ISAE 3402 erklæring om generelle IT-kontroller
pr. 15-04-2020

ISAE 3402-1

Emento A/S

CVR-nr.: 37 32 17 45

April 2020

Indholdsfortegnelse

Afsnit 1: Emento A/S' beskrivelse af kontroller i forbindelse med drift af online platform for forløbsguides

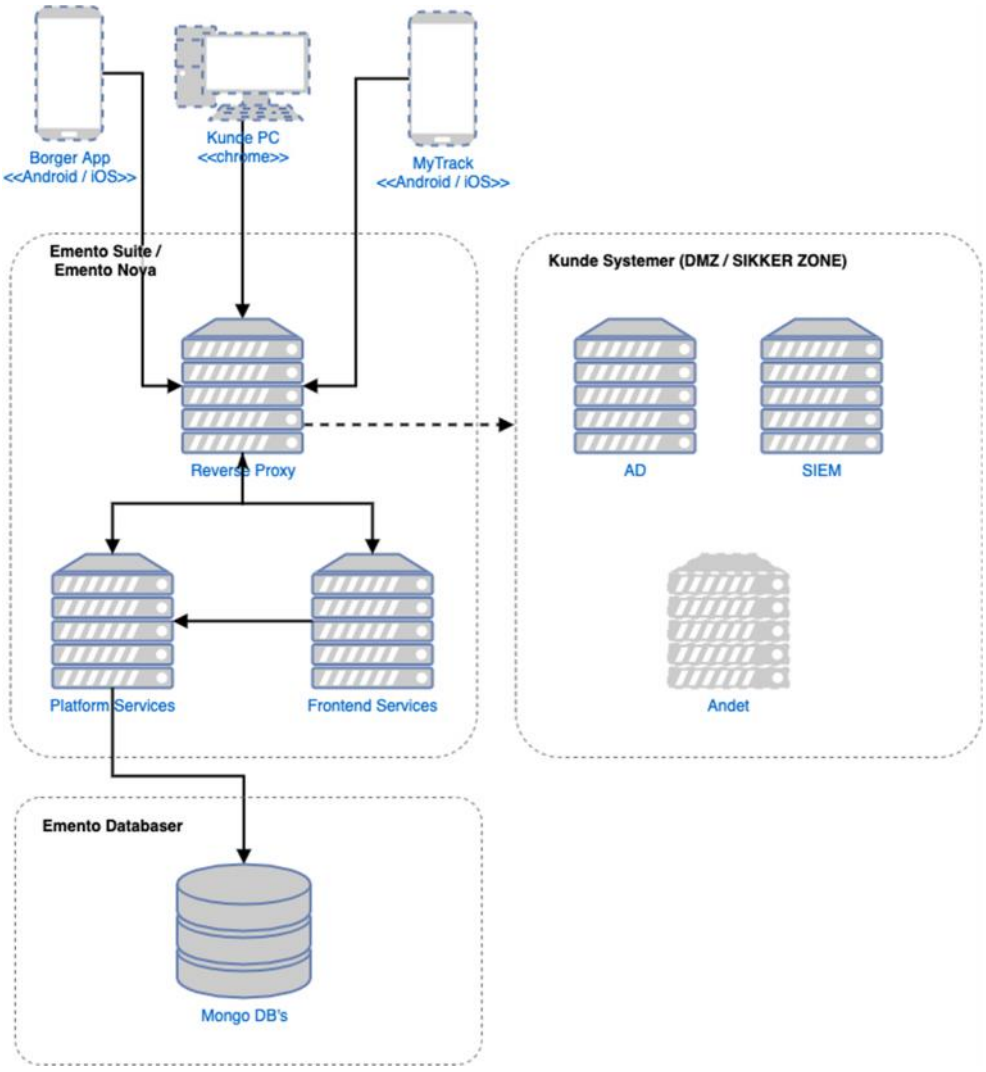
Indledning

Emento har udarbejdet en app (Emento appen) hvilket er en online platform (forløbsguide) som Emento vedligeholder og stiller til rådighed for virksomheder, privatpersoner og offentlige institutioner. Forløbsguiden bruges af Ementos dataansvarlige parter til løbende kommunikation mellem

- patienter/borgere og/eller hospitaler kommuner eller
- medarbejdere og arbejdsgivere.

