MAJ 2016

DANDOMAIN A/S

ISAE 3402 TYPE 2 ERKLÆRING

Revisors erklæring vedrørende de generelle it-kontroller i tilknytning til driften af DanDomains hostingaktiviteter.

Beierholm
Statsautoriseret Revisionspartnerselskab
Ellebjergvej 52, 2.
2450 København SV
CVR-nr. 32 89 54 68
Tlf +45 33 38 98 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Erklæringsopbygning

Kapitel 1:

DanDomain A/S' ledelseserklæring

Kapitel 2:

DanDomain A/S' beskrivelse af de generelle it-kontroller for driften af hostingaktiviteter

Kapitel 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de generelle it-kontroller, deres udformning og funktionalitet

Kapitel 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

KAPITEL 1:

DanDomain A/S' ledelseserklæring

Beskrivelsen af DanDomains generelle it-kontroller i kapitel 2 er udarbejdet til brug for kunder, der har anvendt eller påtænker at anvende DanDomains hostingaktiviteter, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. DanDomain bekræfter hermed, at

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af DanDomain hostingaktiviteters generelle it-kontroller i hele perioden 1. januar 2015 - 31. december 2015. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) redegør for, hvordan kontrollerne 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 styring af de generelle it-kontroller
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af DanDomain, 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 DanDomain generelle it-kontroller foretaget i perioden 1. januar 2015 - 31. december 2015.

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller 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 kontroller, som den enkelte kunde måtte anse som vigtig 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 1. januar 2015 - 31. december 2015. Kriterierne for dette udsagn er, 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 forhindrer opnåelsen af de anførte kontrolmål, og

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2015 - 31. december 2015.

(C) den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af DanDomain standardaftale, grundlaget for hostingaktiviteter og ydelser omkring de generelle it-kontroller. Kriterierne for dette grundlag var:

(i) Service Level Agreement Rev. DK 1.06

(ii) Forretningsbetingelser version 2.7

Randers, den 23. maj 2016

Ronnie Bach Nielsen, Adm. direktør

DanDomain A/S, Normansvej 1, DK-8920 Randers NV, Tel (+45) 8777 9045, CVR: 25476255

KAPITEL 2:

DanDomain A/S' beskrivelse af de generelle it-kontroller for driften af hostingaktiviteter

Indledning

Formålet med nærværende beskrivelse er at levere information til DanDomains kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører, ISAE 3402.

Beskrivelsen giver herudover information om de kontroller, der er anvendt for driften i DanDomains hostingaktiviteter i perioden 1. januar 2015 - 31. december 2015.

Beskrivelse af DanDomain A/S

DanDomain A/S er blandt de førende danske hosting-virksomheder inden for domæneregistrering, webhosting, webshop og IT-outsourcing. DanDomain A/S' kunder spænder bredt fra private til større virksomheder, foreninger og offentlige institutioner.

Virksomheden er grundlagt i 1999 og har i alle årene vækstet organisk. Grundfilosofien for DanDomain A/S defineres ud fra et DNA bestående af 4 kerneværdiord: Empatisk, kundecentrisk, kompetent og ekstraordinær.

Dette betyder, at vi sætter kunden i centrum i alt, hvad vi tænker, siger og gør. Med udgangspunkt i vores kompetente medarbejdere er missionen at gøre IT-ydelserne så enkle som muligt for kunden, kombineret med markedets bedste kundeservice.

DanDomain råder over eget state-of-the-art datacenter opbygget efter alle best-practices. Fakta om DanDomain A/S

- 80 medarbejdere
- Mere end 67.000 kunder
- Grundlagt i 1999
- Gazellepris i 2005, 2006, 2007, 2008 og 2009
- Initiativtager til og medlem af BFIH

DanDomain leverer hostingydelser i et moderne og professionelt hostingcenter. Hostingydelser kan skræddersyes til den enkelte kundes behov, men tager udgangspunkt i standardløsninger. Vi tilbyder ydelser lige fra enkle domænekøb og outsourcing-løsninger til egetudviklet shopsystem.

