Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med udvalgte konsulent og produktydelser i perioden
01-06-2019 til 31-05-2020

ISAE 3402-II

Ditmer A/S

CVR-nr.: 26 09 72 74

Juni 2020

Indholdsfortegnelse

Afsnit 1: Ditmer A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Ditmer A/S' udvalgte konsulent og produktydelser, 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. Ditmer A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Ditmer A/S' udvalgte konsulent og produktydelser der har behandlet kunders transaktioner i hele perioden fra 01-06-2019 til 31-05-2020. 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, herunder behandlede grupper af transaktioner, når det er relevant
- De tilhørende regnskabsregistreringer, underliggende information, og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle, og rapportere transaktioner, herunder korrektion af ukorrekt information, og hvordan information blev overført til de rapporter, der blev 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 implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificerede 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 01-06-2019 til 31-05-2020

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 01-06-2019 til 31-05-2020. Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01-06-2019 til 31-05-2020.

Århus, 18. juni 2020

Ditmer A/S

Morten Ditmer
Adm. direktør

Afsnit 2: Ditmer A/S' beskrivelse af deres generelle it-kontroller

Om Ditmer

Ditmer A/S blev stiftet i 2001. Ditmer har siden 2001 udviklet sig til i dag at have ca. 45 medarbejdere.

Forretningsområder

Ditmer har to forretningsområder: konsulentydelser og produktydelser:

Konsulentydelser
Ditmer udvikler skræddersyet software for offentlige og private kunder. Ditmer varetager som udgangspunkt hele processen for kunden - fra behovsafdækning over løsningsbeskrivelse, UX, agil softwareudvikling, test og implementering til efterfølgende support og vedligehold. Ditmer hoster som udgangspunkt ikke løsningerne for kunderne, men Ditmer får fjernadgang til kundernes løsning med henblik på support og vedligehold. Enkelte kunder har dog indgået aftale med Ditmer om hosting af løsningen.

Projekterne gennemføres oftest på baggrund af et digitalt forretningsudviklingsforløb sammen med kunderne - for de offentlige kunders vedkommende dog ofte efter EU-udbud og en tilhørende specifikation af krav og behov. Ditmer rådgiver kunderne om løsningens udformning ift. fx brugergrænseflader, arkitektur, sikkerhed og teknologier. Det er således kundens valg, hvilke sikkerhedsmæssige tiltag, der prioriteres i løsningerne.

Produktydelser
Ditmer har udviklet en række produkter, som Ditmer selv ejer rettighederne til og udbyder til kunderne som standardsoftware med begrænset mulighed for individuel tilpasning for kunden. Nogle af disse produkter tilbydes som on-premise løsninger, hvor løsningen installeres på kundens servere, mens andre løsninger tilbydes som Software-as-a-Service (SaaS), hvor Ditmer hoster løsningen ved tredjepart og dermed tilbyder kunden en samlet løsning inkl. hosting.

Det drejer sig om følgende produkter: DitmerFlex, Agenda Management Production, Agenda Publication, Agenda Live, EduAdm, LetDialog, Puljestyring, STABS, StudieOptag og SprogTolk. Evt. nye produkter vil blive udviklet og udbudt efter samme procedurer, som de eksisterende produkter.

On-premise løsningerne hostes ved kunden. Ditmer har udviklet løsningen med en række features og en række parametre, hvor kundens konfiguration kan tilpasses. Kunderne har desuden mulighed for at få udviklet særlige integrationer til sine fagsystemer. Ditmer hjælper i nogle tilfælde kunden med opsætningen, herunder bistår kundens it-afdeling med opsætningen af løsningen i kundens it-miljø. Det er således kundens it-afdeling, der fastlægger sikkerhedsniveauet for den enkelte installation.

SaaS løsningerne, som hostes af Ditmer ved en af Ditmer valgt leverandør. Ditmer har også i disse tilfælde udviklet løsningen og tilbyder kunden muligheder for indstilling af parametre, så kundens konfiguration kan tilpasses. Det er mere begrænset, om kunden kan få lavet individuelle udvikling på løsningen. Ditmer opsætter kundens adgang på det driftsmiljø, løsningen hostes på. Ditmer har således fastlagt sikkerhedsniveauet.

Det fremgår tydeligt af den enkelte kundes abonnement, om produktet leveres on-premise eller som SaaS.

Compliance

Både konsulentydelser og produkter leveres til kunderne efter nærmere, skriftlig aftale mellem kunden og Ditmer. Aftalerne baseres som udgangspunkt på Ditmers skabeloner, der er tilpasset Ditmers ydelser. I de situationer, hvor aftalerne er baseret på kundens skabeloner, herunder i forbindelse med udbud eller indkøb på SKI's rammeaftaler, har Ditmer sikret, at ydelsen er tilpasset aftalematerialet.

I de tilfælde, hvor Ditmer behandler persondata for kunden, er der indgået en databehandleraftale, der udgør rammen for persondatabehandlingen. Også disse er som udgangspunkt baseret på Ditmers skabelon, men kan være baseret på andre skabeloner. Også her tilrettelægges behandlingen af persondata til det aftalte, og det vil eksempelvis fremgå tydeligt af databehandleraftalen, om løsningen leveres on-premise eller som hostet/SaaS-løsning.

Målsætninger

Ditmers målsætninger er:

Kunderne skal opleve, at det er så god en forretning at arbejde sammen med Ditmer, at de vælger os igen. Ditmer skal skabe en proces, der bringer kunderne sikkert i mål. Derfor skal vi have relevante ydelser og kompetencer, de rette produkter og velfungerende processer.

Medarbejderne skal synes, at Ditmer er Danmarks bedste arbejdsplads. Derfor skal vi sikre udviklingsmuligheder, god ledelse og en menneskelig kultur.

Økonomien skal give så gode resultater, at vi kan være risikovillige og investere i fremtiden. Det kræver en sund pipeline og en god overskudsgrad.

Informationssikkerhedspolitikkens anvendelsesområde

Sikkerhedspolitikken

Ditmers informationssikkerhedsregler er baseret på ISO27001/27002-standarden, som indeholder retningslinjer for organisationers informationssikkerhedsstandarder og informationssikkerhedsledelse, herunder valg, implementering og styring af kontroller, idet organisationens informationssikkerhedsmæssige risikomiljø(er) tages i betragtning.

Informationssikkerhedspolitikken gennemgås årligt og godkendes af ledelsen.