Forløbsguiden bruges til at definere et forløb som via appen løbende guider og informerer borgere/patienter/medarbejdere. Appen gør det også muligt for borgerne/patienterne/medarbejderne at sende beskeder til den dataansvarliges personale.

Løsningen kan skitseres således:



Emento's platform leveres som en private cloud løsning til den enkelte kunde. Det vil sige at hver kunde har adgang til en servicestack (Emento Suite) kørende på nogle servere tildelt til kunden. Alle servere kører Ubuntu LTS med docker swarm til at administrere services på systemet. Services er udelukkende tilgængeli-

ge via Reverse Proxy som benytter firewall og OWASP CRS for at sikre, at kun godkendt og sikker data kan nå de enkelte services. Det er også igennem Reverse Proxy at eventuel kommunikation med kundens egne systemer foregår.

Generelle IT-kontroller hos Emento A/S

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

Emento 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, aftaleretlige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

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

Risikovurdering og -håndtering

Risikovurdering og -håndtering sker som en løbende aktivitet i Emento. Her tages stilling til hvorvidt nye aktiver, ændringer i udviklingen eller vedligeholdelse eller ændringer i omverdenen giver anledning til revurdering af de nuværende sikkerhedsforanstaltninger. Risici vurderes ud fra en sammenholdelse af sandsynlighed og konsekvens. Relevante procedurer og dokumenter gennemgås årligt.

Med udgangspunkt i risikovurderingen og ISO 27002 har Emento A/S udvalgt hovedområder og kontrolmål for styring af IT-sikkerheden, der er nærmere beskrevet i det følgende:

Organisering af IT-sikkerheden hos Emento A/S

Organiseringen af IT-sikkerheden sker med udgangspunkt i Emento A/S' IT-sikkerhedspolitik og tager udgangspunkt i ISO 27002, som indeholder følgende hovedområder:

5	Informationssikkerhedspolitikker	12	Driftssikkerhed
6	Organisering af informationssikkerhed	13	Kommunikationssikkerhed
7	Medarbejdersikkerhed	14	Anskaffelse, udvikling og vedligeholdelse af systemer
8	Styring af aktiver	15	Leverandørforhold
9	Adgangsstyring	16	Styring af informationssikkerhedsbrud
10	Kryptografi	17	Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
11	Fysisk sikring og miljøsikring	18	Overensstemmelse

Tilrettelæggelsen af IT-sikkerheden indenfor de enkelte områder er beskrevet nedenfor. Kontrolmål og kontroller fremgår endvidere af oversigten i afsnit 4.

5 - Informationssikkerhedspolitikker

Informationssikkerhedspolitikken gennemgås en gang årlig og godkendes af ledelsen.

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

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

Korrekt funktionsadskillelse kontrolleres en gang årligt af generalsekretæren.

7 - Medarbejdersikkerhed

Inden ansættelse: Der skal som minimum altid deltage mindst 2 fra Emento 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 indhenter alle kandidaters samtykke til at indhente referencer.

Under ansættelse: Alle medarbejdere i Emento og hos leverandører, der udfører arbejde på vegne af Emento, 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 sikkerhedspolitikken 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.

8 - 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 sikkerhedsslettet inden bortskaffelse.

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

9 – Adgangsstyring

Adgangen til at udføre handlinger på Ementos 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 Ementos systemer.

Der er etableret procedurer for tildeling og inddragelse af rettigheder.

Adgang til interne netværk fra et eksternt netværk, går igennem Ementos VPN og benytter to-faktor-godkendelse.

Gæster hos Emento har adgang til et gæstenetværk, som ikke giver adgang til Ementos interne systemer.