Omfang for denne beskrivelse

DanDomain A/S er leverandør af services inden for IT, og kerneaktiviteten i DanDomain er leverance af hosting og driftsydelser. Overvågning og support er enten på kunders egne platforme placeret i DanDomains datacenter, eller på løsninger der afvikles på DanDomains egen infrastruktur, som kunder lejer sig ind på. DanDomain har som leverandør ansvaret for at etablere og opretholde passende procedurer og kontroller med henblik på at finde og forebygge fejl, for således at overholde de i aftalerne stillede krav. Det er netop denne kerneaktivitet: hosting og driftsydelser, samt drift og vedligeholdelse, der danner grundlag for nærværende beskrivelse.

Forretningsstrategi/ it-sikkerhedsstrategi

Det er DanDomains strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici.

DanDomain har tre overordnede strategiske pejlepunkter:

- DanDomain hjælper danske virksomheder til en optimal brug af moderne informationsteknologi
- DanDomain arbejder primært med administrative systemer, netværksløsninger og internet/intranetløsninger
- DanDomain er en god arbejdsplads for en stabil og veluddannet medarbejderstyrke

DanDomain arbejder med it-sikkerhed på et forretningsstrategisk niveau og arbejder derfor løbende med at sikre et højt service- og kvalitetsniveau. Ledelsen prioriterer gennem selskabets sikkerhedspolitik, at it-sikkerhed skal være og er en vigtig del af selskabets virksomhedskultur.

DanDomain har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27002:2013, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitik
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhed
- Informationssikkerhedsaspekter ved nød-, beredskabs– og reetableringsstyring

De implementerede kontrolmål og sikringsforanstaltninger hos DanDomain fremgår af bilag 1 til denne beskrivelse.

DanDomain A/S' organisation og organisering af it-sikkerheden

DanDomains formelle ansvar for IT-sikkerhedspolitik og -procedurer er placeret hos CSO/Adm. direktør. IT-sikkerhedspolitik-ken godkendes af virksomhedens bestyrelse.

Hos DanDomain eksisterer der en klar opdelt organisation, hvad ansvar angår, og DanDomain har udførlige ansvars- og rollebeskrivelser på alle niveauer, lige fra ledelsesniveau til de enkelte driftsmedarbejdere.

Alle medarbejdere holdes løbende opdateret med ændringer i IT-sikkerhedspolitikken. Koordinering af udmelding og undervisning planlægges i sikkerhedsrådet.

DanDomain har implementeret en række infrastrukturtiltag for at sikre integriteten, tilgængeligheden og hemmeligholdelsen af data. Disse er:

- Automatiseret redundant brandslukningsanlæg
- Redundant køling af datacentre, basert på inrow køling
- Separat datacenter til backup (backup gemmes ikke på samme lokation som autoriativ data)
- Nødstrømsanlæg der kan holde DanDomains hostingaktiviter kørende i min. 12 timer uden bystrømsleverance
- Redundante internetforbindelser fra to seperate udbydere (Telia og Globalconnect) med seperate fysiske infaldsveje

Der anvendes ikke underleverandører til noget af ovenstående leverance, men alle overnstående punkter anvender underleverandører til kvartalsvis test of kontrol.

Ved brug af eksterne samarbejdspartnere udarbejdes samarbejdsaftale, inden arbejde påbegyndes.

Risikostyring i DanDomain A/S

Det er DanDomains politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift. DanDomain gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

DanDomain har indarbejdet faste procedurer for risikovurdering af forretningen og specielt hostingcenteret. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vurderes relevante i forbindelse med at revurdere vores generelle risikovurdering. Ansvaret for risikovurderingen ligger hos den adm. direktør og skal efterfølgende forankres og godkendes hos virksomhedens ledelse.

Som led i ovenstående it-sikkerhedsstrategi arbejder DanDomain med den danske/internationale standard for it-sikkerhed - ISO27002 – som primær referenceramme for it-sikkerheden. Arbejdsprocessen omkring it-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at DanDomain til hver en tid er i overensstemmelse med kunders krav og behov.

Håndtering af it-sikkerhed

Ledelsen hos DanDomain har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet DanDomains struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

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

DanDomains it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående.

Alle servere og netværksenheder er dokumenteret i DanDomains dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

Sikkerhedspolitikken sætter de grundlæggende politikker for DanDomains infrastruktur, og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet, så DanDomain har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

It-sikkerhedspolitikken er opbygget med ISO27002 som referenceramme. På it-sikkerhedsområdet har DanDomain implementeret de nødvendige procedurer og kontroller i forhold til de enkelte områder inden for ISO27002, som er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, som er implementeret hos DanDomain.

