REVI·IT
IT-REVISION & RÅDGIVNING

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med virksomhedens hosting-ydelse i perioden 01-09-2015 til 31-08-2016

ISAE 3402-II

Solutio ApS
CVR-nr.: 30 56 60 09

oktober 2016

Indholdsfortegnelse

Afsnit 1: Solutio ApS' ledelseserklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Solutio ApS' hostingydelse, 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. Solutio ApS bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Solutio ApS' hostingydelse til kunder i hele perioden fra 01-09-2015 til 31-08-2016. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

- de typer af ydelser, der er leveret, når det er relevant
- de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- relevante kontrolmål og kontroller, udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret 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 behandlingen og rapporteringen af kunders transaktioner.

(ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 01-09-2015 til 31-08-2016

(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 udformet og fungerede effektivt i hele perioden fra 01-09-2015 til 31-08-2016. Kriterierne for denne udtalelse var, at:

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

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

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01-09-2015 til 31-08-2016.

Silkeborg, 31. oktober 2016

Solutio ApS

Brian Reinhold Jensen
Adm. direktør

Afsnit 2: Solutio ApS' beskrivelse af kontroller i forbindelse med drift af deres hostingydelse

Introduktion

Formålet med denne beskrivelse er, at levere information til Solutios kunder og deres revisorer vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

Beskrivelsen har herudover det formål, at give information om de kontroller, der er anvendt for hostingydelser hos Solutio i perioden.

Følgende beskrivelse omfatter de kontrolmål og kontroller hos Solutio, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold, er ikke medtaget i denne beskrivelse.

Beskrivelse af Solutios hostingydelser

Solutio udvikler, administrerer og servicerer en vifte af professionelle hostingydelser for en lang række virksomheder og organisationer i Danmark. Vi arbejder over hele linjen efter at levere løsninger, der kvalitets- og servicemæssigt differentierer sig fra størstedelen af det danske hostingmarked. Med mere end 10 år på bagen har vi erfaret, at graden af kunders tilfredshed har den direkte sammenhæng med niveauet på leverandørens service, tekniske kompetencer og kvaliteten af det hardware, som løsningerne driftes på. Det er derfor i stor stil de værdier, som vi baserer vores forretningsgrundlag på.

Fundamentet i forretningen er et moderne datacenter, som vi drifter med udgangspunkt i, at det skal kunne supportere stabilitet, sikkerhed og en hastighed, der kan imødekomme servicekrav fra kritiske og kvalitetsbevidste kunder. Med vores fagligt erfarne medarbejdere kan vi støtte op omkring mange typer af hostingydelser – altid med yderst kompetent rådgivning.

Organisation

Solutio er en danskejet IT-virksomhed, stiftet i 2000 og som beskæftiger 8 medarbejdere. Solutio har outsourcet en lang række opgaver der ikke er direkte forbundne med vores kerneydelser, herunder bogføring og en del af markedsføringsopgaverne. Solutio beskæftiger derfor udelukkende teknisk personale og har en meget flad struktur med overlappende roller.

- Driftsgruppen har ansvaret for drift af centrale servere, netværk og virtualiseringsmiljø. Samt drift og implementering af kunders servere.
- Servicedesk (support) tager sig af henvendelser via telefon eller mail, samt overvåger driften i almindelig arbejdstid.
- Sikkerhedsgruppen har ansvaret for udarbejdelse og implementering af sikkerhedspolitikker i driftsmiljøet.
- Servicevagten modtager supportopkald og alarmer uden for almindelig arbejdstid.
- Ledelsen er overordnet ansvarlig for IT-sikkerhed og at IT-politikken overholdes.

Risikostyring i Solutio ApS

Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores hostingydelser. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Risiko- og trusselsvurdering af interne systemer, foretages årligt. Processen gennemføres af den sikkerhedsansvarlige, der udarbejder udkast til sikkerhedsgruppen.

Endelig godkendelse af risiko- og trusselsvurdering foretages af Solutios direktør.

Generelt om kontrolstruktur og -rammer og implementering

Vores kvalitetsstyringssystem er defineret ud fra vores overordnede målsætning om, at levere stabil og sikker it-drift til vores kunder. For at kunne gøre det, har vi indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002:2013 (Regelsæt for styring af informationssikkerhed), og er dermed helt overordnet inddelt i følgende kontrolområder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved beredskabsstyring
- Overensstemmelse.

Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Solutio er medlem af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), og vi bliver i den forbindelse årligt revideret for hvorvidt vi lever op til BFIH's regelsæt der centrerer sig om hvordan vi leverer vores driftsydelser, foretager genetablering, håndterer sikkerhedsopdatering mv.

Kontrolmiljø

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

Informationssikkerhedspolitikker

Vi har defineret vores overordnede metodik og tilgang til levering af vores ydelser, i vores it-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter.

Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien og relevant lovgivning. Ledelsens budskab er kommunikeret til alle medarbejdere i Solutio, og vi opdaterer løbende dokumenterne efter behov, og minimum én gang årligt.

Organisering af informationssikkerhed

Formål
Styring af sikkerhed, drift, og generelt styring af vores processer der munder ud i vores leverance, skal ske ensartet og pålideligt.

Ledelsesopbakning
Det er ledelsen der godkender retningslinjerne for politikker og procedurer, og det er ledelsen der periodisk godkender opdateringer hertil. Årligt foretages der gennemgang af politikker og procedurer for at sikre en opdateret politik.

Politik
Vi har etableret it-sikkerhedspolitik der beskriver hvordan vi overordnet skal håndtere vores forretning og vores leverance. Alle medarbejdere kender til denne via interne håndbøger, og informeres når ledelsen godkender opdateringer til politikken.

Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

Vi har i vores politik defineret hvordan vi samarbejder med eksterne parter. Er der tale om parter som er en integreret del af vores leverancer, skal vi føre tilsyn med underleverandørens etablerede kontroller.

Vores tekniske og logiske sikkerhedsmodel kan ikke afviges. Ønsker kunder ændringer, der efter vores opfattelse slækker på deres, vores eller andre kunders systemer, tager vi en dialog med kunden om en tilsvarende løsning. Dette kan være web-services, kodeordspolitik, IP-forhold mv.

Medarbejdersikkerhed

Formål
Vi vil sikre, at alle i virksomheden er bekendte med deres roller og ansvar – herunder også vores underleverandører og 3. parter, og at alle er kvalificerede og egnede til at udføre deres rolle.