Kildekode til Ementos systemer ligger i eksternt depot og kun autoriserede personer har adgang hertil.

Emento 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 Ementos systemer. Alle medarbejderne er instrueret i håndtering af adgange.

Ementos kunder er selv ansvarlige for egen brugeradministration enten via eget AD eller ved brug af Ementos brugeradministrationssystem.

Emento har rettigheder til at logge på alle systemer ifm. support. Det er ikke muligt for kunderne selv at ændre i driftsmiljøerne.

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

10 - 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 Ementos 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 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.

11 – Fysisk sikring og miljøsikring

Alle indgange til Ementos 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 Ementos kontorer.

Alle servere er placeret hos en ekstern hosting-leverandør med krav om passende tekniske og organisatoriske sikkerhedsforanstaltninger. Herunder brandslukningsudstyr, nødstrømsanlæg og backupserver på en sikret ekstern lokation, hvortil der dagligt bliver overført en kopi af Ementos data.

Generalsekretæren indhenter enten revisor erklæring fra hosting leverandør eller foretager eget tilsyn en gang årligt.

Emento har en politik for destruktion af databærende udstyr.

12 - Driftssikkerhed

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 den IT-driftsansvarlige, at security procedure for IT-department, er fulgt.

13 - 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 Ementos firewall. Dette gælder både indgående og udgående trafik.

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

Emento overfører ikke, medmindre andet er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.

14 - 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 Ementos 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.

15 - Leverandørforhold

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

Emento 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 Ementos øvrige medarbejdere.

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

16 - Styring af sikkerhedsbrud

Emento har procedurer for styring af sikkerhedshændelser.

Sikkerhedshændelser bliver registreret og løst uden unødig 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 security procedure for IT-department og procedurer for informationssikkerhedsbrud.

17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici i forhold til sikringsomkostninger.

Emento har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.

Emento 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.

18 - Overensstemmelse

Både Emento 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.

Komplementerende kontroller

Ementos kunder er, medmindre andet er aftalt, ansvarlige for at implementere følgende komplementerende kontroller:

- At det aftalte niveau for backup, dækker kundens behov
- Periodisk gennemgang af kundens egne brugere og meddele lukning af bruger
- At kundes brugere ikke lagrer ulovligt materiale på Ementos servere.

Afsnit 2: Emento A/S' udtalelse

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

Emento A/S anvender serviceunderleverandøren Team Blue. Denne erklæring er udarbejdet efter partielmetoden, og Emento A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Team Blue.

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' onlineplatform, der har behandlet kunders transaktioner pr. 15-04-2020.

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 pr. 15-04-2020

(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 pr. 15-04-2020. 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 pr. 15-04-2020.

Aarhus, den 29. april 2020
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 til opgave at afgive erklæring om Emento A/S' beskrivelse i afsnit 1 af hosting-platform til behandling af kunders transaktioner pr. 15-04-2020 og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Emento A/S anvender serviceunderleverandøren Team Blue. Denne erklæring er udarbejdet efter partielmetoden, og Emento A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Team Blue.

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 udtalelse 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 IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

REVI-IT anvender ISQC 1[1] 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.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Ementos beskrivelse (afsnit 2) 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. 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.

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 hensigtsmæssige.

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

En erklæringsopgave med sikkerhed af denne type omfatter endvidere 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 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

Ementos 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 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Emento A/S' beskrivelse i afsnit 2. Det er vores opfattelse,

(a) At beskrivelsen af kontroller, således som de var udformet og implementeret pr. 15-04-2020, i alle væsentlige henseender er retvisende
(b) At kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 15-04-2020.

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 hovedafsnit (afsnit 4).

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Ementos onlineplatform, 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 risicieene for væsentlige fejlinformationer i deres regnskaber.

København, den 29. april 2020

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Director, CISA

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

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi har konstateret afvigelser, 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 Team Blue.

