AddPro Danmark A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2023 til 31. december 2023 i relation til AddPro Danmark A/S' hosting-aktiviteter til kunder

Marts 2024

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt AddPro Danmark A/S' hosting-aktiviteter, 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.

AddPro Danmark A/S anvender Global Connect og Cibicom som underleverandører for hosting- og back-upydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Global Connect og Cibicom varetager for AddPro Danmark A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos vores kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

AddPro Danmark A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af AddPro Danmark A/S' hosting-aktiviteter, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til hosting-aktiviteterne var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller
   - Relevante kontrolmål og kontroller udformet til at nå disse mål
   - Kontroller, som vi med henvisning til udformningen af hosting-aktiviteterne har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Hvordan andre betydelige begivenheder og forhold end transaktioner behandles
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til hosting-aktiviteterne foretaget i perioden fra 1. januar 2023 til 31. december 2023

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til hosting-aktiviteterne, 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 generelle it-kontroller i relation til hosting-aktiviteterne, som den enkelte kunde måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give 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 udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2023 til 31. december 2023.

Skovlunde, den 5. marts 2024
AddPro Danmark A/S

Brian Sørensen
Direktør

2 Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2023 til 31. december 2023 i relation til AddPro Danmark A/S' hosting-aktiviteter til kunder

Til: AddPro Danmark A/S, AddPro Danmark A/S' kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om AddPro Danmark A/S' beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til AddPro Danmark A/S' hosting-aktiviteter, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2023 til 31. december 2023, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

AddPro Danmark A/S anvender Global Connect og Cibicom som underleverandører for hosting- og backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Global Connect og Cibicom varetager for AddPro Danmark A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos AddPro Danmarks A/S' kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med AddPro Danmark A/S' kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

AddPro Danmark A/S' ansvar

AddPro Danmark A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om AddPro Danmark A/S' beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet 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 sine hosting-aktiviteter samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, 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 opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som AddPro Danmark A/S har specificeret og beskrevet i ledelsens udtalelse.

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

AddPro Danmark A/S' 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 hosting-aktiviteterne, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller 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 en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

a) at beskrivelsen af de generelle it-kontroller i relation til hosting-aktiviteterne, således som de var udformet og implementeret i hele perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er tilfredsstillende præsenteret, og

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 1. januar 2023 til 31. december 2023, 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 opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2023 til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

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

Aarhus, den 5. marts 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3 AddPro Danmark A/S' beskrivelse af generelle it-kontroller for levering af hosting-aktiviteter

3.1 Indledning

Formålet med denne beskrivelse er at levere information til AddPro Danmark A/S' kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Omfanget af denne beskrivelse er en afdækning af de tekniske og organisatoriske sikkerhedsforanstaltninger, som er implementeret i forbindelse med it-driften af hosting-aktiviteter. Implementeringen af de tekniske og organisatoriske sikkerhedsforanstaltninger er sket med udgangspunkt i ISO 27001.

3.2 Virksomheden og ydelserne

AddPro Danmark A/S, der blev stiftet i 2009, tilbyder totale løsninger inden for it-outsourcing og it-drift med fokus på mindre og mellemstore virksomheder og offentlige organisationer. Virksomheden er beliggende i henholdsvis København, Randers og Aalborg og har i alt ca. 120 ansatte.

AddPro Danmark A/S er et aktieselskab og ejet af itm8 | AddPro DK Holding I ApS.

AddPro Danmark A/S' driftsløsninger er karakteriseret ved høj oppetid, stabilitet og stor kundetilfredshed, og via højtuddannet personale med solid erfaring og forretningsforståelse indgår rådgivning, strategisk planlægning og stærk ansvarsfølelse som helt naturlige, implicitte ydelser i alle vores indgåede aftaler.

For AddPro Danmark A/S' kunder betyder det effektivisering, besparelser og konkurrencemæssige fordele – leveret til den aftalte tid.

Med fokus på kundens behov leverer vi de samlede ydelser, der dækker driften af kundens it-systemer, herunder følgende produkter:

- It-outsourcing
- Managed hosting
- Cloud hosting
- Hosted desktop
- Microsoft 365.

AddPro Danmark A/S har datacenter placeret hos Global Connect i Ejby, Cibicom i Ballerup samt offsite-backup hos itm8 datacenter i Valby, som giver helt optimale og sikre fysiske forhold til it-drift.

3.3 Sikkerheds- og kvalitetspolitik

Informationssikkerhedspolitikken skal til enhver tid understøtte AddPro Danmark A/S' værdigrundlag og vision. Hensigten med it-sikkerhedspolitikken er desuden at tilkendegive over for alle, som har en relation til AddPro Danmark A/S, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Fastholdelse og udbygning af et højt it-sikkerhedsniveau er en væsentlig forudsætning for, at AddPro Danmark A/S fremstår troværdig på alle niveauer. For at fastholde AddPro Danmark A/S' troværdighed sikres det, at information behandles med fornøden fortrolighed.

Der skal skabes et effektivt værn mod it-sikkerhedsmæssige trusler, så AddPro Danmark A/S' image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal imødegå såvel naturgivne som tekniske og menneskeskabte trusler. Ingen persongruppe skal være hævet over it-sikkerhedsbestemmelserne.

Målene er derfor at højne den fysiske, logiske og administrative sikkerhed og derved:

- opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer
- opnå fortrolig behandling, transmission og opbevaring af data.

Vi behandler i den forbindelse følgende punkter:

Informationssikkerhedspolitikker

Med udgangspunkt i virksomhedens overordnede strategiplan er virksomhedens sikkerhedspolitik og informationssikkerhedspolitik defineret. Det er ledelsen, der har defineret politikkerne, og det er ledelsen, som tilsikrer, at de efterleves. Kvalitetssystemet er med til at sikre en stabil og sikker drift for vores kunder.