HR, medarbejdere og uddannelse

Alle hos DanDomain skal leve op til den rolle, som er tilegnet dem samt følge vores procedurer jf. vores it-sikkerhedspolitik. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres. Hos DanDomain har det topprioritet, at man passer på kunders data, virksomhedens udstyr og dermed forretningen.

Rolle- og ansvarsfordelingen, herunder opgaver og ansvar i forhold til sikkerheden, er defineret i de udarbejdede rollebeskrivelser, medarbejdernes ansættelseskontrakt, samt i it-sikkerhedspolitikken.

Generelle vilkår for ansættelse omfatter, at medarbejderen til enhver tid er underlagt den gældende it-sikkerhedspolitik.

DanDomain betragter medarbejderne som vigtige aktiver, og fører en struktureret politik i forhold til medarbejdernes kvalifikationer, uddannelse og certificeringer. Der afholdes løbende, dog minimum årligt, kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler.

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Det dokumenteres ved hjælp af relevante certificeringer og intern uddannelse.

DanDomain skal leve op til en række krav fra Microsoft, herunder specifikke krav om at et bestemt antal konsulenter har bestået bestemte produktcertificeringer, som løbende skal fornyes. DanDomain sikrer via løbende produkttræning og kursusdeltagelse at opretholde denne høje certificeringsstatus.

Fysisk sikkerhed

DanDomain har sit eget TIER3 datacenter. Dette TIER-level stiller krav om en høj grad af redundans på de fleste delte infrastrukturkomponenter (køling, UPS mv.).

DanDomains datacenter er placeret på indhegnet grund. Hoveddøren er altid låst og kan kun oplåses af medarbejdere med adgangskort. Datacenteret er beliggende i en kælder, hvortil der er dobbelte ståldøre samt sikkerhedsrullegitre.

Alene autoriserede personer får adgang til lokalerne via den etablerede procedure, og der følges periodisk, minimum årligt, op på, hvilke personer der har denne adgang.
Eksterne personer (leverandører eller kunder) får kun adgang til lokalet i følgeskab med en autoriseret medarbejder.

Alle virksomhedens lokaler er sikret med tyverialarm, som i tilfælde af indbrud alarmerer den private vagtcentral, og relevante personer hos DanDomain alarmeres via SMS og e-mail. Ingen uvedkommende vil kunne gå uhindret omkring i DanDomains kontorer, idet receptionen er bemandet, og yderdøre er aflåste.

Til sikring af driftsfaciliteterne anvendes køle- og brandanlæg, der periodisk testes og serviceres. Endvidere er der monteret tilbageløbssikringer på alle kloakker og afløb, og der er monteret fugtmåler i serverrum og tilstødende lokaler og gang. Der er tillige opsat systemer, som overvåger temperatur og røgudvikling i serverrummet.

Serverne er fysisk placeret i et aflåst lokale, som har monteret køling og brandslukning mv. Serverrummet indeholder centralt netværksudstyr, og er således sikret på samme vis som servere. Strømforsyning til datacenterdrift er UPS- og generatorbeskyttet.

Vedligeholdelse af UPS, køl, generatorer mv. håndteres af vores leverandør jf. serviceaftale. Vedligehold planlægges og koordineres med datacenteransvarlig medarbejder, der ligeså er til stede, når vedligehold udføres i selve datacenteret.

Vi fører natligt data til vores co-location hos vores underleverandør, herunder backup af kunders data og systemer. Vi har en aftale med den pågældende leverandør om housing af vores egne servere, og der er implementeret tilsvarende foranstaltninger mod tyveri, brand, vand og temperatur, som vi har i vores eget serverrum.

Brugerstyring/ adgangssikkerhed

Hos DanDomain er der etableret politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.

DanDomains kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores egne brugere oprettes alene på baggrund af skriftlig autorisation fra systemejer.

DanDomains it-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige, og det alene er brugeren selv, der må kende kodeordet. Medarbejderne skriver årligt under på, at de har læst og forestået seneste version af it-sikkerhedspolitikken.

Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

- Krav til password - alle brugere oprettet i DanDomains centrale brugerdatabase skal skifte password hver 90. dag. Password skal være på mindst 8 tal eller bogstaver, og de seneste 24 passwords kan ikke bruges igen.
- Krav til pauseskærm - pauseskærm er aktiveret på alle vores brugere for at beskytte dem mod uautoriseret adgang.