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

Vi har udført vores tests af kontroller hos Emento A/S' via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Emento. 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.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Risikovurdering og -håndtering

Risikovurdering

Kontrolmål: Formålet er at sikre, at virksomheden periodisk foretager en analyse og vurdering af IT-risikobilledet.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Risikovurdering og -håndtering sker som en løbende aktivitet i Emento. Her tages der stilling til hvorvidt nye aktiver, ændringer i udviklingen eller vedligeholdelse eller ændringer i omverdenen giver anledning til revurdering af de nuværende sikkerhedsforanstaltninger. Risici vurderes ud fra sammenhold af sandsynlighed og konsekvens. Relevante procedurer og dokumenter gennemgås årligt.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af IT-risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i revisionsperioden.	Ingen afvigelser konstateret.

Informationssikkerhedspolitikker

Retningslinjer for styring af informationssikkerhed

Kontrolmål: Formålet er at sikre, at der gives retningslinjer for og understøttelse af 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	Informationssikkerhedspolitikken gennemgås en gang årligt og godkendes af ledelsen.	Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af informationssikkerhedspolitikken, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden, samt inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen afvigelser konstateret.

Organisering af informationssikkerhed

Intern organisering

Kontrolmål: Formålet er at sikre, at der etableres 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	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 er delt op i 3 niveau: Strategisk, taktisk og operationelt. Alt kommunikation med myndigheder eller interessegrupper varetages af det strategiske niveau. Korrekt funktionsadskillelse kontrolleres en gang årligt af generalsekretæren.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser. Vi har forespurgt til adskillelse af adgang i forhold til funktion. Vi har forespurgt til retningslinjer for kontakt med myndigheder. Vi har forespurgt til kontakt med interessegrupper. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed.	Ingen afvigelser konstateret.

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	Bærbare enheder må ikke efterlades synligt i biler og skal medbringes som håndbagage på flyrejser. Såfremt fortrolige data opbevares på mobile enheder, beskyttes data med passende sikkerhedsprodukter godkendt af de operationelle niveauer. Bærbare enheder må ikke efterlades synligt i biler og skal medbringes som håndbagage på flyrejser. Såfremt fortrolige data opbevares på mobile enheder, beskyttes data med passende sikkerhedsprodukter godkendt af de operationelle niveauer.	Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen. Vi har forespurgt til sikring af fjernarbejdspladser.	Ingen afvigelser konstateret.

Medarbejdersikkerhed

Før ansættelsen

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Inden ansættelse: Der skal som minimum altid deltage mindst 2 fra Emento i samtaler med kandidater ligesom der potentielt kan gennemføres check af kandidater omfattende referencer, CV, uddannelsesmæssige kvalifikationer samt straffeattest. Det er kun ledelsen, der kan verificere kandidaters straffeattest og straffeattester opbevares ikke. Emento indhenter alle kandidaters samtykke til at indhente referencer.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter.	Ingen afvigelser konstateret.

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	Det er kun ledelsen, der kan verificere kandidaters straffeattest og straffeattester opbevares ikke. Kontrol af, at proces for ansættelse er fulgt, sker løbende af ledelsen. Under ansættelse: alle medarbejdere i Emento og leverandører som udfører arbejde på vegne af Emento 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 sikkerhedspolitikken kan medføre en sanktion overfor den ansatte	Vi har forespurgt til ledelsens ansvar for videreformidling af politikker og procedurer, og vi har inspiceret dokumentation for tildeling af ansvar. Vi har forespurgt til videreuddannelse af personale. Vi har forespurgt til retningslinjer for sanktionering.	Ingen afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

Kontrolmål: Formålet er 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	Ved ophør af ansættelsesforhold er fortrolighed også gældende.	Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelsen, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver

Kontrolmål: Formålet er 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	Information skal håndteres i henhold til information classification policy. Al information klassificeres på 4 forskellige niveauer. Det strategiske niveau har ansvar for klassificeringen. Korrekt håndtering af aktiver verificeres minimum en gang årligt af generalsekretæren.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til oversigt af ejerskab for aktiver, og vi har inspiceret oversigten. Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne. Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Klassifikation af information **Kontrolmål: Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
8.2	Information skal håndteres i henhold til information classification policy. Alle databærende aktiver er registreret med ejer og unik ID Al information klassificeres på 4 forskellige niveauer. Det strategiske niveau har ansvar for klassificeringen Korrekt håndtering af aktiver verificeres minimum en gang årligt af generalsekretæren.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken. Vi har forespurgt til mærkning af data, og vi har inspiceret retningslinjerne for mærkning af data. Vi har forespurgt til retningslinjer for håndtering af aktiver.	Ingen afvigelser konstateret.

Mediehåndtering **Kontrolmål: Formålet er at sikre hindring af 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	Alle databærende aktiver er registreret med ejer og unik ID. CTO vedligeholder liste over samtlige informationssystemer. Ved bortskaffelse af datamedier bliver disse sikkerhedsslettet inden bortskaffelse. Bærbare enheder må ikke efterlades synligt i biler og skal medbringes som håndbagage på flyrejser.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til retningslinjer for bortskaffelse af medier. Vi har forespurgt til transport af bærbare medier.	Ingen afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

Kontrolmål: Formålet er at begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Adgangen til at udføre handlinger på Ementos 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 Ementos systemer. Der er etableret procedurer for tildeling og inddragelse af rettigheder. Adgang til interne netværk fra et eksternt netværk går igennem Ementos VPN og benytter 2 faktor godkendelse.	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken. Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.

Administration af brugeradgange

Kontrolmål: Formålet er 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	Det er kun udvalgte medarbejdere, der har adgang til at oprette nye brugere, tildele og ændre passwords i Ementos systemer. Alle medarbejderne er instrueret i håndtering af adgange.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret dokumentation for oprettelse og nedlæggelse af brugere. Vi har forespurgt til proces for tildeling af rettigheder, og vi har inspiceret processen. Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har forespurgt til opbevaring af fortrolige adgangskoder. Vi har forespurgt til proces for periodisk gennemgang af brugere. Vi har forespurgt til procedure for inddragelse af rettigheder, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.3	Emento 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.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen afvigelser konstateret.

Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Det er kun udvalgte medarbejdere, der har adgang til at oprette nye brugere, tildele og ændre passwords i Ementos systemer. Alle medarbejderne er instrueret i håndtering af adgange. Emento har rettigheder til at logge på alle systemer ifm. support. Det er ikke muligt for kunderne selv at ændre i driftsmiljøerne. Generalsekretæren verificerer en gang årligt at procedurer for adgangskontrol er fulgt. Kildekode til Ementos systemer ligger i eksternt depot og kun autoriserede personer har adgang hertil.	Vi har forespurgt til begrænsning af adgang til data, og vi har inspiceret dokumentation for begrænsning. Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen. Vi har forespurgt til system til styring af adgangskoder. Vi har inspiceret løsningen og udvalgte konfigurationer.	Ingen afvigelser konstateret.

Kryptografi

Kryptografiske kontroller

Kontrolmål: Formålet er 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	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 Ementos 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 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.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Ingen afvigelser konstateret.

Fysisk sikring og miljøsikring

Sikre områder

Kontrolmål: Formålet er 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	Alle indgange til Ementos 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 Ementos kontorer. Alle servere er placeret hos en ekstern hosting-leverandør med krav om passende tekniske og organisatoriske sikkerhedsforanstaltninger. Herunder brandslukningsudstyr, nødstrømsanlæg og backupserver på en sikret ekstern lokation, hvortil der dagligt bliver overført en kopi af Ementos data.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør. Vi har inspiceret de fysiske forhold hos virksomhedens kontorer med henblik på at kontrollere den fysiske sikring.	Ingen afvigelser konstateret.