Organisering af informationssikkerhed

Det overordnede ansvar ligger hos virksomhedens CEO, der er den øverst ansvarlige for det tekniske område. Virksomhedens CTO er ansvarlig for det tekniske område og implementerer indholdet af politikkerne på de forskellige tekniske niveauer og tilsikrer, at der løbende sker en evaluering af hele det tekniske miljø for til stadighed at kunne opfylde virksomhedens interne krav og målsætninger. Sideløbende hermed foretages der en evaluering af det tekniske personale med henblik på at opgradere dets tekniske kvalifikationer, således at AddPro Danmark A/S fortsat kan tilbyde kunderne den allernyeste og bedste teknologi.

Den tekniske organisation er delt op i tre områder, der refererer til den tekniske chef. Hvert af områderne ledes af en teamleder.

- Service og support
- Drift og konsulenter
- Infrastruktur og projekter.

Kontakt til myndigheder og særlige interessegrupper skal gå igennem ledelsen for at sikre høj kvalitet og fuld transparens.

Personalesikkerhed

AddPro Danmark A/S' medarbejdere er instruerede i håndtering af følsomme data, ligesom de følger den udfærdigede sikkerhedspolitik. Der er defineret politikker for, når en medarbejder ansættes i eller forlader AddPro Danmark A/S.

Kravene til medarbejderne er anført i deres ansættelseskontrakter og eventuelle yderligere stillings- og ansvarsbeskrivelser, som justeres løbende i ansættelsesforholdet. Af ansættelseskontrakten fremgår krav om fortrolighed og tavshedspligt både under og efter ansættelsesforholdet.

Under ansættelsen modtager medarbejderen relevant træning i kvalitetssystemets arbejdsinstruktioner og understøtter dermed ajourføring af viden om procedurer. Herudover modtager medarbejderen løbende generel information om eventuelle relevante sikkerhedsaspekter på møder eller i form af informationsbreve.

Ved ophør af ansættelse gælder tavshedspligten fortsat, og alle rettigheder og adgange til systemer og information fjernes.

Medarbejdere, der bryder de gældende it-sikkerhedsbestemmelser hos AddPro Danmark A/S, vil blive sanktioneret. De nærmere regler om dette fastsættes i gældende ansættelseskontrakter.

Styring af aktiver

Alle aktiver identificeres entydigt og fremgår i vores asset management-systemer. Alle informationer og aktiver i relation til informationsbehandlingsudstyr "ejes" af den tekniske afdeling i AddPro Danmark A/S.

Der er rettighedsstyring, til at sikre at data kun kan tilgås af de brugere, som skal have adgang til data. Der er politikker for kryptering af diske i bærbare maskiner samt for sikker bortskaffelse af datamedier.

Adgangsstyring

Vi vil sikre, at vores og vores kunders adgange ske efter hensigten, og at det alene er personer med autoriseret adgangsniveau, der har adgang til data. Vi vil sikre, at der er sporbarhed i brugen af systemer og data, og at adgangen sker it-sikkerhedsmæssigt betryggende. Der er derfor faste procedure for, hvem der kan oprette nye brugere i AddPro Danmark A/S, samt for tildeling eller inddragelse af rettigheder. Der er krav om, at alle brugere holder deres passwords hemmelige samt anvender MFA, hvor det er muligt.

Alle koder, der opbevares på vegne af vores kunder, ligger krypteret i vores passwordmanager, med fuld logning af hvem der tilgår de enkelte koder og hvornår.

Kryptografi

AddPro Danmark A/S anvender primært kryptografi i forbindelse med backupløsninger, netværkstrafik mellem sikre lokationer samt dial-up-VPN-forbindelser til eksempelvis hjemmearbejdspladser og til udveksling af fortrolige eller følsomme e-mails.

Hvis kunden ønsker kryptering af selve netværksforbindelsen mellem kunden og AddPro Danmark A/S, er der mulighed for opsætning af hardware- eller softwarebaseret VPN. Løsningen aftales særskilt.

Alle gemte koder skal opbevares i krypteret passwordmanager.

Fysisk sikring og miljøsikring

Fysisk sikkerhed dækker dels over tiltag til sikring af den fysiske adgang til datacenteret såsom hærdede ståldøre og -vægge m.v. Herudover kommer bl.a. også tiltag som strømsystem bestående af UPS og dieselgenerator, redundante køleanlæg samt brandsikringsanlæg, som kan kvæle enhver ild uden at ødelægge infrastrukturen. Alle vitale områder såsom temperatur, fugt og fysisk indtrængen overvåges og alarmerer 24/7/365 relevant personale eller eksterne partnere. Sikkerhedsafgrænsninger (barrierer som fx vægge, kortstyrede indgangsporte eller bemandede receptioner) anvendes til at beskytte områder, der indeholder informationer og informationsbehandlingsfaciliteter. Kun autoriseret personale har mulighed for at skaffe adgang til datacenteret efter forudgående clearing. Personer, der ikke er ansat hos AddPro Danmark A/S, kan kun få adgang til udstyr, hvis det er strengt nødvendigt, og de bliver ledsaget af en ansvarlig medarbejder fra AddPro Danmark A/S samt registreres i en logbog ved ind- og udgang.

Driftssikkerhed og patch management

Driftsprocedurer og ansvarsområder

Der udarbejdes procedurer for de opgaver, der skal udføres ensartet og korrekt hver gang.

Driften i datacenteret, herunder netværket, overvåges aktivt 24/7/365. Ved driftsforstyrrelser vil teknisk personale blive tilkaldt, og forstyrrelsen vil blive afhjulpet omgående. Desuden monitorerer AddPro Danmark A/S kapacitet samt ressourceforbrug på såvel delte som kundespecifikke elementer for i videst muligt omfang at kunne skalere, inden fejl opstår.

Dette betyder, at vi har bygget sikkerhed ind de systemer, vi bruger til driften af alt fra enkelte servere til centralt udstyr i datacenteret, om det så drejer sig om vores AddPro Danmark A/S sagsstyringssystem, vores overvågnings-, patchmanagement- eller dokumentationssystemer.

AddPro Danmark A/S søger at optimere kvaliteten af vores ydelser gennem principperne i ITIL og ved brug af AddPro Danmark A/S' sagsstyringssystem.