Overvågning

DanDomain har etableret automatisk overvågning af servere, storagesystemer, netværk, m.v. og har 1. line support personale på vagt 24/7/365. Ligeledes er 2nd og 3rd level support på vagt i en turnusordning således, at nødvendig kompetence er til rådighed 24/7/365.

Hvis en fejl konstateres, afsendes alarm både visuelt på en overvågningsskærm og på SMS. Opstår en situation, hvor der konstateres en fejl på en komponent, der ikke er en del den automatiske overvågning, tages der skridt til, at den fremover registreres i systemet.

Hostingcenteret overvåges med hensyn til strømafbrydelser, temperatur, brand, vand, luftfugtighed, og hele hostingcenteret er i øvrigt kameraovervåget.

Hvis der sker hændelser, som kan påvirke driften, vil overvågningssystemet automatisk alarmere vagtberedskabet, og der forefindes en indarbejdet procedure for eskalation, sluttende med at den adm. direktør involveres.

Drift af hosting-aktiviteter

Faste driftsopgaver udføres med fast interval. Disse opgaver styres i DanDomains driftsafdeling for manuelle driftsopgaver, og programmatisk af egenudviklet jobqueue. Alle kontroller mht. faste opgaver befinder sig ved drift og kontrolleres i høj grad af CSO/SO, eller driftschef.

Backup

Formålet med backup er at sikre, at kundens data i DanDomains hostingcenter kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid. Der tages kryds-backup af alle data til andet fysisk serverrum.

DanDomain sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis og efter de aftaler, der eksisterer med DanDomains kunder.

DanDomain har etableret en testplan for verificering af, hvorvidt sikkerhedskopieringen fungerer, samt en test af, hvordan systemer og data praktisk kan reetableres. Der føres en log over disse tests, så der kan følges op på, om der foreligger forbedringsmuligheder for procedurer og processer.

Med mindre andet er aftalt med kunderne, foretager DanDomain sikkerhedskopiering af hele deres miljø. DanDomain foretager sikkerhedskopiering af egne systemer og data på samme vis, som for sine kunders systemer og data.

DanDomain har udarbejdet faste procedurer og beskrivelser for opsætning og vedligehold. Hver nat føres der en fuld kopi af data fra DanDomains centrale systemer til en co-location ved hjælp af backup-systemet. Dermed er data fysisk separeret fra driftssystemer.

En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket samt foretager det fornødne, hvis jobbet er fejlet og logfører herefter dette.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres. Dette sker for at sikre systemerne mod nedetid og uautoriseret adgang, og for at implementeringen sker på en kontrolleret måde.

Alle servere med adgang fra internettet og terminalservere med Windows opdateres automatisk om natten, mens alle andre servere opdateres manuelt 1 gang månedligt med opdateringer.

DanDomain har udarbejdet en fall back plan i forbindelse med patch management. Formålet med fall back planen er at sikre, at systemerne kan komme tilbage i normal drift, hvis opdateringen ikke virker efter hensigten.

Styring af it-sikkerhedshændelser

DanDomains helpdesk-system, hvori langt de fleste sager for kunder og interne håndteres, er samtidig system til håndtering af sikkerhedshændelser. Heri kan forhold eskaleres således, at opgaver får højere prioritet end andre. Herudover vil sikkerhedshændelser afstedkommet fra henholdsvis egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blives eskaleret fra DanDomains hotline til driftsafdelingen med samtidig orientering af ledelsen.

Gennem DanDomains medlemskab af BFIH har man etableret kontakt til hotline hos DK-CERT, hvor man gensidigt har aftale om orientering ved væsentlige sikkerhedsrelaterede forhold vedrørende internettrafik.
Sikkerhedshændelser og svagheder i DanDomain systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i DanDomain er bekendt med procedurerapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af DanDomains drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til ledelsen.

Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Beredskabsstyring

DanDomain har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer. Beredskabsplanen omfatter it-systemer og processer på alle niveauer. Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen.

I udformningen af beredskabsplaner, og review heraf, vurderes disse løbende i forhold til DanDomains gældende it-sikkerhedspolitik.