Håndtering af risici

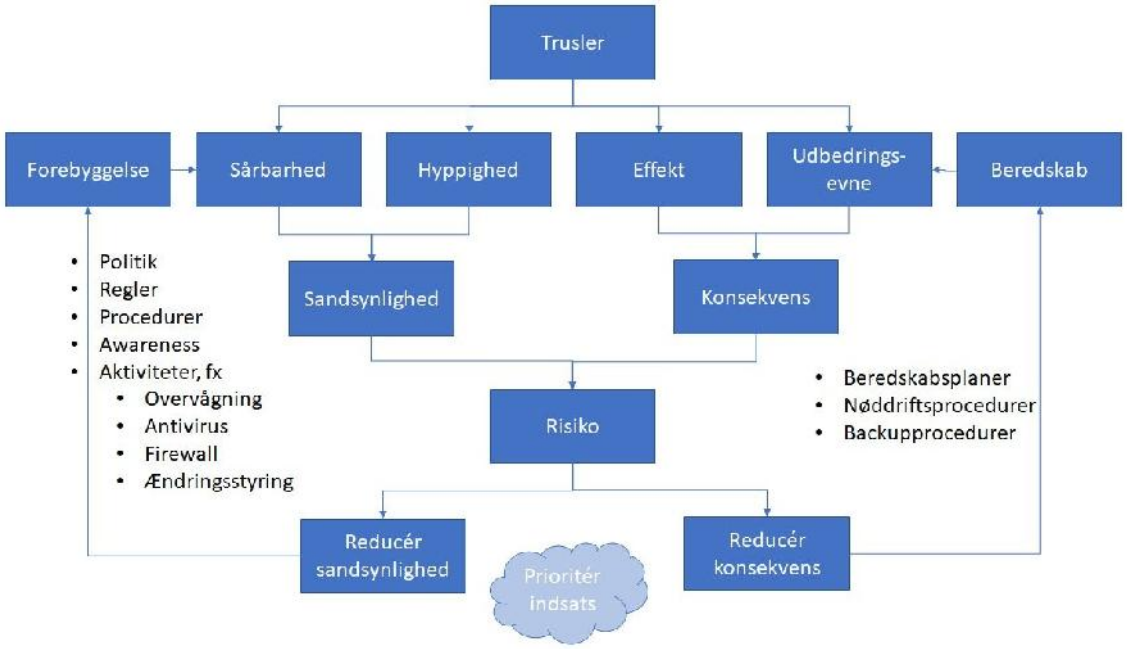
Ditmer følger løbende udviklingen i risici og muligheder for at sikre, at Ditmers informationssikkerhedsarbejde tager højde for de væsentligste risici og muligheder, så vi kan

- sikre, at vi opnår de tilsigtede resultater,
- forebygge eller minimere uønskede virkninger og
- opnå løbende forbedring.

Vi planlægger:

- handlinger til håndtering af disse risici og muligheder, og hvordan
  - handlingerne integreres og implementeres i de informationssikkerhedsrelaterede ledelsessystemprocesser og
  - den resultatrelaterede effektivitet af disse handlinger evalueres.

Vi tager generelt udgangspunkt i denne model for håndtering af trusler mod Ditmers informationssikkerhed:



Baseret på denne model udarbejdes der en risikoanalyse for trusler mod forretningskritiske aktiver. Risikoanalysen udarbejdes af den relevante systemansvarlige og Ditmers informationssikkerhedsansvarlige. Hvis risikoanalysen viser en høj sandsynlighed eller en stor konsekvens af en given trussel, laves der en beredskabsplan for hændelsen, og der kan samtidig iværksættes tiltag for at forebygge. Risikoanalysen for det enkelte aktiv gennemgås årligt, og den samlede risikoanalyse godkendes årligt af ledelsen.

Organisering af informationssikkerhed

Intern organisering

Ditmer har et forum for informationssikkerhed, der har ansvar for at sikre, at informationssikkerhedspolitikken er synlig, koordineret og i overensstemmelse med Ditmers mål. Informationssikkerhedsforummet ledes af et medlem af Ditmers øverste ledelsesgruppe.

Sikkerhedsansvarlige systemejere for virksomhedskritiske systemer har ansvar og beføjelser til at sikre tilstrækkelig beskyttelse.

For at mindske risikoen for misbrug af privilegier, skal alle forretningskritiske systemer beskyttes ved hjælp af funktionsadskillelse, så ingen enkeltpersoner kan få adgang til, ændre eller bruge aktiver uden autorisation, og uden at det opdages.

Ditmer samarbejder med tilsynsmyndighederne for datasikkerhed, når disse kontakter Ditmer, eller hvis Ditmer oplever en hændelse, hvor tilsynsmyndighederne skal involveres. Der udarbejdes beredskabsplaner for de mest sandsynlige tilfælde, hvor der er behov for kontakt med myndighederne, herunder en procedure for sikring af beviser.

Organisationens ansvarlige for it-sikkerhed skal holde sig orienteret om ændringer i sikkerhedstrusler inden for de relevante teknologier, bl.a. for at:

- forbedre viden om bedste praksis og være ajour med relevant sikkerhedsinformation
- sikre et bredt og opdateret kendskab til informationssikkerhed
- modtage tidlige varsler om alarm, meldinger og patches vedrørende angreb og sårbarheder
- skabe passende kontaktpunkter ved håndtering af informationssikkerhedsbrud.

Mobilt udstyr og fjernarbejdspladser

Ditmer anvender i visse sammenhænge mobilt udstyr og fjernarbejdspladser i opgaveløsningen. Ditmer har derfor fastlagt en række regler og procedurer samt gennemført en række tiltag for at minimere den særlige sikkerhedsrisiko, som mobilt udstyr og fjernarbejdspladser kan udgøre.

Personalesikkerhed

Ditmers medarbejdere er vores væsentligste aktiv, både generelt set og set i forhold til informationssikkerhed. Det er vores dygtige medarbejdere, der skal sikre et højt niveau af informationssikkerhed, men medarbejderne kan også udgøre en risiko for sikkerhedsbrud, forsætligt eller uforsætligt. Det er således vigtigt, at vores medarbejdere er udvalgt og uddannet til at sikre høj grad af informationssikkerhed.

Der er fastlagt regler og udarbejdet procedurer for, hvordan personalesikkerheden håndteres før, under og efter ansættelsen.

Faste og midlertidige medarbejdere med adgang til Ditmers it-systemer skal ved tiltrædelsen have en gennemgang af informationssikkerhedspolitikken og kvittere for at have læst denne. De skal ligeledes orienteres om reglerne i Straffeloven og Forvaltningsloven om håndtering af fortrolige data for offentlige kunder, og de skal ligeledes kvittere for at have modtaget denne information.