AddPro Danmark A/S' sagsstyringssystem sikrer, at ITIL er integreret i interne processer og er også værktøjet, hvor hændelser vedrørende kundens systemer bliver registreret, og løbende opdateres med status og fremdrift.

Måling af performance og belastning er en integreret del af AddPro Danmark A/S' overvågning og vil i samspil med capacity management-processen sørge for, at kapacitetsudvidelser adresseres proaktivt og rettidigt.

Beskyttelse mod malware

Der installeres antivirussoftware på alle supporterede operativsystemer. Softwaren opdateres automatisk og rapporterer hændelser til cloud controller.

Backup

Med en backuppolitik sikrer kunden, at data gemmes i backuplageret i det antal versioner (antal ændringer) og i det tidsrum (retention-perioden), som lever op til kundens behov. Kunden kan selv være med til at definere sit behov før installation af løsningen.

AddPro Danmark A/S sikrer, at data lagres i AddPro Danmark A/S' backupsystemer med den backuppolitik, som kunden har valgt.

AddPro Danmark A/S gemmer alle versioner af backupdata på lokalt hardware tilknyttet backupløsningen, og der genereres på daglig basis offsite-kopi på andet site. Alle processer og rutiner overvåges alle årets dage.

AddPro Danmark A/S' teknikere foretager til start en fuldstændig backup af den virtuelle maskine, og herefter er backuppen i drift.

Der laves en daglig backup af alle virtuelle servere i miljøet. Det er herved muligt at genskabe en hel server, som den så ud på backuptidspunktet, herunder også at genskabe filer ud fra en serverkopi. Snapshot-baseret backup kan genskabes 30 dage tilbage i tid, medmindre andet aftales skriftligt.

Logning og overvågning

Som værktøj til overvågning af netværk, hardware og driftsmiljøer benytter AddPro Danmark A/S en række værktøjer til overvågning af komponenter. AddPro Danmark A/S' overvågningsplatform anvendes til pro-aktiv fejlfinding samt alarmering af personale. Der sker en lagring af alle monitoreringsdata, så dataene kan bruges til analyser, men også som dokumentation i relation til kunder.

AddPro Danmark A/S konfigurerer monitoreringsværktøjerne med grænseniveauer, der skal gælde for de overvågede komponenter. Alarmer, som har eller kan have indflydelse på den leverede service, genererer automatisk incidents.

Nedenfor er en oversigt over de enheder, der blandt andet er omfattet af overvågningen. For netværk og fysiske hosts overvåges som minimum på linkstatus, båndbreddeforbrug samt vitale driftsparametre.

Netværk:

- Forbindelse til ISP-gateways
- Core switches
- Datacenter-firewalls
- HA status.

Server-hosts:

- CPU-forbrug
- RAM-forbrug
- Diskkapacitet
- Diskperformance
- Netværksperformance
- Patch-niveau
- Status på backup
- Hardwarestatus fra IPMI.

Virtuelle servere:

- CPU-forbrug
- RAM-forbrug
- Diskkapacitet
- Patch-niveau
- Services up/down
- Key event-logge.

Logning er en integreret del af AddPro Danmark A/S' driftsplatform. Der logges bl.a. performancelogge, systemlogge, databaselogge, backuplogge, eventlogge og access-logge. Dette sker for at sikre sporbarhed og dokumentation. Der anvendes som udgangspunkt danske NTP-servere til synkronisering af tid på tværs af systemer.

Alarmer udsendes både via mail samt ticket-system og visuelt på storskærme til den driftsansvarlige inden for normal åbningstid og til de vagthavende konsulenter på alle andre tidspunkter. Alarmerne kan også tilgå kunderne i form af mail og adgang til egne overvågningsdata.

Sårbarhedsstyring/patch management

Vi patcher så vidt muligt vores systemer jævnfør vores leverandørers anvisninger. Dette har til hensigt at sikre systemerne mod nedetid og uautoriseret adgang. Implementeringen af opdateringer sker normalt jævnfør vores change management-proces, såfremt der er risiko for driftsforstyrrelser i forbindelse med opdateringen. Der anvendes software til at overvåge de installerede versioner af software, og vi modtager advarsler om nye sårbarheder via betroede sikkerhedsinformationskilder.

Styring af netværkssikkerhed

Der anvendes opdeling af netværkstrafik igennem brug af VLAN og firewallregler på både software- og hardwareniveau. Der anvendes også "Next Generation Firewall" med nyeste firmware og seneste sårbarhedsscanningspakker. Politikkerne for adgange til services tilpasses til den enkelte service for at sikre den bedste beskyttelse.

Al godkendt netværkstrafik (indgående) kommer igennem vores firewall. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv. Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse.

Vi anvender altid redundante internetforbindelser til at sikre kommunikationen til internettet.

For internetforbindelser stillet til rådighed i forbindelse med hostede ydelser gør følgende sig gældende:

AddPro Danmark A/S benytter sig af separat fremførte fiberforbindelser til internet. AddPro Danmark A/S' interne opsætning understøtter failover ved fejl på fysisk forbindelse eller hos udbyder.

Informationsoverførsel

Vores tekniske setup fokuserer på værdier, og værn mod uvedkommendes adgang til vores data er af højeste prioritet. Vi har desuden antivirussystemer, e-mail-scanning og systemer til overvågning og sikring af netværk og internetbrug. Alle medarbejdere i AddPro Danmark A/S er ansat med en tavshedsaftale.

Leverandørforhold

AddPro Danmark A/S benytter kun velrenommerede, gennemprøvede kvalitetsleverandører, som er i stand til at levere den aftalte kvalitet til en konkurrencedygtig pris, og som er i stand til at opfylde AddPro Danmark A/S' leveringsbehov. Alle godkendte leverandører er oprettet i AddPro Danmark A/S' kreditorsystem.

Én gang årligt gennemgås de væsentligste leverandører for deres leveringsevne, kvalitet, pris og service inkl. marketingassistance. Der vil dog være en løbende vurdering, således at skulle der opstå et problem, vil dette omgående blive løst i samarbejde med den nuværende eller kommende leverandør.