Udstyr **Kontrolmål: Formålet er 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	Generalsekretæren indhenter enten revisor erklæring fra hosting leverandør eller foretager eget tilsyn en gang årligt. Emento har en politik for destruktion af databærende udstyr.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere understøttende forsyninger og sikring af regelmæssig vedligeholdelse af udstyret. Vi har forespurgt til politik for bortskaffelse af udstyr. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og har stikprøvevis inspiceret dokumentation for eftersyn. Vi har endvidere ved genudførelse af kontrol inspiceret den eksterne lokation. Vi har forespurgt på politik for bortskaffelse af databærende medier. Vi har forespurgt til sikring af brugerudstyr uden opsyn, samt stikprøvevis inspiceret, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord.	Ingen afvigelser konstateret.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

Kontrolmål: Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Emento sikrer løbende, at drift og vedligehold af systemer ikke er afhængig af en nøgleperson, men at flere kan sikre driften. 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. Det kontrolleres minimum en gang årligt af den IT-driftsansvarlig, at security procedure for IT-department er fulgt.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistensen af testmiljø.	Ingen afvigelser konstateret.

Malwarebeskyttelse

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

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Der er etableret procedurer for beskyttelse mod malware.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen afvigelser konstateret.

Backup

Kontrolmål: Formålet er at beskytte mod tab af data.

Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.3	Der er etableret procedurer for backup.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen. Vi har forespurgt til opbevaring af backup, og vi har inspiceret erklæring fra underleverandør med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genopprettelse.	Ingen afvigelser konstateret.

Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.4	Der er etableret procedurer for hændelseslog og beskyttelse heraf.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret løsningen. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.
Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.5	Der er etableret procedurer for styring af softwareinstallationer på driftssystemer.	Vi har forespurgt til retningslinjer for installation af software på driftssystemer, og vi har inspiceret retningslinjerne. Vi har forespurgt til rettidig opdatering af driftssystemer, og vi har inspiceret dokumentation for opdatering af driftssystemerne.	Ingen afvigelser konstateret.
Sårbarhedsstyring **Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.6	Der er etableret procedurer for styring af softwareinstallationer på driftssystemer samt sårbarhedsstyring.	Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret dokumentation for styringen. Vi har forespurgt til styring af adgang til programinstallation, og vi har inspiceret dokumentation for begrænsningen af brugere med rettighed til programinstallation.	Ingen afvigelser konstateret.
Overvejelser i forbindelse med audit af informationssystemerne **Kontrolmål: Formålet er at minimere virkningen af auditaktiviteter på systemet.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
12.7	Der er etableret procedurer for håndtering af audit af systemer, herunder både for revision samt for tilsyn fra relevante parter. Der er etableret procedurer for håndtering af audit af systemer, herunder både for revision samt for tilsyn fra relevante parter.	Vi har inspiceret at der er opstillet procedurer for auditkrav og aktiviteter i forbindelse med verifikation af driftssystemer. Vi har yderligere forespurgt til at der er taget stilling i hvilket omfang der gives læseadgang til data for den enkelte auditør.	Ingen afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed

Kontrolmål: Formålet er, 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	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 Ementos firewall. Dette gælder både indgående og udgående trafik.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patching af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen afvigelser konstateret.

Informationsoverførsel

Kontrolmål: Formålet er 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	Alle systemgrupper kører på deres eget VLAN. Opdelingen er beskrevet i systemdokumentationen. Emento overfører ikke, medmindre andet er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til aftaler om dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen afvigelser konstateret.

Anskaffelse, udvikling og vedligeholdelse af systemer

Sikkerhedskrav til informationssystemer

Kontrolmål: Formålet er 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.	Ement A/S' kontrol	REVI-IT's test	Resultat af test
14.1	Udvikling af applikationer til produktionsmiljøet sker udelukkende i udviklingsafdeling af ansatte medarbejdere og/eller konsulenter med særlig forståelse for Ementos kultur og sikkerhed.	Vi har forespurgt til informationssikkerhedsrelaterede krav til virksomhedens løsning, og vi har inspiceret de opstillede krav. Vi har forespurgt til sikring af løsningen på offentlige netværk, og vi har inspiceret løsningen. Vi har forespurgt til sikring af transmissioner, og vi har inspiceret dokumentation for beskyttelse af transmissioner.	Ingen afvigelser konstateret.