Det er ledelsens ansvar, at alle medarbejdere:

- Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til Ditmers systemer og data.
- Er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til Ditmers informationssikkerhedspolitik.
- Har forståelse for behovet for Ditmers informationssikkerhedspolitik og retningslinjer og derfor er motiverede for at følge dem. Holder sig inden for de retningslinjer og bestemmelser, der er for ansættelsen, inkl. Ditmers informationssikkerhedspolitik og konkrete arbejdsmetoder.

Det er ledelsens ansvar, at der tilrettelægges uddannelse, træning og løbende kommunikation om informationssikkerhed for at opnå:

- Viden om Ditmers informationssikkerhedspolitik og baggrundsviden for denne.
- Opdaterede instruktioner i overholdelse af Ditmers informationssikkerhedspolitik for at minimere risikoen for sikkerhedshændelser.
- Viden om og motivation for at højne informationssikkerheden.
- Særlig viden om sikkerhedsaspekterne i den enkelte medarbejders job, herunder de enkelte kunders løsninger.

Det er ledelsens ansvar, at der skabes en kultur, hvor alle brud på informationssikkerheden bliver bragt til relevante parters kendskab, og at der bliver handlet på disse. Det er vigtigt, at alle medarbejdere føler sig trygge ved at fortælle om hændelser, så hændelserne kan give anledning til læring og forbedring af informationssikkerheden. Udgangspunktet er derfor, at medarbejdere ikke straffes for brud på informationssikkerheden. Bevidste eller gentagne overtrædelser kan dog medføre ansættelsesmæssige konsekvenser.

Ditmer skal ved ansættelsens ophør sikre, at medarbejderens adgang til Ditmers og evt. Ditmers kunders systemer ophører.

Styring af aktiver

Fortegnelse over aktiver

Ditmers aktiver omfatter software, hardware, papirarkiver og øvrige databærende medier. Disse aktiver skal vi have styr på, så vi ved, hvor vores data er, og hvordan de er sikret.

Der er implementeret procedurer for at vedligeholde en fortegnelse over samtlige relevante databærende aktiver. Når medarbejdere fratræder, sikres det, at medarbejdernes aktiver returneres og wipes, og aktivet ajourføres i fortegnelsen.

Alle systemer skal have en systemejer, der har ansvaret for anskaffelse, styring af aktivet og risikovurdering.

Accepteret brug af aktiver

Som udgangspunkt må der kun anvendes informationssystemer, som er godkendt af Ditmers forum for informationssikkerhed. Det gælder uanset om der er tale om klient-, mobil-, SaaS-, cloudbaserede eller andre informationssystemer.

Adgangsstyring

Adgang til netværk og netværkstjenester

Det er vigtigt for Ditmers medarbejdere at kunne have adgang til Ditmers aktiver også uden for Ditmers lokation. Det må ikke forøge sikkerhedsrisikoen. Der er derfor fastlagt regler for adgang til netværk og netværkstjenester, der skal sikre, at brugerne ikke kompromitterer sikkerheden, når de anvender deres devices uden for Ditmers netværk.

Adgang til Ditmers netværk

Adgang til Ditmers netværk forudsætter fysisk tilstedeværelse med forbindelse til Ditmers netværk eller adgang via VPN.

Gæster i huset må kun forbindes til et dedikeret netværk for gæster og ikke til Ditmers interne netværk.

Administration af brugeradgang

Som en del af vores informationssikkerhedspolitik har vi faste regler og procedurer for tildeling af brugeradgange, hvor der er en ledelsesmæssig godkendelse af tildeling af rettighederne.

Alle brugere skal have en unik identitet til personlig brug og der skal benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.

Vi anvender i videst muligt omfang AD til at styre brugernes adgang til vores aktiver. I AD anvendes rettighedsgrupper til at sikre, at brugerne kun får adgang til de aktiver, de har et arbejdsbetinget behov for at kunne anvende. AD rettighedsgrupperne anvendes til at understøtte funktionsadskillelsen (se punkt 3.1).

Eksterne brugerprofiler skal, gennem konsistent navngivning, være tydeligt adskilt fra fastansatte medarbejderes brugerprofiler. Det vurderes kritisk i hvert enkelt tilfælde, om og i hvor stort omfang en ekstern brugerprofil skal have adgang til Ditmers aktiver.

Både interne og eksterne brugere skal anvende komplekse passwords efter nærmere definerede krav. Samme password bør ikke anvendes i flere forskellige systemer. Hvor det skønnes nødvendigt baseret på en risikoanalyse, anvendes 2-faktor-login.

Der er regler for, hvordan medarbejderne må opbevare passwords, herunder hvor fælles adgangskoder til aktiver må opbevares.

Alle brugerprofiler skal gennemgås periodisk (mindst en gang årligt) for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede brugerprofiler og rettigheder nedlægges eller trækkes tilbage.

Styring af adgang til kildekoder til programmer

Da Ditmer lever af at udvikle software, er det et særligt fokusområde at sikre, at uvedkommende ikke får adgang til kildekoden til kundernes løsninger eller Ditmers egne produkter. Der er derfor fastsat særlige regler for styring af adgang til kildekoder, så Ditmer kan sikre, at udviklingen af software sker på en sikker måde, hvor uvedkommende ikke får adgang.

Kryptografi

Fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, f.eks. på bærbare computere, håndholdte computere m.m.

Adgang til krypteringsnøgler skal begrænses til færrest mulige nøgleadministratorer.

Fysisk sikring og miljøsikring

Ditmers lokaler er generelt åbne, og vores kunder og samarbejdspartnere er velkomne som gæster. Det må dog ikke kompromittere informationssikkerheden, at vi er et åbent hus, der tager mod gæster.

Der er således fastlagt regler og udarbejdet procedurer for håndtering af gæster i huset for at sikre, at vores gæster ikke udgør en trussel. Derudover er der en række tekniske foranstaltninger, der skal supplere den fysiske sikring.

Videoovervågning

Der er etableret automatisk videoovervågning af relevante steder indendørs og udendørs ved Ditmers lokaler.

Adgang til serverrum

Adgangen til serverrum og krydsfelter er beskyttet med elektronisk lås, så kun autoriserede medarbejdere har adgang. Der er fastlagt en procedure for tildeling af adgang, og adgangslisten gennemgås periodisk.

Brug af adgangskodebeskyttet pauseskærm

Alle devices eller pc-arbejdsplacer skærmlåses automatisk med adgangskodebeskyttelse, når de forlades.

Clean desk

Der er indført en clean desk policy, der skal sikre, at uvedkommende ikke får adgang til at se dokumenter med fortrolige oplysninger.