Styring af informationssikkerhedsbrud

Hvis der konstateres en sikkerhedshændelse, adviseres de berørte kunder så hurtigt som muligt, og samtidigt tages der skridt til at sikre data og systemer med henblik på genetablering af normal drift. Efterfølgende udarbejdes en "root cause analysis", for så vidt muligt at sikre at hændelsen ikke kan optræde igen.

Alle sikkerhedshændelser rapporteres til it-sikkerhedsudvalget og dermed til ledelsen.

Alle opgaver registreres i ITSM-systemet, så det fremgår, hvem der har meldt og taget imod sagen, og sager, der vedrører sikkerhedshændelser, skal markeres, så de kan søges frem på et senere tidspunkt.

Service Desk varetager prioritering af alle indkomne opgaver, herunder sørger de for eskalation af sager til relevante afdelinger.

Kunden informeres løbende om udvikling i incidents og ved løsningen af et incident. Ved major incidents vil samtlige nedenstående eskaleringsniveauer være informeret.

Ved alle større sikkerhedshændelser skal support manager og CTO informeres hurtigst muligt. Følgende eskaleringsniveauer gør sig gældende:

a. Service Desk
   i. Tlf.-nr.+45 31 33 44 55
   ii. Mail: Support@addpro.dk
b. Support manager
c. CTO Rasmus Andersen
d. Adm. direktør Brian Sørensen

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

AddPro Danmark A/S har implementeret en række kontroller for at minimere konsekvensen af tabt information og udarbejdet en katastrofeplan for genoprettelse af driften i tilfælde af kritiske forstyrrelser. Fx opbevares backupdata på to fysisk adskilte lokationer, vi arbejder med beregnet overkapacitet på N+1 på hosts og netværk, og UPS samt nødstrømsanlæg testes med fastlagte mellemrum af vores leverandører af datacenter-housing, Global Connect og Cibicom.

AddPro Danmark A/S arbejder løbende med risikovurdering af vores tekniske setup. Risici vurderes relevante enten i form af alvorlighed eller sandsynlighed, og det angives, hvad der gøres for at eliminere eller reducere disse risici.

Generelle risikovurderinger indsamles løbende af den tekniske chef, som i den sammenhæng rapporterer til direktionen og bestyrelsen. Det er medarbejdernes pligt at indrapportere eventuelle nye risici, så snart de får kendskab til dem.

AddPro Danmark A/S' teknikere er fysisk placeret i afstand fra datacenteret. Der er redundans på alle medarbejdere, så der altid er kompetent personale til rådighed uanset tidspunktet og situationen.

3.4 Overensstemmelse

Vi er ikke underlagt særlig lovgivning i forhold til vores ydelse. Det kan vores kunder dog være, og i disse tilfælde er vores understøttelse heraf aftalt særskilt.

Vi lader os årligt revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse.

Vi har en intern kontrol, hvor vi undersøger, om de etablerede politikker og retningslinjer overholdes af medarbejderne. Derudover har vi en kontrol, der sikrer, at vores udstyr såsom servere, netværksudstyr m.m. overholder vores regler for eksempelvis patching og dokumentation for ændringer i software.

Vi følger Microsofts anbefalinger i forhold til patching af deres software.

AddPro Danmark A/S garanterer, at alle tjenester leveres i overensstemmelse med god it-praksis baseret på anbefalinger fra Danish Cloud Community. Medmindre andet er aftalt, vil AddPro Danmark A/S bruge standardværktøjer, der er i overensstemmelse med god praksis, og som er relevante i forhold til it-miljøet med tilhørende infrastruktur.

AddPro Danmark A/S garanterer på alle tidspunkter, at man overholder lovgivningen, og at AddPro Danmark A/S' tjenester leveres i henhold til gældende lovgivning til enhver tid.

3.5 Komplementære kontroller hos kunder

Leverede serviceydelser

Ovenstående systembeskrivelse er baseret på AddPro Danmarks standardvilkår. Kundernes afvigelser af standardvilkår er derfor ikke omfattet.

Brugeradministration

AddPro Danmark tildeler adgang og rettigheder i overensstemmelse med kundens anvisninger, når disse er meldt ind til supporten. AddPro Danmark er ikke ansvarlig for, at disse oplysninger er korrekte, og det er således kundens ansvar at sikre, at adgangen og rettigheder til systemer og applikationer tildeles hensigtsmæssigt.

AddPro Danmark tildeler også adgang til tredjepartskonsulenter – primært udviklere, der skal vedligeholde applikationer, der indgår i hosting-aftalen. Det sker i henhold til instrukser fra AddPros kunder.

Kundens revisorer bør selv validere, at rettigheder til kundens applikationer og miljøer er i overensstemmelse med kundens forventninger, og eventuelle afvigelser skal rapporteres til AddPro Danmark med henblik på at få rettet afvigelser.

Licenser til software, der ikke stilles til rådighed af AddPro Danmark

Det er alene kundens ansvar, at en passende og gyldig licens er købt eller lejet til den software, der bruges eller installeres af kunden.

Det er alene kundens ansvar at sikrer, at deres respektive applikationer eller services ikke krænker tredjemands rettigheder.

3.6 Personfølsomme oplysninger

I det omfang, det er nødvendigt at videregive identificerbare personoplysninger til AddPro Danmark A/S, skal AddPro Danmark A/S acceptere, at videregivelsen er på følgende vilkår:

Generelt

Personoplysninger kan kun anvendes til opfyldelse af en aftale.

Behandling af personoplysninger må kun tillades af den dataansvarlige, eller på anmodning af den dataansvarlige, på vedkommendes ansvar.

Enhver, der behandler personoplysninger, skal være bekendt med denne bestemmelse i aftalen.

Systemer, der anvendes til at opbevare og behandle personoplysninger, skal være konstrueret til at forhindre adgang af uautoriserede personer.

Personoplysninger må ikke opbevares på en måde, som muliggør identifikation af de registrerede for en periode, der overstiger den tid, der kræves for at opfylde aftalen.