Via medlemsskabet af BFIH (Brancheforeningen for IT-Hosting virksomheder i Danmark) er DanDomain forpligtet til, inden for 3 dage, at kunne retablere enhver enhed i datacenteret. Dette sikres ved, at man har afvejet risici, klassificeret enheder i driftsapparatet og har procedurer, der sikrer, at beredskabsplanlægningen kan foretage udskiftning af driftsplatformen, så de leverede ydelser vil retableres rettidigt.

Der foretages løbende real life test af beredskabet. Efter endt udførsel analyseres resultatet og på den baggrund opdateres de relevante elementer, procedurer og planer.

Væsentlige ændringer i forhold til it-sikkerhed

Ingen væsentlige ændringer for perioden.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Ovenstående beskrivelse er baseret på ovennævnte ramme, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for forretningssystemer og brugersystemer, som drives via DanDomains hostingydelser, er kundernes eget ansvar. Kunderne har ansvaret for sikring af de nødvendige kontroller i forbindelse med systemudvikling, anskaffelse og ændringshåndtering.

DanDomain er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til DanDomains hostingaktiviteter. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunderne er ansvarlige for datatransmission til DanDomains hostingaktiviteter, og det er kundernes ansvar at skabe den nødvendige datatransmission til DanDomains datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

DanDomains beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af DanDomain hostingaktiviteter. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

DanDomain har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2013

5. Informationssikkerhedspolitik
- 5.1. Retningslinjer for styring af Informationssikkerhed

6. Organisering af informationssikkerhed
- 6.1. Intern organisering
- 6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed
- 6.3. Før ansættelse
- 6.4. Under ansættelsen
- 6.5. Ansættelsesforhold ophør eller ændring

8. Styring af aktiver
- 8.1. Ansvar for aktiver
- 8.2. Klassifikation af informationer
- 8.3. Mediehåndtering

9. Adgangsstyring
- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar
- 9.4. Styring af system- og applikationsadgange

11. Fysisk sikkerhed og miljøsikring
- 11.1. Sikre områder
- 11.2. Udstyr

12. Driftsikkerhed
- 12.1. Driftsprocedurer og ansvarsområder
- 12.2. Malwarebeskyttelse
- 12.3. Backup
- 12.4. Logning og overvågning
- 12.5. Styring af driftssoftware
- 12.6. Sårbarhedsstyring

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

15. Leverandørsikkerhed
- 15.1. Informationssikkerhed i leverandørforhold
- 15.2. Styring af leverandørydelser

16. Styring af informationssikkerhedsbrud
- 16.1. Styring af informationssikkerhedsbrud og forbedringer

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- 17.1. Informationssikkerhedskontinuitet
- 17.2. Redundans

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de generelle it-kontroller, deres udformning og funktionalitet.

Til kunder af DanDomain A/S' hostingydelser og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om DanDomains beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af de generelle it-kontroller, som udføres i forbindelse med driften af DanDomain hostingaktiviteter til behandling af kunders transaktioner i perioden 1. januar 2015 - 31. december 2015, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter helhedsmetoden, hvilket betyder, at denne erklæring også omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere.

DanDomain er medlem af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), hvilket medfører en række krav, som virksomheden skal overholde for at opnå retten til at bruge BFIH's kvalitetsmærke – Certificeret IT-hosting. Vores erklæring omfatter også disse forhold, som består – ud over de fysiske forhold såsom server, hardware, LAN, WAN og firewall – af en konklusion om:

- hvorvidt DanDomain har implementeret kritiske sikkerhedsopdateringer inden for 2 mdr. fra frigivelse, og
- hvorvidt DanDomain kan reetablere enheder i datacenter inden for 3 dage.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. virksomhedsbeskrivelsen kapitel 2, afsnittet om komplementerende kontroller.

DanDomain ansvar

DanDomain er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2 (inkl. bilag 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholm' uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi 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.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om DanDomains beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til 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 overholder etiske krav samt planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlig henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelse, udformning og funktionalitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som DanDomain har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

Det er Beierholm' opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos DanDomain

DanDomains beskrivelse 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 vigtig efter deres særlige forhold. Endvidere vil kontroller hos DanDomain, som følge af deres art, muligvis ikke forhindre eller opdage 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 serviceleverandører kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af de af DanDomain generelle it-kontroller til hostingaktiviteter, således som det var udformet og implementeret i hele perioden 1. januar 2015 - 31. december 2015, i alle væsentlige henseender er retvisende, og
b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. januar 2015 - 31. december 2015, og
c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. januar 2015 - 31. december 2015, og
d) at kontrollerne i forhold til de særlige krav, som er tilknyttet DanDomains medlemskab af BFIH jf. virksomhedsbeskrivelsen i kapitel 2, var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden 1. januar 2015 - 31. december 2015.