Underleverandører

Når vi benytter underleverandører, sikrer vi os, at de lever op til de standarder for fysisk sikring, som vi ønsker. Dette gør vi i praksis ved som udgangspunkt at indhente erklæring eller på anden måde at få tilfredsstillende dokumentation for tilfredsstillende fysisk sikring.

Driftssikkerhed

Sikring af arbejdsstationer inden ibrugtagning

Ditmers medarbejdere bruger generelt nyere udstyr fra anerkendte producenter og leverandører. Der anskaffes således en del nyt udstyr løbende, og selvom vi alene køber ind fra anerkendte producenter og leverandører, har vi også fastlagt regler og implementeret procedurer for, hvordan vi installerer arbejdsstationer, så disse sikres inden ibrugtagning.

Sikkerhed i systemplanlægning

Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne. Informationssikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer. Se i øvrigt punkt 13.

Driftsprocedurer

Ditmer er afhængig af en stabil drift af egne løsninger, herunder de SaaS-løsninger, vi tilbyder vores kunder. Det sikres ved, at driften kan opretholdes uden personafhængighed, hvilket bl.a. sker ved aftalte driftsprocedurer med vores driftsleverandører.

Ændringsstyring

Ændringer i egne og kundernes løsninger kan udgøre en trussel med informationssikkerheden i form af fortrolighed, integritet eller tilgængelighed. Vi har derfor defineret en procedure for ændringshåndtering for at sikre, at ændringer sker efter aftale med berørte interne og/eller kunden og med mindst mulig gene for de berørte parter.

Kapacitetsstyring

It-systemernes dimensionering skal afpasses efter kapacitetskrav. Ditmer har fastlagt procedurer for at sikre, at kapaciteten løbende tilpasses behovet.

Adskillelse af udviklings-, test- og driftsmiljøer

Udviklings-, test- og driftsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau. Udviklings- og testmiljøer er fysisk adskilt fra driftsmiljøer, og kun systemadministratorer har adgang til driftsmiljøer med særskilt login.

Beskyttelse mod malware

Kontroller mod malware

Der er implementeret procedurer, der sikrer, at der er installeret aktive end-point protection på samtlige computere i Ditmer, og at disse opdateres automatisk så snart leverandøren frigiver nye versioner af både software og definitioner. Al forbindelse til omverdenen er beskyttet med firewall.

Backup

For at sikre en stabil drift og minimere risikoen for tab af data, skal der foretages backup, så vi kan genskabe systemer og data på hensigtsmæssig vis. Der er implementeret procedurer, der sikrer, at der foretages sikker lagring og backup af data på servere i eget serverrum samt på servere hos underleverandører. Der er automatisk kontrol af backup i form af overvågningssoftware. Der foretages manuel kontrol af backup med nærmere defineret interval for forskellige aktiver.

Backup-data skal opbevares off-site, for at sikre redundans i tilfælde af, at serverrum ødelægges.

Logning og overvågning

Ditmer har fastlagt regler for at sikre, at der foretages fornøden logning og kontrol af disse. Ditmer følger leverandørens anbefaling for opsamling og beskyttelse af logs.

Kommunikationssikkerhed

Ditmer har fastlagt regler og implementeret procedurer for at sikre en høj grad af kommunikationssikkerhed, hvor både det kablede og det trådløse netværk kan anvendes til alle vores systemer. Vores netværk indgår i den løbende risikovurdering.

Anskaffelse, udvikling og vedligeholdelse af systemer

Ditmers anskaffelse eller udvikling af nye systemer samt vedligeholdelse af disse følger en række nærmere definerede regler og procedurer, der skal sikre, at både vi og kunderne kan føle sig trygge ved, at der opretholdes et højt niveau af informationssikkerhed. Reglerne og procedurerne omfatter bl.a. retningslinjer for:

- Risikoanalyse ifm. anskaffelse/udvikling af nye systemer
- Best practices for softwareudvikling
- Inddragelse af informationssikkerhed i design, arkitektur, udvikling og afprøvning af software.
- Validering af inddata
- Kildekodestyring
- Sikkert udviklingsmiljø
- Sikre testdata
- Ændringshåndtering, herunder også efterfølgende afprøvning og ændring af risikoanalyse/beredskabsplaner.

Informationssikkerhed ved projektstyring

Særligt i forbindelse med udvikling eller større ændringer på kunders eller Ditmers egne løsninger, skal informationssikkerhed indgå som en væsentlig del af udviklings-/ændringsprojektet.

Ditmers projektmodel for egne projekter og projekter for kunder skal indeholde følgende overvejelser omkring informationssikkerhed:

- Kundens kravspecifikationen bør indeholde kravene til informationssikkerhed; hvis den ikke gør det, skal Ditmers medarbejder spørge til Kundens behov ift. informationssikkerhed.
- Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger.
- Informationssikkerhed bør være en integreret del af projektledelse og indgå i Ditmers projektmodel.

Leverandørforhold

Ditmer anvender leverandører til en række forskellige opgaver. Vi er afhængige af at have gode, pålidelige leverandører for at kunne give vores kunder den ønskede service. Det drejer sig om såvel hostingleverandører og cloud-leverandører som leverandører af konsulentydelser. Vi anvender større danske eller europæiske hostingleverandører samt markedsledende cloud-leverandørers europæiske datacentre til hosting af

egne og kundernes data. Til den konkrete løsning vælges den leverandør, der sikrer kunden den bedst mulige service. Vores væsentligste hostingleverandører er Zitcom (Danmark) samt Microsoft Azure (Europa) og Amazon AWS (Europa). Hostingleverandører og cloud-leverandører af hosting er ISO27001-certificerede, og der indhentes revisionserklæring efter international standard (fx ISAE3402 eller SOC) årligt.

Vi har fastlagt regler for anvendelsen af leverandører, herunder regler for, hvornår ledelsen skal godkende anvendelsen af en leverandør samt krav til leverandørens sikkerhedsniveau og erklæringer herfor.

Styring af informationssikkerhedsbrud

Ledelsen har fastlagt forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Proces for reaktion på hændelser

Der er etableret en procedure, som sikrer at hændelsesstyringsplanen løbende evalueres og tilpasses i overensstemmelse med indsamlet erfaring og den generelle udvikling inden for industrien.

Organisationen er forpligtet til at indberette enhver observeret sikkerhedshændelse eller mistanke herom hurtigst muligt og ad fastlagt kanal. Der bør være let adgang til rapportering af disse hændelser.

For at kunne mindske sandsynligheden eller effekten af fremtidige sikkerhedshændelser, skal den forgangne periodes hændelser gennemgås mindst en gang om året.