Sikkerhed i udviklings- og hjælpeprocesser

Kontrolmål: Formålet er at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingscyklus.

Nr.	Ement A/S' kontrol	REVI-IT's test	Resultat af test
14.2	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 Ementos 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.	Vi har forespurgt til politik for styring af udvikling, og vi har inspiceret politikken. Vi har forespurgt til procedure for styring af systemændringer, og vi har inspiceret proceduren. Vi har forespurgt til test af applikationer i forbindelse med ændringer og opdatering af driftsplatformen, og vi har inspiceret dokumentation for test. Vi har forespurgt til begrænsning af ændringer på softwarepakker. Vi har forespurgt til principper for sikker udvikling, og vi har inspiceret udarbejdede principper. Vi har forespurgt til sikkert udviklingsmiljø, og vi har inspiceret dokumentation for adskillelse mellem udviklingsmiljø og produktionsmiljø. Vi har forespurgt til outsourcet udvikling, og vi har inspiceret dokumentation for begrænsning af adgang for outsourcet udviklere. Vi har forespurgt til systemsikkerhedstest. Vi har forespurgt til systemgodkendelsestest.	Ingen afvigelser konstateret.

Testdata **Kontrolmål: Formålet er at sikre beskyttelse af data, som anvendes til test.**			
Nr.	Emento A/S' kontrol	REVI-IT's test	Resultat af test
14.3	Den enkelte udvikler har ikke direkte adgang til produktionsserverne fra en udvikler PC, men kan koble op igennem en bastionserver. Er det nødvendigt at tilgå kundernes miljø for at yde support eller fejlfinde, sker dette igennem kundens AD eller via en særlig systemadgang med ekstra sikkerhed og logning. CTO gennemgår log heraf periodisk.	Vi har forespurgt til anvendelse af testdata, og vi har inspiceret retningslinjerne for produktion af testdata.	Ingen afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold **Kontrolmål: Formålet er 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	Der indgås fortrolighedserklæringer med alle konsulenter, der får adgang til Ementos systemer. Som udgangspunkt arbejder de udelukkende med hardware og software problemstillinger og har ikke adgang til data. Emento 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 Ementos øvrige medarbejdere.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse hensyntagen til informationssikkerhed. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren.	Ingen afvigelser konstateret.

Styring af leverandørydelser **Kontrolmål: Formålet er 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	Der indhentes revisorerklæring fra eksterne leverandører senest et år efter kontraktindgåelse eller indhentning af sidste revisorerklæring.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Ingen afvigelser konstateret.

Styring af informationssikkerhedsbrud

Styring af informationssikkerhedsbrud og forbedringer

Kontrolmål: Formålet er 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	Emento har procedurer for utilsigtede hændelser. Sikkerhedshændelser bliver registreret og løst uden unødig 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 security procedure for the IT-department og procedurer for informationssikkerhedsbrud.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret procedure til håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til informationssikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet

Kontrolmål: Formålet er at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring.

Nr.	Ement A/S' kontrol	REVI-IT's test	Resultat af test
17.1	Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici imod sikringsomkostninger. Ement har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer. Ement 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.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen. Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabstest, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen Vi har endvidere forespurgt til revurdering af beredskabsplanen.	Ingen afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Ement A/S' kontrol	REVI-IT's test	Resultat af test
17.2	Ement har implementeret formelle nødplaner og procedurer til beredskab, herunder redundans i kernekomponenter.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen afvigelser konstateret.

Overensstemmelse

Gennemgang af informationssikkerheden

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

Nr.	Ement A/S' kontrol	REVI-IT's test	Resultat af test
18.2	Der foretages evaluering af en ekstern IT-revisor samt i forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Ingen afvigelser konstateret.