Elektronisk information

I tilfælde af overførsel af identificerbare personoplysninger via internettet eller et andet eksternt net skal der træffes de nødvendige sikkerhedsforanstaltninger for at undgå, at oplysningerne kan tilgås af uautoriserede personer. Information skal som minimum være forsvarligt krypteret under hele transmissionen. Ved brug af interne netværk skal det sikres, at uvedkommende ikke kan få adgang til disse oplysninger.

Flytbare lagermedier, backup af data m.v. skal holdes forsvarligt og krypteret og på en sådan måde, at uautoriserede personer ikke kan få adgang til oplysningerne.

Ved levering

Oplysningerne skal slettes eller tilintetgøres, når lagring ikke længere er nødvendig for at opfylde aftalen.

Sletning af oplysninger fra elektroniske medier skal ske på en sådan måde, at oplysningerne ikke kan gendannes.

Aftalen medfører ikke overførsel af information til lande uden for EU/EØS-lande.

I overensstemmelse med Datatilsynets "Krav til en skriftlig aftale med databehandlere" af 2. maj 2001, skal følgende også gælde:

AddPro Danmark A/S skal handle i overensstemmelse med instrukser fra kunden, med hensyn til de oplysninger virksomheden får adgang til. AddPro Danmark A/S skal træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger for at forebygge, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller gøres utilgængelige, eller kommer til uautoriserede personers kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger. AddPro Danmark A/S skal på kundens anmodning give kunden tilstrækkelige oplysninger til at kunne kontrollere, at der er truffet de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger.

AddPro Danmark A/S har principielt ikke adgang til kundens data og dermed heller ikke til personfølsomme data. AddPro Danmark A/S er således databehandler. AddPro Danmark A/S underskriver en standarddatabehandleraftale med kunden, som fastslår AddPro Danmark A/S' forpligtelser.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunder er ikke omfattet af vores testhandlinger.

Vores test af funktionaliteten har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2 Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontrollerne er implementeret og har fungeret i perioden fra 1. januar 2023 til 31. december 2023. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål 4: Risikovurderinger			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
4.1	**Retningslinjer for risikovurderinger** *Virksomheden har en procedure for udarbejdelse af risikovurdering, og der er udarbejdet en aktuel og godkendt risikoanalyse, ligesom der udarbejdes planer for håndtering af risici.* Der foreligger skriftlige procedurer, som indeholder krav om, at der skal udarbejdes risikovurdering. Risikovurderingen skal udarbejdes minimum årligt og godkendes af ledelsen. Risikovurderingen skal indeholde planer for håndtering af risici.	Vi har forespurgt ledelsen om en skriftlig procedure for risikovurdering. Vi har forespurgt ledelsen om den aktuelle risikoanalyse. Vi har endvidere inspiceret, at der foreligger planer for årlig revurdering af risikoanalysen. Vi har inspiceret, at der findes en aktuel risikoanalyse, at den har været gennemgået i Informationssikkerhedsudvalget, og at ledelsen har godkendt risikoanalysen. Vi har inspiceret, at der foreligger planer for håndtering af risici.	Ingen afvigelser noteret.

Kontrolmål 5: Informationssikkerhedspolitikker			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
5.1	**Retningslinjer for styring af informationssikkerhed** *Virksomheden giver retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.* Sikkerhedspolitikker skal være dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken skal være godkendt af ledelsen. Sikkerhedspolitikken er gjort tilgængelig for medarbejderne via intranettet. Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt ledelsen om den seneste sikkerhedspolitik. Vi har inspiceret, at der forefindes en sikkerhedspolitik, og at ledelsen har godkendt sikkerhedspolitikken. Vi har inspiceret, at sikkerhedspolitikken er let tilgængelig for medarbejderne. Vi har inspiceret, at der foreligger planer om revurdering af sikkerhedspolitikken minimum én gang årligt.	Ingen afvigelser noteret.

Kontrolmål 6: Organisering af informationssikkerhed

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.1	**Intern organisering** *Virksomheden etablerer et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver. Der skal opretholdes passende kontakt med relevante myndigheder. Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer. Informationssikkerhed skal opretholdes ved projektstyring.	Vi har forespurgt ledelsen om de organisatoriske roller og ansvar, der gælder i forbindelse med styring af informationssikkerheden. Vi har inspiceret, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret via udvalgte referater fra mødeaktiviteter. Vi har inspiceret, at forhold omkring funktionsadskillelse er vurderet og tilstrækkeligt implementeret, hvor muligt. Vi har inspiceret, at der er uddelegeret ansvar for kontakt med relevante myndigheder. Vi har forespurgt, hvordan der opretholdes kontakt med særlige interessegrupper. Vi har forespurgt ledelsen om retningslinjerne for projektledelse.	Under vores revision af den interne organisering har vi konstateret, at AddPro ikke har afholdt møder i sikkerhedsudvalget. Ingen yderligere afvigelser noteret.
6.2	**Mobilt udstyr og fjernarbejdspladser** *Virksomheden sikrer fjernarbejdspladser og brugen af mobilt udstyr.* Der er udarbejdet politikker og retningslinjer for brugen af mobile enheder. Der er udarbejdet politikker og retningslinjer for fjern- og hjemmearbejdspladser.	Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejdernes brug af mobile enheder. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for brugen af mobile enheder, herunder medarbejdernes eget udstyr (BYOD). Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejdernes brug af hjemmearbejdspladser/fjernarbejdspladser. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for hjemmearbejde. Vi har inspiceret VPN-opsætning til fjernopkobling til det interne netværk.	Ingen afvigelser noteret.