Ditmers forum for informationssikkerhed overvåger typer, omfang og omkostninger ved håndteringen af sikkerhedsbrud. Disse oplysninger skal bruges til at identificere og afbøde tilbagevendende sikkerhedshændelser eller disses konsekvenser.

Ditmers forum for informationssikkerhed skal sikre, at relevant information om sikkerhedsbrud gives til alle medarbejdere.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Ledelsen har fastlagt en ensartet ramme for Ditmers beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse.

Systemejerne er ansvarlige for, at passende beredskabsplaner udarbejdes og vedligeholdes for de enkelte virksomhedskritiske systemer med det formål at minimere nedbrud og udgifter som følge af sikkerhedshændelser.

Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for virksomhedskritiske systemer og processer.

Overensstemmelse

Gennemgang af informationssikkerhed

Uafhængig gennemgang af informationssikkerhed

Ditmers informationssikkerhedsregler er som nævnt baseret på ISO27001/27002-standarden, som indeholder retningslinjer for organisationers informationssikkerhedsstandarder og informationssikkerhedsledelse, herunder valg, implementering og styring af kontroller, idet organisationens informationssikkerhedsmæssige risikomiljø(er) tages i betragtning.

Ditmer får ikke foretaget ekstern ISO-audit, men der udarbejdes årligt en revisionserklæring af typen ISAE3402, der også anvender ISO27001/27002 som rammeværk for sin gennemgang af informationssikkerhed.

Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Ditmers forum for informationssikkerhed har fastlagt et årshjul, hvorefter hovedelementerne i informationssikkerhedspolitikken reviewes årligt i en fast kadence. Ved større anskaffelser af aktiver eller væsentlige sikkerhedshændelser foretages desuden yderligere review af relevante elementer af informationssikkerhedspolitikken. Afprøvning af sikkerhedsforanstaltninger indgår som en del af afprøvning af beredskabsplaner.

Ændringer i it-anvendelsen eller kontrolmiljøet

Ditmer har udviklet et nyt produkt i løbet af 2019/2020, Agenda Live, der er implementeret hos de første kunder i foråret 2020. Det er et spændende produkt, som Ditmer forventer sig meget af. Produktet er udviklet, testet og implementeret iht. de gældende tekniske og organisatoriske sikkerhedsforanstaltninger beskrevet i vores politikker og procedurer – og lever således op til både GDPR og anbefalingerne i ISO27001.

Ditmer har udarbejdet en endnu mere systematisk opfølgning på sikkerhedshændelser. Denne sikrer, bl.a. via forbedrede skabeloner, at alle handlinger og beslutninger i forløbet dokumenteres, og at analyseresultater der danner baggrund for konklusionerne, ligeledes gemmes som dokumentation. Alt materiale opbevares sikkert, så kun personer hos Ditmer med et arbejdsbetinget behov ift. sikkerhedshændelsen, har adgang hertil.

Ditmer har indført et årligt review af vores lovpligtige fortegnelse over behandling af persondata, så vi er sikre på at der er anført de rigtige kontaktpersoner ift. sikkerhedsbrud. Tidligere rettede vi oplysningerne, når vi fx blev opmærksom på at en kontaktperson hos kunden ikke længere var ansat eller havde fået en ny rolle. Hvis der opstår et sikkerhedsbrud, er det vigtigt at vi hurtigt kan informere de rette personer hos kunden – så vi har valgt at investere ressourcer i dette review, der udføres ultimo hvert år.

Komplementerende kontroller

Ditmer har det fulde ansvar for software og hardware ejet af Ditmer samt de ydelser, Ditmer udfører for kunderne. I enhver leverance til en kunde, vil der dog også være forhold, som Ditmer forventer, at kunden tager ansvar for. Det er eksempelvis:

- Kundens krav til sikkerhed baseret på kundens risikoanalyse af den opgave, kunden ønsker løst med det projekt, der gennemføres, eller det produkt der indkøbes.
- Kundens eget it-miljø, herunder servere, pc'ere, netværk, printere, licenser til tredjepartsystemer, backup m.m.
- Kundens egne brugere, herunder tildeling og gennemgang af rettigheder, fornøden instruktion m.m.
- Test, herunder at løsningen bliver afprøvet for at sikre, at den leverer det forretningsmæssige resultat, kunden forventer.
- Organisatorisk indsats, herunder implementering i organisationen, etablering af organisatoriske foranstaltning for at øge sikkerheden af løsningen m.m.
- Lovlighed, herunder hjemmel til håndtering af persondata, sikring af anonymiserede testdata m.m.

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

Til ledelsen hos Ditmer A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Ditmer A/S' beskrivelse, som er gengivet i afsnit 2, af sine udvalgte konsulent og produktydelser til behandling af kunders transaktioner i hele perioden 01-06-2019 til 31-05-2020 og om udformningen og funktionen kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Ditmer A/S' ansvar

Ditmer A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

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

REVI-IT A/S 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 Ditmer A/S' beskrivelse (afsnit 2) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og fungerer effektivt.

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

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

Begrænsninger i kontroller hos en serviceleverandør

Ditmer A/S' 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 vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

(a) at beskrivelsen af kontroller, således som de var udformet og implementeret i hele perioden 01-06-2019 til 31-05-2020, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 01-06-2019 til 31-05-2020

(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 01-06-2019 til 31-05-2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i det efterfølgende hovedafsnit (afsnit 4).

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 2 er udelukkende tiltænkt kunder, der har anvendt Ditmer A/S' udvalgte konsulent og produktydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, 18. juni 2020

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Basel Rimon Obari
It-revisor (CISA, CISM), Director, Partner

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 Ditmer A/S 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 01-06-2019 til 31-05-2020.

Vi har således ikke nødvendigvis testet alle de kontroller, som Ditmer A/S har nævnt i sin beskrivelse i afsnit 2.

Kontroller, udført hos Ditmer A/S' 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 Ditmer A/S 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.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Der er udarbejdet en risikoanalyse for trusler mod forretningskritiske aktiver. Risikoanalysen udarbejdes af den relevante systemansvarlige og Ditmers informationssikkerhedsansvarlige. Risikoanalysen for det enkelte aktiv gennemgås årligt, og den samlede risikoanalyse godkendes årligt af ledelsen.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i revisionsperioden.	Ingen afvigelser konstateret.