Roller og ansvar og samarbejde med eksterne
Alle i vores virksomhed skal leve op til den rolle, som er tilegnet dem samt følge vores procedurer jvf. vores it-sikkerhedspolitik.

Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres. Vigtigst er, at vi passer på vores kunders data, vores udstyr og dermed vores forretning.

Vi har jobbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar.

Ansættelsesvilkår
Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt hvor forhold omkring alle sider af ansættelsen, herunder ophør, er angivet.

Uddannelse og træning
Medarbejdere, og eksterne parter hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer samt når der sker ændringer.

Fratrædelse
Vi har procedurer der sikrer inddragelse af systemrettigheder og aktiver ved en medarbejders fratrædelse.

Styring af informationsrelaterede aktiver

Formål
Systemer, data og enheder skal sikres og dokumenteres betryggende.

Ejerskab
Via ansvarsfordeling og rollebeskrivelser, er centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige i vores virksomhed. Kunders data og systemer er tilegnet kundens kontaktperson.

Vi arbejder med ejerskab for at sikre, at ingen enheder, systemer eller data bliver glemt i forhold til sikkerhedsopdatering, klassifikation, drift og vedligehold.

Klassifikation af data
For at kunne skelne mellem systemer og data og kunne prioritere herimellem – f.eks. ved genskabelse – er data overordnet set klassificeret. Vores kunders data er klassificeret sammen med vores egne data til samme niveau, mens systemdata for netværk, dokumentation er prioriteret højst.

Kontrakter, SLA
Vi har kontrakter på aftalte ydelser for alle vores kunder. Særlige forhold er beskrevet heri som de var ved aftaleindgåelse. Ændringer hertil er beskrevet i bilag til kontrakt og fremsendt til godkendelse, eller beskrevet i vores support-system.

Vores SLA (Service Level Agreement) beskriver vores generelle vilkår i forbindelse med vores ydelse overfor vores kunder, herunder oppetid, driftsvinduer, support mv.

Fysiske enheder
Software, servere og netværksudstyr inkl. konfiguration er registreret til brug ved dokumentation, overblik over udstyr mv.

Medarbejdere og deres certificeringer
Vores aktiver er i høj grad vores medarbejdere, og vi fører en struktureret metodik i forhold til vores medarbejderes kvalifikationer, uddannelse og certificeringer.

Adgangsstyring

Formål
Vi vil sikre, at vores og vores kunders adgange ske efter hensigten, og at det alene er personer med autoriseret adgangsniveau, der har adgang til data. Vi vil sikre, at der er sporbarhed i brugen af systemer og data, og adgangen sker it-sikkerhedsmæssigt betryggende.

Vi har defineret en række retningslinjer og procedurer herfor.

Brugeroprettelse og nedlæggelse
Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores kunder er dermed ansvarlige for oprettelse og nedlæggelse. Vores egne brugere oprettes alene på baggrund af skriftligt ønske fra autoriserede personer hos kunden.

Alle brugere skal være personhenførbare, dvs. have tydligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig log-on, så vidt muligt, deaktiveret.

Ønsker kunden brugerkonti til login og systemvedligeholdelse fra tredjepart, er kunden selv ansvarlig for hændelser i forbindelse med brug af sådanne konti.

Kodeord

Alle brugere på tværs af både kundesystemer og egne systemer, har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger i forhold til udformningen af kodeordet.

Koder skal skiftes regelmæssigt, være komplekse, og brugeradgange deaktiveres automatisk hvis brugeren ikke har skiftet kodeordet inden for det definerede tidsrum.

Vores it-sikkerhedspolitik beskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Gennemgang af brugere

For vores egne brugere, gennemgår ledelsen periodisk en liste med oprettede brugere og deres adgangsniveau for at sikre mod adgang for uautoriserede personer.

Brugeradgang til data

Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen.

Vores kunders brugeradgange til kundens systemer og data, bestemmes af vores kunder.

Skærmlås

Alle interne brugerkonti er indstillede til at gå på skærmlås ved inaktivitet i 20 minutter. Dermed sikrer vi, at uautoriseret personale ikke opnår adgang til fortrolige data.

Adgangsveje til netværk og netværksudstyr

Vores netværk er komplekst med mange systemer og kunder, og for at sikre mod uvedkommendes adgang, og for at sikre gennemskueligheden af opbygningen, har vi udformet en række dokumentationer, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv.

Adgangsmuligheder (log-on, VPN, 2-vejs)

Adgang til vores netværk og dermed potentielt til systemer og data, skal ske for kun autoriserede personer.

Adgang uden vores interne netværk, kan ske på forskellig vis som afhænger af den enkelte aftale med kunden. Der er mulighed for at logge på via krypteret VPN-forbindelse via brugernavn og kode. Herudover har visse kunder direkte adgang via MPLS/VPLS/Lan2Lan.

Adgang til systemer og data via mobile enheder

Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode og certifikater, har vi ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange.

Vores kunder har mulighed for samme, og det er op til vores kunder at implementere deres sikkerhedspolitik for deres brugere.

Kryptografi

Vores driftsmiljø er baseret på Microsofts virtualiseringsplatform (HyperV). På de virtuelle servere benyttes Microsofts Windows Servere og forskellige Linux og *bsd distributioner som operativsystem.

Vi stiller serverplatforme og terminalplatforme, baseret på ovenstående, til rådighed for vore kunder. Vi benytter, i den forbindelse, ikke andre subsystemer eller tillægssystemer, der håndterer kryptering, anden

håndtering af systemfiler, end de foranstaltninger og systemer, som benyttes af operativsystemerne og i de omkransende netværkssikkerhedssystemer.

Fysisk sikring og miljøsikring

Formål

Vi vil sikre, at vi har et betryggende fysisk miljø omkring vores hostingydelser og dermed vores kunders data.

Servere, services, data og informationer generelt er afskærmet mod miljømæssige påvirkninger (brand, vand, temperatur mv.), og herudover skal vi have fornøden og betryggende sikring mod hærværk, tyveri mv.

Serverrum

Vores primære driftscenter er i co-lokation hos en underleverandør.

Vores servere er fysisk placeret i lokale, som har monteret køling og brandslukning mv., alene autoriserede personer har adgang til lokalet. Skal eksterne personer (leverandører eller kunder) have adgang til lokalet, er det i følgeskab med en autoriseret medarbejder.

