at denne gennemgås.</p>	Ingen afvigelser konstateret.
12.4.2	<p><i>Beskyttelse af log- oplysninger</i></p> <p>Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.</p>	<p>Vi har inspiceret proceduren for sikring af logoplysninger.</p> <p>Vi har stikprøvevis inspiceret at logs er beskyttet mod manipulation og uautoriseret adgang.</p>	Ingen afvigelser konstateret.
12.4.3	<p><i>Administrator- og operatørlog</i></p> <p>Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.</p>	<p>Vi har inspiceret proceduren vedrørende logning af aktiviteter udført af systemadministratorer og -operatører.</p> <p>Vi har inspiceret udtræk over adgang til administrator- og operatørlogs, er begrænset til medarbejdere med et arbejdsbetinget behov.</p>	Ingen afvigelser konstateret.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.4.4	<p><i>Tidssynkronisering</i></p> <p>Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne er synkroniserede til en enkelt referencetidskilde.</p>	<p>Vi har forespurgt til proceduren for synkronisering op imod en betryggende tidsserver</p> <p>Vi har inspiceret, at der er tidssynkronisering på maskiner.</p>	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware

Kontrolmål: At sikre integriteten af driftssystemer.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.5.1	<p><i>Softwareinstallation på driftssystemer</i></p> <p>Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.</p>	<p>Vi har inspiceret retningslinjer for installation af software på driftssystemer.</p> <p>Vi har stikprøvevis inspiceret, at retningslinjerne efterleves.</p>	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring

Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.6.1	<p>Styring af tekniske sårbarheder</p> <p>Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.</p>	<p>Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder.</p> <p>Vi har stikprøvevis inspiceret at der er foretaget sårbarhedsscanning fra eksternt part.</p>	Ingen afvigelser konstateret
12.6.2	<p>Begrænsninger på softwareinstallation</p> <p>Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.</p>	<p>Vi har forespurgt til procedurer for begrænsning af softwareinstallation, som foretages af brugere.</p> <p>Vi har inspiceret, at regler for softwareinstallation efterleves.</p>	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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
13.1.1	<i>Netværksstyring</i> Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls og andre relevante sikkerhedsforanstaltninger.	Ingen afvigelser konstateret.
13.1.2	<i>Sikring af netværkstjenester</i> Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcete.	Vi har inspiceret skriftlige krav til sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester. Vi har stikprøvevis inspiceret netværkskomponenter for at vurdere, hvorvidt komponenterne er opsat i overensstemmelse med kravene og leverandørens anbefalede baselines.	Ingen afvigelser konstateret.
13.1.3	<i>Opdeling af netværk</i> Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret netværksdiagrammer og anden netværksdokumentation med hensyn til opdeling af netværk.	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
13.2.1	<p><i>Politikker og procedurer for informationsoverførsel</i></p> <p>Der foreligger formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.</p>	<p>Vi har inspiceret politikker og procedurer for informationsoverførsel.</p>	Ingen afvigelser konstateret.
13.2.3	<p><i>Elektroniske meddelelser</i></p> <p>Informationer i elektroniske meddelelser beskyttes på passende måde.</p>	<p>Vi har inspiceret retningslinjer for afsendelse af fortrolig information.</p> <p>Vi har stikprøvevis inspiceret, at elektroniske meddelelser krypteres.</p>	Ingen afvigelser konstateret.
13.2.4	<p><i>Fortroligheds- og hemmeligholdelsesaftaler</i></p> <p>Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres.</p>	<p>Vi har forespurgt procedurer, som sikrer, at medarbejderne underskriver en fortrolighedsaftale, og at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen.</p> <p>Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden, har underskrevet en fortrolighedsaftale.</p>	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

A.14.1 Sikkerhedskrav til informationssystemer

Kontrolmål: At sikre at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
14.1.1	<p><i>Analyse og specifikation af informations- sikkerheds- krav</i></p> <p>Informationssikkerhedsrelaterede krav omfattes af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.</p>	Vi har inspiceret proceduren for analyse og specifikation af informationssikkerhedskrav.	Ingen afvigelser konstateret.