Kontrolmål 7: Personalesikkerhed			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
7.1	**Før ansættelsen** *Virksomheden sikrer, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.* Efterprøvning af alle jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler og skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici. Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har forespurgt ledelsen om procedurerne for rekruttering af medarbejdere. Vi har inspiceret, at der foretages screening af nyansættelser. Vi har inspiceret, at ansættelsesvilkårene indeholder beskrivelser af ansvar i forbindelse med informationssikkerhed. Vi har inspiceret, at der underskrives en fortrolighedsaftale. Vi har inspiceret, at ansøgerne i rekrutteringsforløbet introduceres for retningslinjerne for informationssikkerhed.	Ingen afvigelser noteret.
7.2	**Under ansættelsen** *Virksomheden sikrer, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.* Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer. Medarbejdere skal løbende informeres og gennemgå awareness-træning for at sikre forståelsen for deres ansvar og rolle, således at de kan opfylde deres informationssikkerhedsansvar.	Vi har forespurgt ledelsen om beskrivelsen af kravene til ledere i forhold til opretholdelse af ansvar for informationssikkerheden. Vi har inspiceret, at ledelsesforholdene er velbeskrevne, og at der forefindes let tilgængelige og opdaterede organisationsdiagrammer. Vi har inspiceret, at der er etableret en proces for løbende awareness-træning.	Ingen afvigelser noteret.

Kontrolmål 7: Personalesikkerhed			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
7.3	**Ansættelsesforholdets ophør eller ændring** *Virksomheden beskytter organisationens interesser som led i ansættelsesforholdets ændring eller ophør.* Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med ansættelsesophør. Vi har inspiceret, at der findes en proces til sikring af tilbagelevering af væsentlige aktiver i forbindelse med fratrædelse og suspendering af brugerrettigheder eller lignende. Vi har inspiceret, at brugerrettighederne vurderes i forbindelse med en væsentlig ændring i ansættelsesforholdet. Vi har foretaget stikprøvekontrol af dokumentation for udførelsen.	Ingen afvigelser noteret.

Kontrolmål 8: Styring af aktiver			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
8.1	**Ansvar for aktiver** *Virksomheden identificerer organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.* Alle væsentlige aktiver i relation til information og in- formationsbehandlingsfaciliteter skal identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver, i en database. Det skal fremgå af databasen hvilken status det enkelte aktiv har, inklusive information som beskriver aktivet, samt ansvar og ejerskab.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med identifikation af informationsaktiver. Vi har stikprøvevis inspiceret fortegnelsen over kritiske informationsaktiver. Vi har inspiceret, at det organisatoriske ansvar for informationsaktiver er dokumenteret og implementeret, og at der er placeret ejerskab i forhold til ansvar for den tilhørende informationssikkerhed. Vi har forespurgt ledelsen om procedurerne vedrørende accepteret brug af aktiver.	Ingen afvigelser noteret.
8.3	**Mediehåndtering** *Virksomheden forhindrer uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.* Der skal implementeres procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget. Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer. Medier, der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af bærbare medier. Vi har inspiceret, at der findes en procedure til sikker bortskaffelse af informationsbærende medier. Vi har forespurgt på eksempler på udført bortskaffelse af informationsbærende medie.	Ingen afvigelser noteret.

Kontrolmål 9: Adgangsstyring			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
9.1	**Forretningsmæssige krav til adgangsstyring** *Virksomheden begrænser adgangen til information og informationsbehandlingsfaciliteter.* En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav. Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret politikken for adgangsstyring, herunder om denne er opdateret og godkendt. Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret et udvalg af brugere med henblik på at konstatere, at de kun har adgang til netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.	Ingen afvigelser noteret.

Kontrolmål 9: Adgangsstyring

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
9.2	**Administration af brugeradgange** *Virksomheden sikrer adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.* Alle brugere skal være registreret med et unikt bruger-id, og deres rettigheder til netværk og systemer skal være i overensstemmelse med virksomhedens politikker. Endvidere sikres det, at rettigheder begrænses mest muligt, er betinget af et arbejdsrelateret behov, er godkendt og oprettet korrekt i systemerne. Administratorkonti kontrolleres med jævne mellemrum for at sikre systemets integritet. Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af en formel administrationsproces. Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder. Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med brugeradministration. Vi har stikprøvevis indhentet oversigter over brugerkonti på systemer og netværk. Vi har stikprøvevis udvalgt nye brugere og inspiceret, at anmodning om adgang fra disse var dokumenteret og godkendt i overensstemmelse med relevant sikkerhedspolitik. Vi har forespurgt ledelsen om procedurerne for hemmelig autentifikationsinformation. Vi har inspiceret et udvalg af bruger-review-rapporter, herunder de konklusioner, der er draget. Vi har stikprøvevis sammenholdt oversigten over ophørte brugere med oversigten over aktuelle brugerkonti og inspiceret, at brugerkonti var deaktiveret eller slettet.	Under vores revision af brugeroprettelser har vi for en ud af fire brugerrettelser ikke modtaget dokumentation på, brugeroprettelsen har fulgt AddPros retningslinjer. Vi har noteret, at AddPro har formaliserede retningslinjer for brugerkontrol, men at denne ikke er blevet udført i revisionsperioden. Ingen yderligere afvigelser noteret.

Kontrolmål 9: Adgangsstyring			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
9.3	**Brugernes ansvar** *Virksomheden gør brugerne ansvarlige for at sikre deres autentifikationsinformation.* Det skal være et krav, at brugerne følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation. Adgange til systemer, netværk, databaser og datafiler er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, kompleksitet og udløbstid, ligesom passwordopsætninger medfører, at passwords ikke kan genbruges. Endvidere bliver brugeren deaktiveret ved gentagne fejlagtige forsøg på login.	Vi har inspiceret passwordpolitikken. Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordadministration. Vi har inspiceret passwordindstillingerne i serverinfrastruktur og databaser ved inspektion af konfigurationsudtræk.	Ingen afvigelser noteret.
9.4	**Styring af system- og applikationsadgang** *Virksomheden forhindrer uautoriseret adgang til systemer og applikationer.* Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring. Adgang til systemer og applikationer styres af en procedure for sikker logon. Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet. Brugen af systemer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med retningslinjerne for begrænsning af adgang til information. Vi har inspiceret, at der er implementeret en procedure for sikker logon. Vi har forespurgt ledelsen om anvendelsen af systemer til administration af adgangskoder. Vi har forespurgt ledelsen om anvendelsen af privilegerede systemprogrammer. Vi har forespurgt ledelsen om retningslinjerne for adgang til kildekode.	Ingen afvigelser noteret.