Mindst en gang i kvartalet føres overordnet tilsyn med de fysiske forhold i datacenteret.

Vores sekundære driftscenter fungerer som backup-site for vores primære driftscenter og er placeret i forbindelse med vores kontorer.

Driftssteder og co-lokation

Vi fører natligt data til vores sekundære driftscenter som backup og sikring af vores kunders data og systemer. Såfremt vores primære driftscenter, af den ene eller anden årsag bliver utilgængelig. Vi har aftale med den pågældende leverandør om housing af vores egne servere og netværksudstyr og der er implementeret foranstaltninger mod tyveri, brand, vand og temperatur, efter gældende branchestandarder. Vi modtager årligt revisorerklæring, der afdækker den fysiske sikkerhed hos vores underleverandører.

Kontorer

Vores kontorlokaler er monteret med tyverialarm, som på samme vis som ved alarmering i vores serverrum, alarmerer relevante personer hos vagtselskab og os.

Vi har etableret mulighed for, at vores medarbejdere kan arbejde hjemmefra af hensyn til bl.a. driftsvagt, og vi har politik for, at udstyr (bærbare mv.) ikke benyttes til andet end arbejdsrelaterede forhold, ikke efterlades uden opsyn mv.

Bortskaffelse

Alt databærende udstyr destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt.

Driftssikkerhed

Formål

Vi vil sikre, at vores organisering af implementering, drift og ændring i og af vores ydelser sker struktureret og efter aftale med vores kunder. Vi skal sikre at it-sikkerheden generelt er høj, og via systemer og procedurer sikre at vi ikke kompromitterer vores eller vore kunders systemer og data. Vi skal have procedurer for genskabelse, overvågning og logning af data, og vi skal generelt have opmærksomhed på fortroligheden omkring vores kunders data.

Drift

Vi vil sikre, at vi har en stabil, korrekt og sikker drift af vores systemer. Opgaver fastsættes, uddelegeres, og via procedurer for styring af den operative drift, sikrer vi dette. Vores dokumentationer og processer generelt sikrer herudover, at vi udelukker eller minimerer nøglepersonsafhængighed.

Ændringshåndtering

Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og tilrettelagt hensigtsmæssigt i forhold til interne forhold. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer. Herudover følges en proces omkring udvikling og test, og accept fra både os og fra kundens side.

Uanset hvilken ændring, der er tale om, sikres det altid, som minimum, at;

- Alle væsentlige ændringer drøftes, prioriteres og godkendes af ledelsen
- Alle væsentlige ændringer testes
- Alle ændringer på backbone servere godkendes før idriftsættelse
- Alle ændringer idriftsættes på et fastsat tidspunkt efter aftale med forretningen og kunder
- Der fortages fallback-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis de ikke fungerer
- Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt

Afhængighed af nøglepersoner

Vores organisation gør, at vi kan have overlap inden for alle opgaver og systemer, sikrer vi via dokumentationer og beskrivelser – og via kompetente og flittige medarbejdere – at medarbejdere eller nye medarbejdere kan påbegynde et arbejde på et system, som vedkommende ikke har operationel og historisk erfaring med. Vi opererer med dobbeltroller på alle systemer således, at den primære ansvarlige medarbejder har ansvar for at kommunikere praktiske forhold til kollegaer.

Kapacitet og systemtest

Via vores generelle overvågningssystem, har vi sat grænseværdier for hvornår vores overordnede systemer, og dermed vores kunders systemer, skal skaleres op af hensyn til elektronisk plads, svartider mv. Når vi opsætter nye systemer foretages test af funktionalitet og herunder kapacitet- og performancetest.

Skadevoldende kode

Vi har implementeret scannings- og overvågningssystemer til at opdage kendt skadevoldende kode, dvs. hvad vi og vores kunder – via vores platforme – kan risikere at blive inficeret med på internettet, via mails mv. vi har antivirus-systemer på relevante servere, systemer til overvågning af internetbrug og trafik, sikringer i øvrige tekniske og centrale installationer (firewall mv.), og herudover er vores kundesystemer sikret mod at almindelige brugere kan installere programmer og tilgå systemfiler.

Sikkerhedskopiering

Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder.

Vi har etableret en plan for verificering af hvorvidt sikkerhedskopieringen fungerer samt en test af hvordan systemer og data praktisk kan retablereres. Der føres en log over disse tests således, at vi kan følge op på om vi kan ændre på procedurer og processer for at højne vores løsning.

Med mindre andet er aftalt med vores kunder, foretager vi sikkerhedskopiering af hele deres miljø hos os. Vi foretager sikkerhedskopiering af vores egne systemer og data på samme vis, som vores kunders systemer og data.

Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering. Der tages backup af alle databærende servere hver nat. Der laves backup af øvrige servere en gang hver uge. Sikkerhedskopi føres fra driftssteder til backup-site (hos os). Dermed er data fysisk separeret fra vores driftssystemer, og efter endt afvikling, foretages der en automatiseret verificering af, hvorvidt datamængde og indhold mellem vores driftssystem og backup-site, stemmer overens.

En ansvarlig medarbejder (Support-vagten) sikrer herefter, at sikkerhedskopieringen er sket. Hvis der er fejl i backupjobs foretages det fornødne og herefter logføres dette.

Hvis der er opsat backup af lokale enheder (Remote Backup) er kunden selv ansvarlig for at sikre, at backup-jobs kører korrekt.

Det er kundens ansvar at sikre at backupjobs inkluderer de filer/mapper der ønskes backup af. Såfremt kunden konfigurerer backupjobs med et krypteringskodeord, er kunden selv ansvarlig for at dette krypteringskodeord opbevares forsvarligt og sikkert. Mistes dette krypteringskodeord vil hverken kunden eller Solutio være i stand til at reetablere data.

Håndtering af databærende medier

Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (USB-nøgler, CD/DVD) uden forudgående aftale med kunderne samt ved passende fysisk beskyttelse mod miljømæssige påvirkninger (varme mv.) samt hærværk og tyveri.

Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt.

Vores dokumentation er naturligvis livsvigtig for os, og på alle måder fortrolig i forhold til omverdenen. For dels at have mulighed for at have dokumentationen tilgængelig også i forbindelse med fejl eller nedbrud på egne servere, men samtidig for at sikre fortroligheden af informationerne, har vi informationerne fordelt på flere steder og platforme.

På alle operationelle bærbare computere i organisationen, er harddiskene krypterede.