A.14.2 Sikkerheds, udviklings- og hjælpeprocesser

Kontrolmål: At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
14.2.1	<p><i>Sikker udviklingspolitik</i></p> <p>Der fastlægges og anvendes regler for udvikling af software og systemer i organisationen.</p>	Vi har inspiceret regler for udvikling af software og systemer.	Ingen afvigelser konstateret.
14.2.2	<p><i>Procedurer for styring af systemændringer</i></p> <p>Ændringer af systemer inden for udviklingslivscyklussen styres ved hjælp af formelle procedurer for ændringsstyring.</p>	<p>Vi har inspiceret proceduren for Change Management med henblik på at konstatere, hvorvidt proceduren indeholder krav om:</p> <ul style="list-style-type: none"> ● Risikovurdering ● Test ● Godkendelse ● Systemdokumentation ● Fall back plan <p>Vi har stikprøvevis inspiceret ændringer med henblik på at konstatere, om kravene til ændringshåndtering blev fulgt.</p>	Ingen afvigelser konstateret.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
14.2.3	<p><i>Teknisk gennemgang af applikationer efter ændringer af driftsplatforme</i></p> <p>Ved ændring af driftsplatforme gennemgås forretningskritiske applikationer og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.</p>	<p>Vi har forespurgt til proceduren for teknisk gennemgang af applikationer efter ændringer af driftsplatforme.</p> <p>Vi har stikprøvevis inspiceret, at ændringer på operativsystemer og infrastruktur er blevet vurderet m.h.t. deres eventuelle konsekvenser for applikationssystemer, inden de er blevet gennemført.</p>	Ingen afvigelser konstateret.
14.2.4	<p><i>Begrænsning af ændringer af softwarepakker</i></p> <p>Ændringer af softwarepakker vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer styres effektivt.</p>	<p>Vi har forespurgt vedrørende proceduren for begrænsning af ændringer af softwarepakker.</p> <p>Vi har inspiceret udtræk over brugere, med adgang til at ændre i systemer fra leverandører, og påset at dette er begrænset til medarbejdere med et arbejdsbetinget behov.</p>	Ingen afvigelser konstateret.
14.2.5	<p><i>Principper for udvikling af sikre systemer</i></p> <p>Principper for udvikling af sikre systemer fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationssystemer.</p>	<p>Vi har inspiceret proceduren for udvikling af systemer.</p> <p>Vi har stikprøvevis inspiceret, at proceduren har været fulgt.</p>	Ingen afvigelser konstateret.
14.2.6	<p><i>Sikkert udviklingsmiljø</i></p> <p>Der er etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus</p>	<p>Vi har inspiceret proceduren for etablering af sikkert udviklingsmiljø.</p> <p>Vi har forespurgt, hvordan sikre udviklingsmiljøer er beskyttet.</p>	Ingen afvigelser konstateret.
14.2.8	<p><i>Systemikkerhedstest</i></p> <p>Test af sikkerhedsfunktionalitet udføres ved udvikling.</p>	Vi har stikprøvevis inspiceret, at der foretages test af sikkerhedsfunktionalitet som led i systemudviklingsprocessen.	Ingen afvigelser konstateret.
14.2.9	<p><i>Systemgodkendelsestest</i></p> <p>Der etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.</p>	<p>Vi har forespurgt vedrørende godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer.</p> <p>Vi har stikprøvevis inspiceret, at der foretages test af nye systemer.</p>	Ingen afvigelser konstateret.

A.14.3 Testdata

Kontrolmål: At sikre beskyttelse af data, som anvendes til test

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
14.3.1	<p><i>Sikring af testdata</i></p> <p>Testdata udvælges omhyggeligt og beskyttes og styres.</p>	<p>Vi har forespurgt vedrørende udvælgelse og beskyttelse af testdata.</p> <p>Vi har stikprøvevis inspiceret, at testdata er oprettet af Emento samt at der er tale om fiktive data.</p>	Ingen afvigelser konstateret.

A.15 Leverandørforhold

A.15.1 Informationssikkerhed i leverandørforhold

Kontrolmål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
15.1.1	<p><i>Informationssikkerhedspolitik for leverandørforhold</i></p> <p>Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres.</p>	Vi har inspiceret proceduren for indgåelse af aftaler med leverandører.	Ingen afvigelser konstateret.
15.1.2	<p><i>Håndtering af sikkerhed i leverandøraftaler</i></p> <p>Alle relevante informationssikkerhedskrav fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information.</p>	<p>Vi har inspiceret proceduren for indgåelse af aftaler med leverandører.</p> <p>Vi har forespurgt hvorvidt indgåede leverandøraftaler indeholder relevante informationssikkerhedskrav.</p>	Ingen afvigelser konstateret.