Vi skal bemærke, at der for de enkelte kunder kan være specifikke forhold, som gør, at den generelle konklusion ikke er dækkende. Hvis det er aftalt mellem kunden og DanDomain, at der udarbejdes en specifik erklæring vedrørende kundens kontrakt, vil forholdene fremgå heraf.

Beskrivelse af testkontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt DanDomain kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 23. maj 2016

Beierholm P/S
statsautoriserede revisorer

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
It Auditor, Manager

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med IASE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27002:2013.

Derefter opremser vi i første kolonne de aktiviteter, som DanDomain jf. sin dokumentation har iværksat for at leve op til kontrolmålene, i anden kolonne hvordan vi har valgt at teste, om det forholder sig som beskrevet, og i tredje kolonne, hvad resultatet af vores test har været.

Hvad angår periode har vi i vores test forholdt os til, om DanDomain har levet op til kontrolmålene i perioden 1. januar 2015 - 31. december 2015.

INDLEDENDE KONTROLMÅL:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af hostingaktiviteter. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede hostingaktiviteter. Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for hostingaktiviteter arbejdes med en løbende risikovurdering, som opstår som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risikovurderingen er forankret ned igennem de organisatoriske forhold. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Det er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendte af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes efter planlagte intervaller.	Vi har indhentet og revideret DanDomains seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrollet, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via DanDomains intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til kunder er håndteret.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos Komplex its har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikringsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering. Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer. Der foreligger passende forretningsgange for medarbejdere omkring angivelse af tavshedserklæring.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til hostingaktiviteter. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder. Gennem forespørgsler og stikprøve på ansættelsesaftale har vi kontrolleret, at medarbejdere i DanDomain er bekendte med deres tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Revisionen har stikprøvevis inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Der skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Via fastlagte arbejdsprocesser og procedurer er det sikret, at alle nye medarbejdere får oplyst deres særlige ansvar og rolle i forbindelse med ansættelse i DanDomain. Herunder de fastlagte rammer for deres arbejde og den omkringliggende it-sikkerhed. Eventuelle sikkerhedsansvar er fastlagt, og nærmere beskrevet gennem stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Medarbejderne er bekendte med deres tavshedspligt via en underskrevet ansættelseskontrakt og via DanDomains personalepolitik.	Vi har kontrolleret, at de af ledelsen udarbejdede forretningsgange og procedurer i forbindelse med ansættelse og ansættelsesophør er overholdt. Gennem stikprøver har vi testet, om ovenstående forretningsgange og procedurer er overholdt både i forhold til ansættelse og ansættelsesophør. Ved interview har vi kontrolleret, at væsentlige medarbejdere for hostingaktiviteter er bekendt med deres tavshedspligt. Vi har gennemgået centrale medarbejderes stillingsbeskrivelser, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revisionen har påset, at DanDomains personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos DanDomain.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til hostingaktiviteter får et passende beskyttelsesniveau.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver. Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af hostingaktiviteter.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af DanDomain hostingaktiviteter. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow systemer for driften af hostingaktiviteter. Vi har ved observationer og forespørgsler kontrolleret, at DanDomain overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data i relation til hostingaktiviteter og den efterfølgende drift af hostingcenter er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har kontrolleret, at der er passende opdeling og tilhørende procedurer/forretningsgange ifm. beskyttelse omkring ejerskab mellem applikationer og data samt øvrige enheder i forhold til DanDomains drift af hostingaktiviteter. Vi har kontrolleret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definition, adskillelse og afgrænsning mellem DanDomains ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler det typisk kunden et eget ansvar at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: • forespurgt ledelsen om hvilke procedurer/kontrolaktiviteter, der udføres. • stikprøvevist gennemgået procedurerne for destruktion af databærende medier, til bekræftelse af at de er formelt dokumenterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for DanDomains adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i DanDomain. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. DanDomain retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger DanDomains retningslinjer, og at autorisationer tildeles i henhold til aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.	Vi har forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i DanDomain. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i DanDomain. • at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i DanDomains systemer, og at der foretages løbende opfølgning på registrerede brugere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Interne brugers adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.	Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder: • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder hver 3. måned • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder hver 6. måned.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer, at der sker skift af standardpassword.	Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i DanDomain. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