Overvågning og logning

Vores driftsmedarbejdere foretager den daglige overvågning af vores systemer via automatiserede systemer til måling af grænseværdier.

I dagtimerne ses alarmer på overvågningsskærme der overvåges af vores support-vagt. Udenfor almindelig arbejdstid, sker alarmering via sms til vagthavende driftstekniker, såfremt kritiske hændelser konstateres.

Hændelser for login og logout på vores platforme logføres.

I kraft af, at vi alle benytter personhenførbare brugerkonti, er det muligt at konstatere hvilke personer der i givet fald har været logget på.

Udover hændelseslogning har vi også proaktiv logning, der overvåger ressourceforbrug så vi alarmeres når grænseværdier for eks. diskplads, ram-forbrug m.m. nås.

Styring af driftssoftware

Via vores medlemskab af BFIH, er vi forpligtede til at sikre, at kritiske sikkerhedsopdateringer implementeres inden for 2 måneder efter frigivelse. Dette sikrer vi ved, at vi efter strukturerede processer afvejer alle væsentlige opdateringer og implementerer dem inden for tidsrammen.

Kommunikationssikkerhed

Netværkssikkerhed

Vi mener at have sikret data og systemer inde i netværket, men det ydre værn mod uvedkommende adgang til vores netværk, er af højeste prioritet.

Adgang til vores systemer fra vore kunder, sker enten via de offentlige netværk, hvor adgang sker via krypteret adgang, eller via MPLS/VPLS. Adgang og kommunikation mellem enheder på det primære og sekundære driftscenter, sker via VPLS.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.

Vi er ansvarlige for driften og sikkerheden hos os, dvs. fra og med systemerne hos os og ud til internettet (eller MPLS/VPLS). Vore kunder er selv ansvarlige for at kunne tilgå internettet.

Ekstern datakommunikation

Ekstern datakommunikation sker alene via mails, idet vores kunders adgang og brug af vores servere, ikke betragtes som ekstern datakommunikation.

Fortrolige informationer udveksles ikke via mails, uden de – eller de medfølgende vedhæftede filer – er krypterede eller kodeord beskyttede. Førstegangskodeord til kundesystemer fremsendes via mails, men disse skal ændres ved første log-on. Glemte kodeord, personoplysninger, bestillinger mv. håndteres af Servicedesken og først efter vores medarbejdere har konstateret, at det er den rigtige og autoriserede person, vi har kontakt til.

Anskaffelse, udvikling og vedligehold af informationssystemer

Formål

Vi vil sikre, at alle nyanskaffelser og implementeringer af servere, systemer, services og software håndteres på struktureret og sikker vis.

For at alle aspekter af nye tiltag (indfasning af ny hardwareplatforme, softwareplatforme og andre tilsvarende systemer og processer forbundet med vores service) håndteres sikkert, struktureret og risikoafvejet.

Denne beskrivelse omhandler ikke udvikling eller tilpasning af software eller programmel.

Projektstyring

Opgaver af en vis størrelse, som kan være væsentlige ændringer i vores generelle driftssystem på tværs af kunder, eller implementering af kundeløsninger baseret på vores standardydelse, har vi en klar og struktureret projektstyring for at sikre en ensartet styring af projektet.

Vores projektmodel er baseret på vores egen og praktiske metodik, men er inddelt i en række faser: Analyse, design, test, implementering, test og evaluering. Hver fase indeholder accept fra interessent (kunde, eller ved interne opgaver, fra vores ledelse). Hver fase dokumenteres således, at der efterfølgende er gennemsigtighed for fasens udvikling og afslutning.

Et projekt kan blive til som et resultat af en ændringsanmodning (change), en sikkerhedshændelse (incident), ved et projekteret internt tiltag eller ved implementering af nye kunder.

Systemændringer håndteres efter vores model til formålet, proceduren er beskrevet i ”afsnittet” Systemændringer.
Ganske kort så er modellen bygget op efter fire forskellige systemændringer, Standard, Minor, Major og Emergency.

Væsentlige ændringer i driftssystemer

Vores driftssystem består af en kompleks konfiguration, og når vi planlægger ændringer heri – selv når disse er af mindre karakter, men som kan have en væsentlig påvirkning – drøftes det internt på driftsmøder. Først herefter foretages ændringen, efter godkendelse fra ledelsen. Ændringen sker i vores fastsatte servicevinduer, og vi har forøget overvågning efter test og implementering. Vi planlægger samtidig et tilbagerulningsscenarie, og vi beskriver dels ændringen og opdaterer vores dokumentation.

Vores driftsmiljø er baseret på Microsoft-platforme med virtuelle servere fra Microsoft. Vi stiller serverplatforme og terminalplatforme baseret på Remote Desktop Services til rådighed for vores kunder. I den forbindelse benytter vi ikke andre subsystemer eller tillægssystemer, der håndterer kryptering, anden håndtering af systemfiler, end de foranstaltninger og systemer, som vi benytter i Microsoft systemerne samt i de omkransende netværkssikkerhedssystemer.

Leverandørforhold

Underleverandører

Hvor vi bruger underleverandører fører vi tilsyn med de aftalte leverancer, idet disse skal efterleve vores egne politikker for ydelseslevering, herunder vores forretningsvilkår med vores kunder.

Som omtalt under 'Fysiske sikkerhed' har vi aftale med ekstern virksomhed om placering af driftsservere hos dem. Det er en professionel virksomhed som lever af at sælge plads til servere til virksomheder som os. Vi henviser til førnævnte afsnit for forhold omkring Co-location og kontroller forbundet hermed.

Styring af informationssikkerhedsbrud

Formål

Håndtering af sikkerhedshændelser tager vi meget alvorligt. Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser såsom opdateringer af patches, virusinficerede filer og systemer, overvågning for hackerangreb mv. for at sikre, at vi beskytter vores og vores kunders systemer og data bedst muligt.

Rapportering af sikkerhedshændelser

Vores support-system, hvori vi håndterer alle sager for kunder og interne forhold, er samtidig vores system til håndtering af sikkerhedshændelser. Heri kan vi eskalere forhold således, at opgaver får højere prioritet end andre. Herudover vil sikkerhedshændelser afstedkommet fra hhv. egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret fra vores hotline til driftsafdelingen med samtidig orientering til ledelsen.

Vi holder os fagligt opdaterede vha. producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Via vores medlemskab af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark) har vi etableret kontakt til hotline hos DK-CERT, hvor vi gensidigt har aftale om orientering ved væsentlige sikkerhedsrelaterede forhold vedrørende internettrafik.