Kontrolmål 10: Kryptografi			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
10.1	**Kryptografiske kontroller** *Virksomheden sikrer korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.* Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information. Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.	Ingen afvigelser noteret.

Kontrolmål 11: Fysisk sikring og miljøsikring			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
11.1	**Fysiske kontroller** *Virksomheden har defineret og anvendt perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.* Der er klassificerede informationsbehandlingsfaciliteter, og adgangen til disse sker på baggrund af denne klassifikation. Faciliteterne er opdelt i tre grupper: Lukket, begrænset og åben. Gæster er kun tilladt i åbne eller begrænsede områder, hvis de ledsages af en medarbejder. Adgang til lukkede områder er tilladt for gæster, hvis de har et arbejdsbetinget behov.	Vi har forespurgt ledelsen om styring af fysisk sikring. Vi har inspiceret, at AddPro Danmark A/S indhenter relevante revisionserklæringer på serviceleverandører samt fører tilsyn med disse.	Ingen afvigelser noteret.
11.2	**Fysisk adgangskontrol** *Virksomhed sikrer områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.* Der er sikret, at adgangen til virksomhedens lukkede områder er sikret, at adgangen til disse områder er begrænset til personer med et arbejdsbetinget behov, og at denne adgang hyppigt revideres.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at adgang til sikre områder er tildelt efter et arbejdsbetinget behov.	Ingen afvigelser noteret.

Kontrolmål 12: Driftssikkerhed

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
12.1	**Driftsprocedurer og ansvarsområder** *Virksomheden sikrer korrekt og sikker drift af informationsbehandlingsfaciliteter* Der skal være tilfredsstillende procedurer og forretningsgange for opretholdelse af driften, herunder find.es overvågning, registrering af hændelser og opfølgning på disse. Nye systemer og væsentlige opgraderinger bliver testet, herunder foretages brugeraccepttest af kvalificerede medarbejdere, og de dokumenteres og godkendes før implementering i produktionsmiljøet. Der udføres endvidere efterfølgende verifikation af implementeringer. Problemer identificeret under udvikling og implementering af nye systemer og væsentlige opdateringer bliver løst tilfredsstillende. Ændringer er underlagt konfigurationsstyring. Nødændringer af systemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende. Anvendelsen af ressourcer skal styres og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemerne fungerer som krævet. Der er implementeret politikker og procedurer til sikring af funktionsadskillelse i virksomheden. Disse politikker og procedurer omfatter krav til: • at ansvar og aktiviteter for udvikling, test og produktion er adskilte • at administratorer med ansvar for produktion har ikke adgang til applikationer og transaktioner.	Vi har forespurgt ledelsen, om alle relevante driftsprocedurer er dokumenteret. I forbindelse med revisionen af de enkelte driftsområder har vi kontrolleret, at der foreligger dokumenterede procedurer, samt stikprøvevis kontrolleret, at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. Vi har stikprøvevis inspiceret ændringsønsker for følgende: • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. • Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. • Dokumenteret plan for tilbagerulning, hvor relevant. Vi har inspiceret brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har noteret, at der ikke er implementeret klare beskrivelser af incident- og change management procedurer, hvilket medfører, at vi har konstateret at en række changes håndteres som incidents uden tilstrækkelig dokumentation af test, godkendelse og fallback-planer. Ingen yderligere afvigelser noteret.

Kontrolmål 12: Driftssikkerhed

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
12.2	**Beskyttelse mod malware** *Virksomheden sikrer, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.* Der er installeret centralt overvåget antivirus på arbejdsstationer og laptops. Disse funktioners databaser opdateres regelmæssigt og kan ikke modificeres af de enkelte medarbejdere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med malwarebeskyttelse. Vi har inspiceret tilstedeværelsen af antivirusprogrammer på arbejdsstationer og laptops.	Ingen afvigelser noteret.
12.3	**Backup** *Virksomheden beskytter mod tab af data.* Det sikres, at der foretages løbende backup af relevante komponenter i infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med backup. Vi har stikprøvevis inspiceret backupprocedurer til bekræftelse af, at de er formelt dokumenteret. Vi har stikprøvevis inspiceret backuplogge vedrørende backups til bekræftelse af, at backups er gennemført succesfuldt; alternativt, at der foretages afhjælpning i tilfælde af mislykkede backups. Vi har stikprøvevis inspiceret restore-logge.	Ingen afvigelser noteret.
12.4	**Logning og overvågning** *Virksomheden registrerer hændelser og tilvejebringe bevis.* Der udføres hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser, som opbevares og gennemgås regelmæssigt. Logningsfaciliteter og logoplysninger er beskyttet mod manipulation og uautoriseret adgang. Transaktioner eller aktiviteter samt brugere med privilegerede rettigheder (fx superbrugere) bliver logget. Dette inkluderer også databaser. Afvigende forhold undersøges og løses rettidigt. Der er etableret tidssynkronisering i hele infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med overvågning af systemanvendelse og logning. Vi har stikprøvevis inspiceret logindstillingerne ud fra systemudtræk af platforme og systemer. Vi har forespurgt til proces og foranstaltninger til sikring mod manipulation af logge. Vi har stikprøvevis gennemgået logge for administratorer og systemoperatører. Vi har forespurgt til konceptet for tidssynkronisering.	Ingen afvigelser noteret.

Kontrolmål 12: Driftssikkerhed			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
12.5	**Styring af driftssoftware** *Virksomheden sikrer integriteten af driftssystemer.* Der bør implementeres procedurer til styring af softwareinstallationen i driftssystemer.	Vi har forespurgt ledelsen om procedure og kontrolaktiviteter, som udføres i forbindelse med softwareinstallationer i driftssystemer.	Ingen afvigelser noteret.
12.6	**Sårbarhedsstyring** *Virksomheden forhindrer, at tekniske sårbarheder udnyttes.* Der er etableret procedurer for patch management, således at kritiske netværkskomponenter, servere og andre enheder holdes opdateret på et passende niveau og overvåges for sikkerhedsmæssige, kritiske rettelser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med patch management. Vi har stikprøvevis inspiceret ændringer til kritiske netværkskomponenter og servere.	Ingen afvigelser noteret.