Informationssikkerhedspolitikker

Retningslinjer for styring af informationssikkerhed

Kontrolmål: Formålet er at sikre, at der gives retningslinjer for og understøttelse af informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
5.1	Ditmers informationssikkerhedsregler er baseret på ISO27001/27002-standarden, som indeholder retningslinjer for organisationers informationssikkerhedsstandarder og informationssikkerhedsledelse, herunder valg, implementering og styring af kontroller, idet organisationens informationssikkerhedsmæssige risikomiljø(er) tages i betragtning. Informationssikkerhedspolitikken gennemgås årligt og godkendes af ledelsen.	Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af informationssikkerhedspolitikken, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden, samt inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen afvigelser konstateret.

Organisering af informationssikkerhed

Intern organisering

Kontrolmål: Formålet er at sikre, at der etableres et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
6.1	Ditmer har et forum for informationssikkerhed, der har ansvar for at sikre, at informationssikkerhedspolitikken er synlig, koordineret og i overensstemmelse med Ditmers mål. Informationssikkerhedsforummet ledes af et medlem af Ditmers øverste ledelsesgruppe. Sikkerhedsansvarlige systemejere for virksomhedskritiske systemer har ansvar og beføjelser til at sikre tilstrækkelig beskyttelse. Organisationens ansvarlige for it-sikkerhed skal holde sig orienteret om ændringer i sikkerhedstrusler inden for de relevante teknologier.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser. Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret dokumentation for differentieret adgang. Vi har forespurgt til retningslinjer for kontakt med myndigheder. 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. Vi har stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed	Ingen afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
6.2	Ditmer anvender i visse sammenhænge mobilt udstyr og fjernarbejdspladser i opgaveløsningen. Ditmer har derfor fastlagt en række regler og procedurer samt gennemført en række tiltag for at minimere den særlige sikkerhedsrisiko, som mobilt udstyr og fjernarbejdspladser kan udgøre.	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 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.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Der er fastlagt regler og udarbejdet procedurer for, hvordan personalesikkerheden håndteres før, under og efter ansættelsen. Det er ledelsens ansvar, at alle medarbejdere: • Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til Ditmers systemer og data. • Er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til Ditmers informationssikkerhedspolitik. • Har forståelse for behovet for Ditmers informationssikkerhedspolitik og retningslinjer og derfor er motiverede for at følge dem. Holder sig inden for de retningslinjer og bestemmelser, der er for ansættelsen, inkl. Ditmers informationssikkerhedspolitik og konkrete arbejdsmetoder.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter.	Ingen afvigelser konstateret.

Under ansættelsen

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
7.2	Det er ledelsens ansvar, at der tilrettelægges uddannelse, træning og løbende kommunikation om informationssikkerhed for at opnå: Viden om Ditmers informationssikkerhedspolitik og baggrundsviden for denne. Opdaterede instruktioner i overholdelse af Ditmers informationssikkerhedspolitik for at minimere risikoen for sikkerhedshændelser. Viden om og motivation for at højne informationssikkerheden. Særlig viden om sikkerhedsaspekterne i den enkelte medarbejders job, herunder de enkelte kunders løsninger.	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 afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring **Kontrolmål: Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
7.3	Der er fastlagt regler og udarbejdet procedurer for, hvordan personalesikkerheden håndteres før, under og efter ansættelsen. Ditmer skal ved ansættelsens ophør sikre, at medarbejderens adgang til Ditmers og evt. Ditmers kunders systemer ophører.	Vi har forespurgt til medarbejdernes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver **Kontrolmål: Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
8.1	Der er implementeret procedurer for at vedligeholde en fortegnelse over samtlige relevante databærende aktiver. Når medarbejdere fratræder, sikres det, at medarbejdernes aktiver returneres og wipes, og at aktivet ajourføres i fortegnelsen. Alle systemer skal have en systemejer, der har ansvaret for anskaffelse, styring af aktivet og risikovurdering.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til oversigt af ejerskab for aktiver, og vi har inspiceret oversigten. Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne. Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Klassifikation af information **Kontrolmål: Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
8.2	Vi har defineret retningslinjer for klassificering af data for at sikre, at disse håndteres med fornøden fortrolighed i forhold til indholdet.	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 afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Det er vigtigt for Ditmers medarbejdere at kunne have adgang til Ditmers aktiver også uden for Ditmers lokation. Det må ikke forøge sikkerhedsrisikoen. Der er derfor fastlagt regler for adgang til netværk og netværkstjenester, der skal sikre, at brugerne ikke kompromitterer sikkerheden, når de anvender deres devices uden for Ditmers netværk.	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken. Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.

Administration af brugeradgange

Kontrolmål: Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
9.2	Som en del af vores informationssikkerhedspolitik har vi faste regler og procedurer for tildeling af brugeradgange, hvor der er en ledelsesmæssig godkendelse af tildeling af rettighederne. Alle brugerprofiler skal gennemgås periodisk (mindst en gang årligt) for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres. Både interne og eksterne brugere skal anvende komplekse passwords efter nærmere definerede krav. Samme password bør ikke anvendes i flere forskellige systemer. Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede brugerprofiler og rettigheder nedlægges eller trækkes tilbage.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret dokumentation for oprettelse og nedlæggelse af brugere. Vi har forespurgt til proces for tildeling af rettigheder, og vi har inspiceret processen. Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har forespurgt til opbevaring af fortrolige adgangskoder, og vi har inspiceret dokumentation for betryggende opbevaring. Vi har forespurgt til proces for periodisk gennemgang af brugere, og vi har inspiceret dokumentation for seneste gennemgang. Vi har forespurgt til procedure for inddragelse af rettigheder, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
9.3	Der er regler for, hvordan medarbejderne må opbevare passwords, herunder hvor fælles adgangskoder til aktiver må opbevares.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen afvigelser konstateret.
Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Ditmer anvender i videst muligt omfang AD til at styre brugernes adgang til vores aktiver. I AD anvendes rettighedsgrupper til at sikre, at brugerne kun får adgang til de aktiver, de har et arbejdsbetinget behov for at kunne anvende. AD rettighedsgrupperne anvendes til at understøtte funktionsadskillelsen (se punkt 3.1). Hvor det skønnes nødvendigt baseret på en risikoanalyse, anvendes 2-faktor-login Da Ditmer lever af at udvikle software, er det et særligt fokusområde at sikre, at uvedkommende ikke får adgang til kildekoden til kundernes løsninger eller Ditmers egne produkter. Der er derfor fastsat særlige regler for styring af adgang til kildekode, så Ditmer kan sikre, at udviklingen af software sker på en sikker måde, hvor uvedkommende ikke får adgang.	Vi har forespurgt til begrænsning af adgang til data, herunder kildekode, og vi har inspiceret dokumentation for begrænsning. Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen. Vi har forespurgt til system til styring af adgangskoder. Vi har inspiceret løsningen og udvalgte konfigurationer.	Ingen afvigelser konstateret.