Håndtering af sikkerhedshændelser

Reaktionen i forbindelse med sikkerhedshændelser er beskrevet i vores procedurer, og dokumenter, vedr. sikkerhed, herunder graden af information og evt. aktivering af beredskab.

Vores medarbejdere indgår i en driftsvagtordning således, at vi kan reagere 24 timer i døgnet.

Indenfor almindelig arbejdstid håndteres første reaktion af servicedesken.

Herefter foretages det fornødne for at orientere kunder og omverden, udbedre forholdet.

Via vores medlemskab af BFIH, er vi forpligtede til at sikre, at kritiske sikkerhedsopdateringer implementeres inden for 2 måneder efter frigivelse. Dette sikrer vi ved, at vi efter strukturerede processer afvejer alle væsentlige opdateringer og implementerer dem inden for tidsrammen.

Evaluering af sikkerhedshændelser

En sikkerhedshændelse kan – afhængig af forholdet – blive genstand for efterfølgende efterforskning. Dette kan ske internt af hensyn til evaluering og eventuel ændring i procedurer, tekniske eller logiske forhold. Det er også muligt, at der ved kriminelle forhold skal ske en politimæssig efterforskning. I alle tilfælde vil vores logføring og øvrige overvågningssystemer kunne benyttes til at evaluere på sikkerhedshændelsen.

Informationssikkerhedsaspekter ved beredskabsstyring

Formål

Vi vil have mulighed for at genoptagelse af vores primære og centrale forretningsprocesser og systemer efter en katastrofelignende situation.

Beredskabsplan

Skulle der opstå en nødsituation, har Solutio udarbejdet en beredskabsplan. Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen. Planen testes som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation.

Planen og procedurerne er forankret i vores driftsdokumentation og -procedurer.

Via vores medlemskab af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), er vi forpligtet til, at vi inden for 3 dage kan retablere enhver enhed i vores datacenter. Dette sikrer vi ved, at vi har afvejet risici, klassificeret enheder i vores driftsapparat, og har procedurer der sikrer, at vi i vores beredskabsplanlægning kan foretage udskiftning af vores driftsplatform, så de leverede ydelser vil retableres rettidigt.

Redundans

I vores primære driftscenter har vi fuld redundans på alle relevante enheder, som køling, strøm, internetlinjer, firewalls, switche, servere og storage.

Overensstemmelse

Overensstemmelse med lovbestemte og kontraktlige krav

Vi er ikke underlagt særlig lovgivning i forhold til vores ydelse. Vores kunder kan dog være, og de steder, er vores understøttelse heraf aftalt særskilt.

Gennemgang af informationssikkerhed

Vi lader os årligt revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse. I kraft af, at vi er medlemmer af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), skal vi årligt kunne attestere at vi følger rammerne inden for ISO 27002:2013. Omtalte revisorerklæring sikrer dette, ligesom BFIH ønsker ekstern revisors bekræftelse på vores overholdelse af foreningens øvrige krav omhandlende forsikringsforhold, gennemsigtighed i forretningsvilkår, selskabsretlige forhold for vores virksomhed, mv. disse bekræftelser fra revisor er hjælp til BFIH's certificering af vores virksomhed.

Ændringer i perioden

Gennem perioden er der sket ganske få væsentlige ændringer. Vi har:

- Udskiftet core-netværksudstyr
- Forbedret rutinerne for kontrol af bl.a. backup
- Optimeret system til yderligere funktionsadskillelse for daglige driftsopgaver.
- Etableret flere mindre procedurer for at sikre drift og stabilitet, primært omkring opgavehåndtering i servicedesk.
- Fortsat arbejdet med indgåelse af kontrakter med kunder vi har overtaget i forbindelse med overtagelsen af SkolePlan.

Komplementerende kontroller

Solutios kunder er, med mindre andet er aftalt, ansvarlige for at etablere forbindelse til Solutios servere. Herudover er Solutios kunder, med mindre andet er aftalt, ansvarlige for:

- periodisk gennemgang af kundens egne brugere.
- at der opretholdes sporbarhed i tredjeparts software som kunden selv administrerer.
- Solutios standard backup-rutine benytter Change Block Tracking (CBT) teknologi. Solutio garanterer ikke for konsistens af backup såfremt kundespecifikke softwareprodukter ikke understøtter denne teknologi. Dette er oftest relevant for databaser, eksempelvis Dynamics NAV Native. Kunden er selv ansvarlig for at sikre at specifikke softwareprodukter understøtter CBT teknologi.
- backup af lokale enheder er kunden selv ansvarlig for at sikre, at backup jobs kører korrekt.
- at sikre at backupjobs inkluderer de filer/mapper der ønskes backup af. Såfremt kunden konfigurerer backupjobs med et krypteringskodeord, er kunden selv ansvarlig for at dette krypteringskodeord opbevares forsvarligt og sikkert. Mistes dette krypteringskodeord vil hverken kunden eller Solutio være i stand til at reetablere data.

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

Til ledelsen hos Solutio ApS, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Solutio ApS' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af Solutio ApS' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hostingydelse i perioden 01-09-2015 til 31-08-2016, samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Solutio ApS' ansvar

Solutio ApS er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. Solutio ApS er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål og for udformningen, implementeringen og effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

Vores 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.

Firmaet anvender ISQC 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 Solutio ApS' beskrivelse (afsnit 2) og om udformningen og funktionaliteten af de 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 udformet og fungerer effektivt.

Opgaven med afgivelse af en erklæring med sikkerhed 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 udformede 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 endvidere en vurdering af den samlede præ-

sentation 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

Solutio ApS' beskrivelse i afsnit 2 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 vigtige efter sine 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Solutio ApS' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

(a) at beskrivelsen af kontroller, således som de var udformet og implementeret i hele perioden 01-09-2015 til 31-08-2016, 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 udformede i hele perioden fra 01-09-2015 til 31-08-2016
(c) at 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 hele perioden 01-09-2015 til 31-08-2016.

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 er udelukkende tiltænkt kunder, der har anvendt Solutio ApS' hostingydelse, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 31. oktober 2016

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CRISC, adm. direktør

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

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Solutio ApS har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 01-09-2015 til 31-08-2016.

Vi har således ikke nødvendigvis testet alle de kontroller, som Solutio ApS har nævnt i sin beskrivelse i afsnit 2.