Kontrolmål 13: Kommunikationssikkerhed			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
13.1	**Styring af netværkssikkerhed** *Virksomheden sikrer beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.* Virksomheden opretter selvstændige virtuelle netværk til kunderne. Der oprettes selvstændige VLAN'er, virtuelle firewalls og virtuelle routingtabeller. Administration af netværksudstyr håndteres udelukkende af autoriseret personale. Der udføres periodiske sårbarheds- og penetrationstests.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med netværksstyring. Vi har foretaget en inspektion af firewallkonfigurationen, samt at der gøres brug af Intrusion Detection-systemer, som løbende og aktivt giver oplysninger om mulige ændringer, der kan påvirke fortroligheden, integriteten og tilgængeligheden af data. Vi har foretaget inspektion af, at netværket er opsat med selvstændige VLAN'er og DMZ-zoner. Vi har inspiceret, at der er foretaget periodisk sårbarheds- og penetrationstest. Vi har inspiceret, at der er taget stilling til konstaterede svagheder samt iværksat tiltag til udbedring.	Vi har noteret, at der ikke systematisk udføres sårbarheds- og penetrationstests. Seneste sårbarhedsscanningsrapport er fra 2020. Ingen yderligere afvigelser noteret.
13.2	**Informationsoverførsel** *Virksomheden opretholder informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.* Der skal være tilfredsstillende procedurer og forretningsgange for datakommunikation, der på hensigtsmæssig måde sikrer mod risiko for tab af ægthed, integritet og fortrolighed. Adgang for administration af kunders systemer kan udelukkende foretages fra virksomhedens kontrollerede netværk. Kritisk netværkskommunikation skal sikres ved anvendelse af sikre protokoller samt autorisation. Mailkommunikation mellem AddPro Danmark og kunderne skal anvende TLS-kryptering mellem mailservere. Der er defineret krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information.	Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter, der udføres i forbindelse med sikker datakommunikation. Vi har foretaget en inspektion af, at administrationen af kunders systemer udelukkende kan foretages via kablet netværk, sikret trådløst netværk eller VPN. Vi har inspiceret konfigurationen, som sikrer, at der anvendes tilstrækkelig kryptering af mailkommunikation. Vi har forespurgt til proceduren for etablering af fortrolighedsaftaler. Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 15: Leverandørforhold			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
15.1	**Informationssikkerhed i leverandørforhold** *Virksomheden sikrer beskyttelse af organisationens aktiver, som leverandører har adgang til.* Der er etableret passende kontroller til sikring af informationssikkerheden i forbindelse med serviceydelser leveret af underleverandør, hvor underleverandøren har adgang til virksomhedens systemer. Hvis relevant for den leverede service, så kræves kontrolerklæringer fra underleverandøren, som vurderes med hensyn til mulige informationssikkerhedsmæssige svagheder i kontrollerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af leverandører. Vi har forespurgt ledelsen, om underleverandører underskriver fortrolighedsaftaler. Vi har stikprøvevist inspiceret, at der er indhentet kontrolerklæringer for relevante leverandører.	Ingen afvigelser noteret.

Kontrolmål 16: Styring af informationssikkerhedsbrud			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
16.1	**Styring af informationssikkerhedsbrud og forbedringer** *Virksomheden sikrer en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.* Der er placeret ledelsesansvar og etableret procedurer til at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. Alle sikkerhedshændelser rapporteres til og behandles i Informationssikkerhedsudvalget, som sikrer, at hændelserne gennemgås med det primære formål at sikre passende tiltag til forebyggelse af gentagelser. Medarbejderne er via retningslinjerne instrueret om at indrapportere alle informationssikkerhedssvagheder, de måtte mistænke eller opdage.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med håndtering af sikkerhedshændelser. Vi har inspiceret udleveret materiale vedrørende behandling af sikkerhedshændelser i mødereferater fra Informationssikkerhedsudvalget og security incidentlogge. Vi har inspiceret retningslinjerne.	Ingen afvigelser noteret.

Kontrolmål 17: Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
17.1	**Informationssikkerhedskontinuitet** *Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.* Den samlede plan for katastrofeberedskab er opbygget af en overordnet katastrofestyringsprocedure samt operationelle katastrofeplaner for de konkrete katastrofeområder. Den operationelle katastrofeplan indeholder beskrivelse af katastrofeorganisationen med de ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser for de nødvendige indsatsgrupper. Liste over kunder samt procedurebeskrivelser skal være på plads. Der foretages minimum årlig test af katastrofeberedskabet i form af såvel skrivebordstest som faktiske testscenarier. Disse tests kan være i form af almindelige operationelle procedurer i forbindelse med systemvedligeholdelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret det udleverede materiale vedrørende katastrofeberedskabet samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vi har noteret, at planen for katastrofeberedskab ikke er testet som planlagt. Vi har noteret, at det i beredskabsplanen fremgår, at der er krav til årlig test. Ingen yderligere afvigelser noteret.
ok17.2	**Redundans** *Virksomheden sikrer tilgængelighed af informationsbehandlingsfaciliteter.* Alle datacenterets fælles infrastrukturenheder er dimensioneret med redundante enheder. Alle systemer har derfor en individuel backup. Internetforbindelsen er ligeledes redundant.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret udleveret materiale vedrørende strøm (herunder UPS), køling, firewalls, servere (hosts), disksystemer og internetforbindelse.	Ingen afvigelser noteret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Brian Sørensen
Kunde
Serienummer: f54a7919-d3b2-440d-a6bd-032d436eb654
IP: 80.208.xxx.xxx
2024-03-05 17:49:21 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2024-03-05 18:03:53 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 80.208.xxx.xxx
2024-03-05 19:07:35 UTC