	• at standard password ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standard password.	
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (5 tegn), ingen krav til kompleksitet, maksimal løbetid (max 90 dage), lige som password opsætninger medfører, at password ikke kan genbruges (husker de seneste 5 versioner). Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i DanDomain. Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for: • minimum længde for password • minimum levetid for password • maksimal levetid for password • minimum historik for password • lockout efter fejlede login forsøg	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser. Der skal opbygges sikkerhedstiltag, som sikrer, at der undgås tab af, skader på eller kompromittering af virksomhedens informationsaktiver samt sikre at der undgås forstyrrelser af virksomhedens forretningsaktiviteter. Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr samt nødvendige forsyninger som el, vand og ventilation samt kabelinstallationer.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret en sikker fysisk afgrænsning, som beskytter de områder, hvorfra hostingaktiviteter driftes. De sikre områder er beskyttet med adgangskontrol, så kun autoriserede personer kan få adgang. Der er etableret overvågning af områder til af- og pålæsning samt øvrige områder, hvortil offentligheden har adgang.	Jf. serviceleverandørers beskrivelse er den fysiske adgangssikkerhed bl.a. gennemgået og kontrolleret med udgangspunkt i de af ledelsen fastsatte krav. Vi har gennemgået og kontrolleret de fysiske adgange til begge datacentre, som bl.a. sikres via et nøglesystem kombineret med personlig kode, som sikrer begrænset adgang til DanDomains datacenter. Via besøg, interview og observation er det kontrolleret, at adgangen til begge DanDomains datacentre er i overensstemmelse med ovenstående forretningsgange omkring adgangsbegrænsning. Vi har stikprøvevist gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt at personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse. Vi har stikprøvevis gennemgået medarbejdere med adgang til sikre områder og påset, at de er oprettet i henhold til de fastlagte procedurer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Udstyr som er placeret i datacenter beskyttes mod fysiske trusler såsom brand, vandskade, strømafbrydelse, tyveri eller hærværk. Datacenteret er sikret mod forsyningssvigt som elektricitet, vand, varme og ventilation. Der er installeret udstyr til overvågning af indeklima, såsom luftfugtighed. Kabler til brug for datakommunikation og elforsyning er beskyttet imod uautoriserede indgreb.	Vi har gennemgået og kontrolleret, at DanDomains datacenter overholder de af ledelsen fastsatte krav. Revisionen har kontrolleret overholdelsen af de nødvendige sikringsforanstaltninger jf. ISO 27002 afsnit 11 i forholdene til beskyttelse mod skader forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk. Konkret har vi: • påset tilstedeværelse af brandbekæmpelsessystemer og køling i datacenter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Udstyret til brug for hostingaktiviteter vedligeholdes efter forskrifterne for at sikre dets tilgængelighed og pålidelighed. Det udstyr, der benyttes uden for datacenteret, beskyttes efter samme retningslinjer, som gælder for udstyr inden i datacenter, under hensyntagen til de særlige risici ved ekstern anvendelse. Alt udstyr med lagringsmedier kontrolleres for at sikre, at kritiske/følsomme informationer og licensbelagte systemer er fjernet eller overskrevet, når udstyret bortskaffes eller genbruges.	• gennemgået og kontrolleret dokumentation for vedligeholdelse til bekræftelse af, at UPS og dieselgenerator løbende vedligeholdes og testes. • observeret under besøg i datacenter, at der foretages monitering af UPS og dieselgenerator. • påset tilstedeværelse af udstyr til overvågning af indeklima i datacentre. • påset sikring af kabler for datakommunikation og elforsyning. • stikprøvevis gennemgået dokumentationen for at vedligeholdelse af udstyr til beskyttelse mod fysiske trusler sker ved løbende vedligeholdelse. • gennemgået og kontrolleret de af ledelsen udarbejdede procedurer til bortskaffelse af udstyr tilknyttet driften af hostingaktiviteter.	
I forbindelse med anvendelse af datacenter 2 skal sikkerhedstiltagene være ligestillet med kravene til DanDomains eget datacenter.	Gennem revision har vi testet, at datacenter 2 indeholder og overholder de samme tiltag som DanDomains eget datacenter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedure og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedure for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.	Vi har: • forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevist kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Malwarebeskyttelse