Kontroller udført hos Solutio ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos Solutio ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Risikovurdering og -håndtering

Risikovurdering

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
4.1	Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores hostingydelser. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risiko- og trusselsvurdering af interne systemer foretages årligt. Processen gennemføres af den sikkerhedsansvarlige, der udarbejder udkast til sikkerhedsgruppen. Endelig godkendelse af risiko- og trusselsvurdering foretages af Solutios direktør.	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. Ydermere har vi observeret, at der er en kontrol for periodisk revurdering af risikoanalysen.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
5.1	Vi har defineret vores overordnede metodik og tilgang til levering af vores ydelser i vores it-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter. Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien og relevant lovgivning. Ledelsens budskab er kommunikeret til alle medarbejdere i Solutio, og vi opdaterer løbende dokumenterne efter behov, og minimum én gang årligt.	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 dokumentation for, 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 væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
6.1	Vi opererer med dobbeltroller på alle systemer således, at den primære ansvarlige medarbejder har ansvar for at kommunikere praktiske forhold til kollegaer. Vores projektmodel er baseret på vores egen og praktiske metodik, men er inddelt i en række faser: Analyse, design, test, implementering, test og evaluering. Hver fase indeholder accept fra interessent (kunde, eller ved interne opgaver, fra vores ledelse). Hver fase dokumenteres således, at der efterfølgende er gennemsigtighed for fasens udvikling og afslutning.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen. Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret retningslinjer for funktionsadskillelse. Vi har endvidere inspiceret dokumentation for differentieret adgang. Vi har forespurgt til kontakt med interessegrupper, og vi har inspiceret dokumentation for kontakt. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter, og vi har stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
6.2	Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode og certifikater, har vi ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange. Vores kunder har mulighed for samme, og det er op til vores kunder at implementere deres sikkerhedspolitik for deres brugere. Adgang udenfor vores interne netværk, kan ske på forskellig vis, som afhænger af den enkelte aftale med kunden. Der er mulighed for at logge på via krypteret VPN-forbindelse via brugernavn og kode. Herudover har visse kunder direkte adgang via MPLS/VPLS/Lan2Lan.	Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen. Vi har forespurgt til sikring af fjernarbejdspladser, og vi har inspiceret løsningen.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
7.1	Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør, er angivet.	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 væsentlige afvigelser konstateret.

Under ansættelsen

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
7.2	Vi har jobbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar. Medarbejdere, og eksterne parter, hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer, samt når der sker ændringer. Vores aktiver er i høj grad vores medarbejdere, og vi fører en struktureret metodik i forhold til vores medarbejderes kvalifikationer, uddannelse og certificeringer.	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, og vi har stikprøvevis inspiceret dokumentation for videreuddannelse. Vi har forespurgt til retningslinjer for sanktionering, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

Kontrolmål: Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
7.3	Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør, er angivet.	Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen væsentlige afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver

Kontrolmål: Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
8.1	Systemer, data og enheder skal sikres og dokumenteres betryggende. Via ansvarsfordeling og rollebeskrivelser er centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige i vores virksomhed. Kunders data og systemer er tilegnet kundens kontaktperson. Vi arbejder med ejerskab for at sikre, at ingen enheder, systemer eller data bliver glemt i forhold til sikkerhedsopdatering, klassifikation, drift og vedligehold. Software, servere og netværksudstyr inkl. konfiguration er registreret til brug ved dokumentation, overblik over udstyr mv. Vi har procedurer, der sikrer inddragelse af systemrettigheder og aktiver ved en medarbejders fratrædelse.	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. Vi har stikprøvevis inspiceret dokumentation for, at proceduren er fulgt.	Ingen væsentlige afvigelser konstateret.

Klassifikation af information

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
8.2	For at kunne skelne mellem systemer og data og kunne prioritere herimellem – fx ved genskabelse – er data overordnet set klassificeret. Vores kunders data er klassificeret sammen med vores egne data til samme niveau, mens systemdata for netværk, dokumentation er prioriteret højst.	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, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Mediehåndtering **Kontrolmål: Formålet er at sikre hindring af uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
8.3	Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (USB-nøgler, CD/DVD) uden forudgående aftale med kunderne samt ved passende fysisk beskyttelse mod miljømæssige påvirkninger (varme mv.) samt hærværk og tyveri. Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt. Vores dokumentation er naturligvis livsvigtig for os, og på alle måder fortrolig i forhold til omverdenen. For dels at have mulighed for at have dokumentationen tilgængelig også i forbindelse med fejl eller nedbrud på egne servere, men samtidig for at sikre fortroligheden af informationerne, har vi informationerne fordelt på flere steder og platforme. På alle operationelle bærbare computere i organisationen er harddiskene krypterede.	Vi har forespurgt til retningslinjer for anvendelsen af bærbare medier, og vi har inspiceret retningslinjerne. Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til procedure for destruktion af hardware, og vi har inspiceret proceduren. Vi har endvidere inspiceret dokumentation for sikker destruktion af hardware i perioden. Vi har forespurgt til transport af bærbare medier.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
9.1	Vi vil sikre, at vores og vores kunders adgange sker efter hensigten, og at det alene er personer med autoriseret adgangsniveau, der har adgang til data. Vi vil sikre, at der er sporbarhed i brugen af systemer og data, og at adgangen sker it-sikkerhedsmæssigt betryggende. Vi har defineret en række retningslinjer og procedurer herfor. Adgang til vores netværk, og dermed potentielt til systemer og data, skal ske for kun autoriserede personer. Adgang udenfor vores interne netværk kan ske på forskellig vis, som afhænger af den enkelte aftale med kunden. Der er mulighed for at logge på via krypteret VPN-forbindelse via brugernavn og kode. Herudover har visse kunder direkte adgang via MPLS/VPLS/Lan2Lan.	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 væsentlige afvigelser konstateret.

Administration af brugeradgange **Kontrolmål: Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
9.2	Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores kunder er dermed ansvarlige for oprettelse og nedlæggelse. Vores egne brugere oprettes alene på baggrund af skriftligt ønske fra autoriserede personer hos kunden. Alle brugere skal være personhenførbare, dvs. have tydligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig log-on, så vidt muligt, deaktiveret. Førstegangskodeord til kundesystemer fremsendes via mails, men disse skal ændres ved første log-on. Glemte kodeord, personoplysninger, bestillinger mv. håndteres af Servicedesken, og først efter vores medarbejdere har konstateret, at det er den rigtige og autoriserede person, vi har kontakt til. For vores egne brugere gennemgår ledelsen periodisk en liste med oprettede brugere og deres adgangsniveau for at sikre mod adgang for uautoriserede personer.	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 i perioden. 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, og vi har inspiceret dokumentation for betryggende opbevaring. 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 væsentlige afvigelser konstateret.

Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
9.3	Vores it-sikkerhedspolitik beskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
9.4	Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevante for arbejdsindsatsen. Alle brugere på tværs af både kundesystemer og egne systemer har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger i forhold til udformningen af kodeordet. Koder skal skiftes regelmæssigt, være komplekse, og brugeradgange deaktiveres automatisk, hvis brugeren ikke har skiftet kodeordet inden for det definerede tidsrum.	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, og vi har inspiceret løsningen. Vi har endvidere inspiceret de opsatte krav til kvaliteten af kodeord.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
11.1	Vores servere er fysisk placeret i lokale, som har monteret køling og brandslukning mv., alene autoriserede personer har adgang til lokalet. Skal eksterne personer (leverandører eller kunder) have adgang til lokalet, er det i følgeskab med en autoriseret medarbejder. Vores primære driftscenter er i co-lokation hos en underleverandør. Vi modtager årligt revisorerklæring, der afdækker den fysiske sikkerhed hos vores underleverandører. Servere, services, data og informationer generelt er afskærmet mod miljømæssige påvirkninger (brand, vand, temperatur mv.), og herudover skal vi have fornøden og betryggende sikring mod hærværk, tyveri mv. Vores kontorlokaler er monteret med tyverialarm, som på samme vis som ved alarmering i vores serverrum, alarmerer relevante personer hos vagtselskab og os.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold og har inspiceret erklæringen for betryggende fysisk sikring, herunder perimetersikring, adgangskontroller og miljømæssig sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har stikprøvevis inspiceret dokumentation for tildeling og nedlæggelse af adgang til driftsfaciliteter. Vi har inspiceret de fysiske forhold hos Solutios kontorer med henblik på at kontrollere den fysiske sikring. Vi har forespurgt til levering af pakker og varer.	Ingen væsentlige afvigelser konstateret.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
11.2	Vores servere er fysisk placeret i lokale, som har monteret køling og brandslukning mv., alene autoriserede personer har adgang til lokalet. Skal eksterne personer (leverandører eller kunder) have adgang til lokalet, er det i følgeskab med en autoriseret medarbejder. Mindst en gang i kvartalet føres overordnet tilsyn med de fysiske forhold i datacenteret. Vores sekundære driftscenter fungerer som backup-site for vores primære driftscenter og er placeret i forbindelse med vores kontorer. Alt databærende udstyr destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt. Alle interne brugerkonti er indstillede til at gå på skærmlås ved inaktivitet i 20 minutter. Dermed sikrer vi, at uautoriseret personale ikke opnår adgang til fortrolige data.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring, herunder identificering af understøttende forsyninger og vedligeholdelse af udstyret. Vi har observeret, at erklæring fra underleverandør dækker perioden frem til d. 31. maj 2016, og vi har derfor forespurgt til dokumentation for periodisk eftersyn hos leverandør. Vi har stikprøvevis inspiceret dokumentation for eftersyn hos underleverandøren. Vi har forespurgt til sikring af kabler, og vi har inspiceret erklæring fra leverandør. Vi har forespurgt til politik for bortskaffelse af udstyr, og vi har inspiceret dokumentation for sikker bortskaffelse. Vi har forespurgt til sikring af brugerudstyr uden opsyn, og vi har stikprøvevis inspiceret, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord, og vi har inspiceret politikken.	Ingen væsentlige afvigelser konstateret.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.1	Vi vil sikre, at vores organisering af implementering, drift og ændring i og af vores ydelser sker struktureret og efter aftale med vores kunder. Vi skal sikre, at it-sikkerheden generelt er høj, og via systemer og procedurer sikre, at vi ikke kompromitterer vores eller vore kunders systemer og data. Vi skal have procedurer for genskabelse, overvågning og logning af data, og vi skal generelt have opmærksomhed på fortroligheden omkring vores kunders data. Vi vil sikre, at vi har en stabil, korrekt og sikker drift af vores systemer. Opgaver fastsættes, uddelegeres, og via procedurer for styring af den operative drift, sikrer vi dette. Vores dokumentationer og processer generelt sikrer herudover, at vi udelukker eller minimerer nøglepersonsafhængighed. Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og er tilrettelagt hensigtsmæssigt i forhold til interne forhold. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer. Herudover følges en proces omkring udvikling og test, samt accept fra både os og fra kundens side. Via vores generelle overvågningssystem har vi sat grænseværdier for, hvornår vores overordnede systemer, og dermed vores kunders systemer, skal skaleres op af hensyn til elektronisk plads, svartider mv. Når vi opsætter nye systemer, foretages test af funktionalitet og herunder kapacitet- og performancetest.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til procedure for ændringsstyring, og vi har inspiceret proceduren. Vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har inspiceret dokumentation for overvågning af kapacitet. Vi har endvidere inspiceret dokumentation for styring af kapacitet. Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for anvendelse af testmiljø.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.2	Vi har implementeret scannings- og overvågningssystemer til at opdage kendt skadevoldende kode, dvs. hvad vi og vores kunder – via vores platforme – kan risikere at blive inficeret med på internettet, via mails mv. Vi har antivirus-systemer på relevante servere, systemer til overvågning af internetbrug og trafik, sikringer i øvrige tekniske og centrale installationer (firewall mv.), og herudover er vores kundesystemer sikret mod, at almindelige brugere kan installere programmer og tilgå systemfiler.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen væsentlige afvigelser konstateret.

Backup

Kontrolmål: Formålet er at beskytte mod tab af data.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.3	Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder. Vi har etableret en plan for verificering af, hvorvidt sikkerhedskopieringen fungerer samt en test af, hvordan systemer og data praktisk kan retablereres. Der føres en log over disse tests således, at vi kan følge op på, om vi kan ændre på procedurer og processer for at højne vores løsning. Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering. Der tages backup af alle databærende servere hver nat. Der laves backup af øvrige servere en gang hver uge. Sikkerhedskopi føres fra driftssteder til backup-site (hos os). Dermed er data fysisk separeret fra vores driftssystemer, og efter endt afvikling, foretages der en automatiseret verificering af, hvorvidt datamængde og indhold mellem vores driftssystem og backup-site, stemmer overens.	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 verificere, at backup opbevares forsvarligt. Vi har forespurgt til kontrol med backup, og vi har stikprøvevis inspiceret kontrol for backup. Vi har forespurgt til test af genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse.	Ingen væsentlige afvigelser konstateret.

Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.4	Hændelser for login og logout på vores platforme logføres. I kraft af, at vi alle benytter personhenførbare brugerkonti, er det muligt at konstatere, hvilke personer der i givet fald har været logget på. Udover hændelseslogning har vi også proaktiv logning, der overvåger ressourceforbrug, så vi alarmeres når grænseværdier for eks. diskplads, ram-forbrug mm. nås.	Vi har forespurgt til logning af brugeraktivitet, og vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til overvågning og gennemgang af logoplysninger, og vi har inspiceret dokumentation for overvågning og gennemgang af logoplysninger. 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 væsentlige afvigelser konstateret.

Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.5	Via vores medlemskab af BFIH er vi forpligtede til at sikre, at kritiske sikkerhedsopdateringer implementeres inden for 2 måneder efter frigivelse. Dette sikrer vi ved, at vi efter strukturerede processer afvejer alle væsentlige opdateringer og implementerer dem inden for tidsrammen.	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 væsentlige afvigelser konstateret.

Sårbarhedsstyring **Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.**			
Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
12.6	Via vores medlemskab af BFIH er vi forpligtede til at sikre, at kritiske sikkerhedsopdateringer implementeres inden for 2 måneder efter frigivelse. Dette sikrer vi ved, at vi efter strukturerede processer afvejer alle væsentlige opdateringer og implementerer dem inden for tidsrammen. Vi holder os fagligt opdaterede vha. producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.	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 væsentlige afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed

Kontrolmål: Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
13.1	Vi mener at have sikret data og systemer inde i netværket, men det ydre værn mod uvedkommende adgang til vores netværk er af højeste prioritet. Adgang til vores systemer fra vore kunder sker enten via de offentlige netværk, hvor adgang sker via krypteret adgang, eller via MPLS/VPLS. Adgang og kommunikation mellem enheder på det primære og sekundære driftscenter sker via VPLS. Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen væsentlige afvigelser konstateret.

Informationsoverførsel

Kontrolmål: Formålet er at opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
13.2	Ekstern datakommunikation sker alene via mails, idet vores kunders adgang og brug af vores servere ikke betragtes som ekstern datakommunikation. Fortrolige informationer udveksles ikke via mails, uden de – eller de medfølgende vedhæftede filer – er krypterede eller kodeordbeskyttede.	Vi har forespurgt til politikker for dataoverførsel, og vi har inspiceret politikken. Vi har forespurgt til aftaler om dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information, og vi har inspiceret retningslinjerne. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
15.1	Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere. Vi har i vores politik defineret, hvordan vi samarbejder med eksterne parter. Er der tale om parter som er en integreret del af vores leverancer, skal vi føre tilsyn med underleverandørens etablerede kontroller.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse, at der er etableret sikkerhedsforhold i aftalen. Vi har inspiceret erklæring fra underleverandør med henblik på at efterse, om der er observeret væsentlige forhold.	Ingen væsentlige afvigelser konstateret.

Styring af leverandørydelser

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

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
15.2	Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere. Vi har i vores politik defineret, hvordan vi samarbejder med eksterne parter. Er der tale om parter som er en integreret del af vores leverancer, skal vi føre tilsyn med underleverandørens etablerede kontroller.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
16.1	Håndtering af sikkerhedshændelser tager vi meget alvorligt. Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser såsom opdateringer af patches, virusinficerede filer og systemer, overvågning for hackerangreb mv. for at sikre, at vi beskytter vores og vores kunders systemer og data bedst muligt. Reaktionen i forbindelse med sikkerhedshændelser er beskrevet i vores procedurer, og dokumenter vedr. sikkerhed, herunder graden af information og evt. aktivering af beredskab. En sikkerhedshændelse kan – afhængig af forholdet – blive genstand for efterfølgende efterforskning. Dette kan ske internt af hensyn til evaluering og eventuel ændring i procedurer, tekniske eller logiske forhold. Det er også muligt, at der ved kriminelle forhold skal ske en politimæssig efterforskning. I alle tilfælde vil vores logføring og øvrige overvågningssystemer kunne benyttes til at evaluere på sikkerhedshændelsen.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling samt 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, og vi har stikprøvevis inspiceret håndtering af sikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
17.1	Skulle der opstå en nødsituation, har Solutio udarbejdet en beredskabsplan. Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen. Planen testes som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation. Planen og procedurerne er forankret i vores driftsdokumentation og -procedurer. Via vores medlemskab af BFIH (Brancheforeningen for IT-Hostingvirksomheder i Danmark), er vi forpligtet til, at vi inden for 3 dage kan retablere enhver enhed i vores datacenter. Dette sikrer vi ved, at vi har afvejet risici, klassificeret enheder i vores driftsapparat, og har procedurer der sikrer, at vi i vores beredskabsplanlægning kan foretage udskiftning af vores driftsplatform, så de leverede ydelser vil retableres rettidigt.	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 test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Ingen væsentlige afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
17.2	I vores primære driftscenter har vi fuld redundans på alle relevante enheder, som køling, strøm, internetlinjer, firewalls, switche, servere og storage.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige 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.	Solutio ApS' kontrol	REVI-IT's test	Resultat af test
18.2	Vi lader os årligt revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse. I kraft af, at vi er medlemmer af BFIH (Brancheforeningen for IT-Hostingvirksomheder i Danmark), skal vi årligt kunne attestere, at vi følger rammerne inden for ISO 27002:2013. Omtalte revisorerklæring sikrer dette, ligesom BFIH ønsker ekstern revisors bekræftelse på vores overholdelse af foreningens øvrige krav omhandlende forsikringsforhold, gennemsigtighed i forretningsvilkår, selskabsretlige forhold for vores virksomhed, mv. Disse bekræftelser fra revisor er hjælp til BFIH's certificering af vores virksomhed.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden hos Solutio. Vi har forespurgt til interne kontroller med politikker, og vi har inspiceret dokumentation for interne kontroller. Vi har forespurgt til kontroller for undersøgelse af teknisk overensstemmelse, og vi har inspiceret dokumentation for undersøgelse i perioden.	Ingen væsentlige afvigelser konstateret.