Kryptografi

Kryptografiske kontroller

Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
10.1	Fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, f.eks. på bærbare computere, håndholdte computere m.m. Adgang til krypteringsnøgler skal begrænses til færrest mulige nøgleadministratorer.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Ingen afvigelser konstateret.

Fysisk sikring og miljøsikring

Sikre områder

Kontrolmål: Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
11.1	Der er fastlagt regler og udarbejdet procedurer for håndtering af gæster i huset for at sikre, at vores gæster ikke udgør en trussel. Derudover er der en række tekniske foranstaltninger, der skal supplere den fysiske sikring. Der er etableret automatisk videoovervågning af relevante steder indendørs og udendørs ved Ditmers lokaler. Adgangen til serverrum og krydsfelter er beskyttet med elektronisk lås, så kun autoriserede medarbejdere har adgang. Der er fastlagt en procedure for tildeling af adgang, og adgangslisten gennemgås periodisk.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har stikprøvevis inspiceret dokumentation for tildeling af adgang til driftsfaciliteter. Vi har inspiceret de fysiske forhold hos virksomhedens kontorer med henblik på at kontrollere den fysiske sikring. Vi har forespurgt til levering af pakker og varer.	Ingen afvigelser konstateret.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
11.2	Når vi benytter underleverandører, sikrer vi os, at de lever op til de standarder for fysisk sikring, som vi ønsker. Dette gør vi i praksis ved som udgangspunkt at indhente erklæring eller på anden måde at få tilfredsstillende dokumentation for tilfredsstillende fysisk sikring. Alle devices eller pc-arbejdspladser skærmlåses automatisk med adgangskodebeskyttelse, når de forlades. Der er indført en clean desk policy, der skal sikre, at uvedkommende ikke får adgang til at se dokumenter med fortrolige oplysninger.	Vi har inspiceret erklæring fra underleverandør med henblik på at identificere fysiske forhold, herunder understøttende forsyninger og sikring af regelmæssig vedligeholdelse af udstyret, sikring af kabler og bortskaffelse af udstyr. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. Vi har forespurgt på politik for bortskaffelse af databærende medier. Vi har forespurgt til sikring af brugerudstyr uden opsyn, samt stikprøvevis inspiceret, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord.	Ingen afvigelser konstateret.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Ved planlægning af systemer skal informationssikkerhedskrav tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer. Ditmer har aftalte driftsprocedurer med vores driftsleverandører. Vi har defineret en procedure for ændringshåndtering for at sikre, at ændringer sker efter aftale med berørte interne og/eller kunden og med mindst mulig gene for de berørte parter. Ditmer har fastlagt procedurer for at sikre, at kapaciteten løbende tilpasses behovet. Udviklings-, test- og driftsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau. Udviklings- og testmiljøer er fysisk adskilt fra driftsmiljøer, og kun systemadministratorer har adgang til driftsmiljøer med særskilt login.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring, og vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til anvendelsen af udvikling og testmiljø, og vi har inspiceret dokumentation for eksistensen af disse miljøer.	Vi har observeret at virksomheden ikke konsekvent sikrer dokumentation for opretholdelse af funktionsadskillelse ved ændringer ifm. pull/merge requests, herunder relevante godkendelser samt review af koden. Vi har dog fået oplyst at processerne ifm. opretholdelse af funktionsadskillelsen foregår på et uformel og ofte mundtligt niveau. Ingen afvigelser konstateret i øvrigt.

Malwarebeskyttelse

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Der er implementeret procedurer, der sikrer, at der er installeret aktiv end-point protection på samtlige computere i Ditmer, og at disse opdateres automatisk så snart leverandøren frigiver nye versioner af både software og definitioner.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen afvigelser konstateret.

Backup

Kontrolmål: Formålet er at beskytte mod tab af data.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
12.3	For at sikre en stabil drift og minimere risikoen for tab af data, skal der foretages backup, så vi kan genskabe systemer og data på hensigtsmæssig vis. Der er implementeret procedurer, der sikrer, at der foretages sikker lagring og backup af data på servere i eget serverrum samt på servere hos underleverandører. Der er automatisk kontrol af backup i form af overvågningssoftware. Der foretages manuel kontrol af backup med nærmere defineret interval for forskellige aktiver. Backup-data skal opbevares offsite, for at sikre redundans i tilfælde af, at serverrum ødelægges.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen. Vi har forespurgt til opbevaring af backup, og vi har inspiceret erklæring fra underleverandør med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse.	Ingen afvigelser konstateret.

Logning og overvågning

Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
12.4	Ditmer har fastlagt regler for at sikre, at der foretages den fornødne logning og kontrol af disse. Ditmer følger leverandørens anbefaling for opsamling og beskyttelse af logs.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
13.1	Ditmer har fastlagt regler og implementeret procedurer for at sikre en høj grad af kommunikationssikkerhed, hvor både det kablede og det trådløse netværk kan anvendes til alle vores systemer.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patchning af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen afvigelser konstateret.

Anskaffelse, udvikling og vedligeholdelse af systemer

Sikkerhedskrav til informationssystemer

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
14.1	Ditmers anskaffelse eller udvikling af nye systemer samt vedligeholdelse af disse følger en række nærmere definerede regler og procedurer, der skal sikre, at både vi og kunderne kan føle sig trygge ved, at der opretholdes et højt niveau af informationssikkerhed.	Vi har forespurgt til informationssikkerhedsrelaterede krav til virksomhedens løsning, og vi har inspiceret de opstillede krav. Vi har forespurgt til sikring af løsningen på offentlige netværk, og vi har inspiceret løsningen. Vi har forespurgt til sikring af transmissioner, og vi har inspiceret dokumentation for beskyttelse af transmissioner.	Ingen afvigelser konstateret