15.2 Styring af leverandørydelser

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
15.2.1	<p><i>Overvågning og gennemgang af leverandørydelser</i></p> <p>Leverandørydelser overvåges, gennemgås og auditeres.</p>	<p>Vi har forespurgt til proceduren for overvågning og gennemgang af serviceydelser leveret af underleverandøren er i overensstemmelse med det aftalte.</p> <p>Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører.</p>	<p>Ingen afvigelser konstateret.</p>
15.2.2	<p><i>Styring af ændringer af leverandørydelser</i></p> <p>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.</p>	<p>Vi har forespurgt til styring af ændringer hos leverandøren.</p>	<p>Vi er blevet informeret om, at der ikke har været nogle væsentlige ændringer af leverandørydelser i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

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.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
16.1.1	<p><i>Ansvar og procedurer</i></p> <p>Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.</p>	<p>Vi har forespurgt til ansvar og procedurer i forbindelse med informationssikkerhedshændelser.</p> <p>Vi har inspiceret dokumentation for ansvarsfordeling.</p> <p>Vi har inspiceret proceduren til håndtering af informationssikkerhedshændelser.</p>	Ingen afvigelser konstateret.
16.1.2	<p><i>Rapportering af informationssikkerhedshændelser</i></p> <p>Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.</p>	<p>Vi har inspiceret retningslinjer for rapportering af informationssikkerhedshændelser.</p> <p>Vi har stikprøvevis inspiceret, at informationssikkerhedshændelser er rapporteret ad passende ledelseskanaler.</p>	Ingen afvigelser konstateret.
16.1.3	<p><i>Rapportering af informationssikkerhedssvagheder</i></p> <p>Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.</p>	<p>Vi har inspiceret retningslinjer for rapportering af informationssikkerhedssvagheder.</p>	Ingen afvigelser konstateret.
16.1.4	<p><i>Vurdering af og beslutning om informations-sikkerhedshændelser</i></p> <p>Informationssikkerhedshændelser vurderes, og det beslutes, om de skal klassificeres som informationssikkerhedsbrud.</p>	<p>Vi har inspiceret proceduren for vurdering af informationssikkerhedshændelser.</p>	Ingen afvigelser konstateret.
16.1.5	<p><i>Håndtering af informationssikkerhedsbrud</i></p> <p>Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.</p>	<p>Vi har stikprøvevis inspiceret, at informationssikkerhedsbrud har været håndteret i overensstemmelse med proceduren.</p>	Ingen afvigelser konstateret.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
16.1.6	<p><i>Erfaring fra informationssikkerhedsbrud</i></p> <p>Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.</p>	Vi har stikprøvevis inspiceret, at der foretages analyse af informationssikkerhedsbrud samt forespurgt hvordan dette håndteres.	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 beredskabs- og reetableringsstyring.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
17.1.1	<p><i>Planlægning af informationssikkerhedskontinuitet</i></p> <p>Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.</p>	Vi har inspiceret beredskabsplanen til sikring af videreførelse af driften i forbindelse med nedbrud og lignende.	Ingen afvigelser konstateret.
17.1.2	<p><i>Implementering af informationssikkerheds-kontinuitet</i></p> <p>Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.</p>	<p>Vi har forespurgt til procedurer der sikrer, at alle relevante systemer indgår i beredskabsplanlægningen.</p> <p>Vi har inspiceret om beredskabsplanen vedligeholdes.</p>	Ingen afvigelser konstateret.
17.1.3	<p><i>Verificer, gennemgå og evaluer informations-sikkerhedskontinuiteten</i></p> <p>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.</p>	<p>Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test.</p> <p>Vi har endvidere forespurgt til regelmæssig revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurderingen.</p>	Ingen afvigelser konstateret.

A.18.2 Gennemgang af informationssikkerheden

Kontrolmål: At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
18.2.1	<p><i>Uafhængig gennemgang af informationssikkerhed</i></p> <p>Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.</p>	<p>Vi har inspiceret, at der er etableret krav om regelmæssig uafhængig revisionsmæssig gennemgang af informationssikkerheden.</p>	<p>Ingen afvigelser konstateret.</p>
18.2.2	<p><i>Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder</i></p> <p>Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.</p>	<p>Vi har forespurgt vedrørende lederes sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder.</p> <p>Vi har stikprøvevis inspiceret, at der udføres og dokumenteres interne kontroller samt årshjul.</p>	<p>Ingen afvigelser konstateret</p>
18.2.3	<p><i>Undersøgelse af teknisk overensstemmelse</i></p> <p>Informationssystemer undersøges regelmæssigt for, om de er i overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.</p>	<p>Vi har inspiceret, at procedurer for regelmæssig kontrol af systemers overholdelse af sikkerhedsstandarder er implementeret.</p>	<p>Ingen afvigelser konstateret</p>