At beskytte mod skadevoldende programmer, som eksempelvis virus, orme, trojanske heste og logiske bomber.
Der skal træffes foranstaltninger til at forhindre og konstatere angreb af skadevoldende programmer.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret både forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger, herunder den nødvendige uddannelses- og oplysningsindsats for virksomhedens brugere af informationssystemer mod skadevoldende programmer.	Vi har: • forespurgt og inspiceret de procedurer/ kontrolaktiviteter, der udføres i tilfælde af virusangreb eller –udbrud. • forespurgt og inspiceret de aktiviteter, som skal gøre medarbejdere opmærksomme på forholdsregler ved virusangreb eller udbrud. • Kontrolleret, at servere har installeret antivirusprogrammer, inspiceret signaturfiler, der dokumenterer, at de er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Backup

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foretages sikkerhedskopiering af alle virksomhedens væsentlige informationsaktiver, herunder eksempelvis parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. • stikprøvevis gennemgået backup-log vedrørende backup, for bekræftelse af at backup er gennemført succesfuldt og at tilfælde af mislykkede backup håndteres rettidigt. • gennemgået fysisk sikkerhed (bl.a. adgangsbegrænsning) for intern opbevaringslokation, til bekræftelse af, at backup opbevares betryggende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Logning og overvågning

At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges, og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. DanDomain logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter der udføres, og gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. • stikprøvevis kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. Om muligt overvåges for, om en fejl er ved at opstå, for at kunne handle proaktivt. Alarmer sker igennem en overvågningsskærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms. Der indmeldes statusrapporter pr. mail fra forskellige systemer. Nogle dagligt – andre når der opstår en hændelse i systemet. Driftsvagten har til ansvar dagligt at kontrollere disse mails.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere. • påset, at der afgives alarmer pr. mail og sms ved opståede fejl. • gennemgået statusrapporter • påset, at der er etableret en driftsvagt, samt at denne tjekker rapporter dagligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware samt Sårbarhedsstyring

At sikre, at der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der anvendes faste procedurer og arbejdsgange til håndtering af installation for styresystemer og de tilhørende software opdatering. Ændringer i eksisterende driftssystemer skal følger formaliserede forretningsgange og processer. Der skal løbende indhentes informationer om tekniske sårbarheder omkring de anvendte styresystemer. Sårbarhederne skal løbende evalueres, og der skal iværksættes passende foranstaltninger for håndtering at den tilhørende risiko.	Vi har forespurgt ledelsen, om der er etableret procedurer for change management i DanDomain. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til DanDomains produktionsmiljøer • at ændringer til driftsmiljøer i DanDomain følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. Vi har stikprøvevis inspiceret, at styresystemerne er opdateret efter gældende procedurer, samt at status herpå registreres. Vi har forespurgt ledelsen, om der er etableret procedurer for change management i DanDomain. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til change management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at alle ændringer er underlagt formel godkendelse inden idriftsætning • at ændringer er underlagt formelle konsekvensvurderinger • at der beskrives fall-back planer • at der sker identifikation af systemer, der påvirkes af ændringer • at der sker en dokumenteret test af ændringer inden idriftsætning • at dokumentationen opdateres så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination i et "change board".	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttelse af informationsbehandlingsfaciliteter.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • er etableret et ansvar for procedurer for styring af netværksudstyr • at der er etableret funktionsadskillelse omkring central roller • procedurer og ansvar for styring af netværksudstyr inkl. fjernarbejdspladser • de fornødne lognings- og overvågningsprocedurer skal være etableret • styringen af virksomhedens netværk skal koordineres for at sikre en optimal udnyttelse og et sammenhængende sikkerhedsniveau.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevis inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser. Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår de rette steder i organisationen jf. retningslinjer. Vi har kontrolleret, at ansvaret for håndteringen af kritiske hændelser er klart placeret, og at de tilhørende forretningsgange sikrer, at der sker en hurtig, effektiv og metodisk håndtering af et brud på sikkerhed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering

DanDomain A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for hostingaktiviteter i DanDomain. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har en tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategier og procedurer for kommunikation med Dan-Domains interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Vi har ikke ved vores test konstateret væsentlige afvigelser