Sikkerhed i udviklings- og hjælpeprocesser **Kontrolmål: Formålet er at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingscyklus.**			
Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
14.2	Reglerne og procedurerne omfatter bl.a. retningslinjer for: • Risikoanalyse ifm. anskaffelse/udvikling af nye systemer • Best practices for softwareudvikling • Inddragelse af informationssikkerhed i design, arkitektur, udvikling og afprøvning af software. • Validering af inddata • Kildekodestyring • Sikkert udviklingsmiljø • Sikre testdata • Ændringshåndtering, herunder også efterfølgende afprøvning og ændring af risikoanalyse/beredskabsplaner. Ditmers projektmodel for egne projekter og projekter for kunder skal indeholde følgende overvejelser omkring informationssikkerhed: • Kundens kravspecifikationen bør indeholde kravene til informationssikkerhed; hvis den ikke gør det, skal Ditmers medarbejder spørge til kundens behov ift. informationssikkerhed. • Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger. • Informationssikkerhed bør være en integreret del af projektledelse og indgå i Ditmers projektmodel.	Vi har forespurgt til politik for styring af udvikling, og vi har inspiceret politikken. Vi har forespurgt til procedure for styring af systemændringer, og vi har inspiceret proceduren. Vi har stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til test af applikationer i forbindelse med ændringer og opdatering af driftsplatformen, og vi har inspiceret dokumentation for test. Vi har forespurgt til principper for sikker udvikling, og vi har inspiceret udarbejdede principper. Vi har forespurgt til sikkert udviklingsmiljø, og vi har inspiceret dokumentation for adskillelse mellem udviklingsmiljø og produktionsmiljø. Vi har forespurgt til systemsikkerhedstest, og vi har stikprøvevis inspiceret dokumentation for systemsikkerhedstest. Vi har forespurgt til systemgodkendelsestest, og vi har stikprøvevis inspiceret dokumentation for systemaccept i forbindelse med udvikling.	Vi har observeret at virksomheden ikke sikrer overholdelse af et mindre udsnit af egne politikker vedrørende tekniske foranstaltninger for sikker webudvikling. Ingen afvigelser konstateret i øvrigt.

Leverandørforhold

Informationssikkerhed i leverandørforhold

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
15.1	Vi har fastlagt regler for anvendelsen af leverandører, herunder regler for, hvornår ledelsen skal godkende anvendelsen af en leverandør samt krav til leverandørens sikkerhedsniveau og erklæringer herfor. Det drejer sig om såvel hostingleverandører og cloud-leverandører som leverandører af konsulentydelser.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse hensyntagen til informationssikkerhed.	Ingen afvigelser konstateret.

Styring af leverandørydelser

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
15.2	Der indhentes revisionserklæring efter international standard (fx ISAE3402 eller SOC) årligt.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren.	Ingen afvigelser konstateret.

Styring af 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.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
16.1	Der er etableret en procedure, som sikrer at hændelsesstyringsplanen løbende evalueres og tilpasses i overensstemmelse med indsamlet erfaring og den generelle udvikling inden for industrien. Organisationen er forpligtet til at indberette enhver observeret sikkerhedshændelse eller mistanke herom hurtigst muligt og ad fastlagt kanal. Der bør være let adgang til rapportering af disse hændelser. For at kunne mindske sandsynligheden eller effekten af fremtidige sikkerhedshændelser, skal den forgangne periodes hændelser gennemgås mindst en gang om året. Ditmers forum for informationssikkerhed overvåger typer, omfang og omkostninger ved håndteringen af sikkerhedsbrud. Disse oplysninger skal bruges til at identificere og afbøde tilbagevendende sikkerhedshændelser eller disses konsekvenser. Ditmers forum for informationssikkerhed skal sikre, at relevant information om sikkerhedsbrud gives til alle medarbejdere.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret procedure til håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til informationssikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
17.1	Ledelsen har fastlagt en ensartet ramme for Ditmers beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse. Systemejerne er ansvarlige for, at passende beredskabsplaner udarbejdes og vedligeholdes for de enkelte virksomhedskritiske systemer med det formål at minimere nedbrud og udgifter som følge af sikkerhedshændelser. Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for virksomhedskritiske systemer og processer.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen. Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabstest, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Ingen afvigelser konstateret.

Overensstemmelse

Gennemgang af informationssikkerheden

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

Nr.	Ditmer A/S' kontrol	REVI-IT's test	Resultat af test
18.2	Der udarbejdes årligt en revisionserklæring af typen ISAE3402, der anvender ISO27001/27002 som rammeværk for sin gennemgang af informationssikkerhed. Ditmers forum for informationssikkerhed har fastlagt et årshjul, hvorefter hovedelementerne i informationssikkerhedspolitikken reviewes årligt i en fast kadence.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Ingen afvigelser konstateret.

Afsnit 5: Anden information stillet til rådighed af Ditmer A/S

Risikovurdering og -håndtering		
Nr.	Resultat af test	Ditmer A/S' redegørelse
12.1	Vi har observeret at virksomheden ikke sikrer dokumentation for opretholdelse af funktionsadskillelse ved ændringer ifm. pull/merge requests, herunder relevante godkendelser samt review af koden. Vi har dog fået oplyst at processerne ifm. opretholdelse af funktionsadskillelsen foregår på et uformelt og ofte mundtligt niveau. Ingen afvigelser konstateret i øvrigt.	Ditmers politik og procedurer for Change skal overholdes af alle ansatte. Dette indebærer fx, at al kode skal gennem et review af en kompetent kollega. Det er den ansvarlige udvikler der skal sikre denne godkendelse. Ved flytning af allerede reviewet kode til vores produktionsmiljø er det ikke dokumenteret i vores system, at denne handling er godkendt af en kollega, selvom der selvfølgelig altid er sket godkendelse. Vi er opmærksomme på, at selvom vi har en robust proces der sikrer kunderne en meget høj grad af sikkerhed omkring brug af Ditmers løsninger, så er det også væsentligt at kunne fremvise dokumentation herfor. Vi justerer derfor snarest vores brug af 'systemerne' der styrer pull/merge requests, så alle godkendelser af kodeændringer er dokumenteret.

Sikkerhed i udviklings- og hjælpeprocesser		
Nr.	Resultat af test	Ditmer A/S' redegørelse
14.2	Vi har observeret at virksomheden ikke sikrer overholdelse af et mindre udsnit af egne politikker vedrørende tekniske foranstaltninger for sikker webudvikling. Ingen afvigelser konstateret i øvrigt.	Ditmer justerer løbende politikker og procedurer, så de løsninger der udvikles, til enhver tid minimum lever op til gældende branchestandard. Når vi indfører skærpede krav til fx tekniske foranstaltninger for sikker webudvikling, gælder disse for al nyudvikling, men også for eksisterende løsninger, hvis der foretages væsentlige ændringer i disse. Vi indførte en række skærpede krav i efteråret 2018, men ikke alle løsninger udviklet før dette tidspunkt, lever nødvendigvis op til de skærpede krav. Ditmer har planlagt at gennemgå alle løsninger og vurdere, om nogle af de skærpede krav skal implementeres i disse. Dette vil ske på baggrund af en grundig risikovurdering. Gennemgangen igangsættes i 2. halvår 2020, og forventes afsluttet i 1. kvartal 2021. Hvis der i en løsning foretages væsentlige ændringer inden dette tidspunkt, vil gennemgangen ske som en del af udviklingsprojektet.