Enversion A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2020 til 31. december 2020 i relation til Enversions SaaS-ydelse kaunt

April 2021

Indholdsfortegnelse

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Enversions SaaS-ydelse kaunt, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i kunders regnskaber.

Enversion anvender ECIT Solutions A/S og Microsoft Ireland Operations Ltd. som serviceunderleverandører af en række hosting ydelser. Erklæringen anvender partielmetoden og omfatter således ikke kontrolaktiviteter, som ECIT Solutions A/S og Microsoft Ireland Operations Ltd. varetager for Enversion.

Enversion bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af Enversions SaaS-ydelse kaunt, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt 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 Enversions SaaS-ydelse kaunt 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 de generelle it-kontroller

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt foretaget i perioden fra 1. januar 2020 til 31. december 2020

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt, 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 Enversions SaaS-ydelse kaunt, 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 2020 til 31. december 2020. 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 2020 til 31. december 2020.

Aarhus, den 20. april 2021
Enversion A/S

Jacob Høy Berthelsen
CEO & Founder Enversion A/S

Frank Aaquist
CEO Kaunt A/S

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 2020 til 31. december 2020 i relation til Enversions SaaS-ydelse kaunt

Til: Enversion, deres kunder og kunders revisor

Omfang

Vi har fået som opgave at afgive erklæring om Enversions beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2020 til 31. december 2020, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Enversion anvender ECIT Solutions A/S og Microsoft Ireland Operations Ltd. som serviceunderleverandører af en række hosting ydelser. Erklæringen anvender partielmetoden og omfatter således ikke kontrolaktiviteter, som ECIT Solutions A/S og Microsoft Ireland Operations Ltd. varetager for Enversion.

Enversions ansvar

Enversion 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 FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Enversions 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 retvisende, 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 sin ydelse samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev 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 Enversion 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

Enversions 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 SaaS-ydelsen kaunt, 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, hvordan generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt, således som de var udformet og implementeret i hele perioden fra 1. januar 2020 til 31. december 2020, i alle væsentlige henseender er retvisende, 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 2020 til 31. december 2020, 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 2020 til 31. december 2020.

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 Enversions SaaS-ydelse kaunt, 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 20. april 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jess Kjær Mogensen
statsautoriseret revisor

Rico Lundager
senior manager

3. Enversions beskrivelse af generelle it-kontroller i relation til Enversions SaaS-ydelse kaunt

Indledning

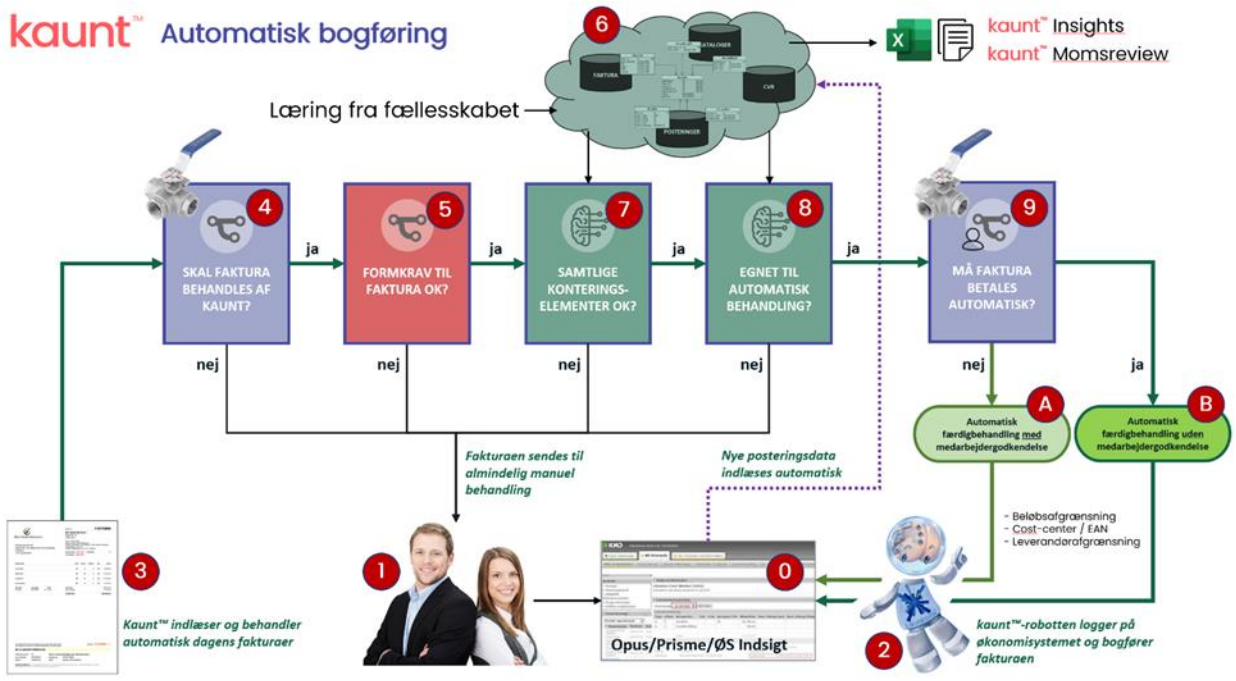
Formålet med nærværende beskrivelse er at levere information til Enversion A/S' og Kaunt A/S' kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Omfanget af denne beskrivelse er en afdækning af de tekniske og organisatoriske sikkerhedsforanstaltninger, som er implementeret i forbindelse med Enversions software as a service (SaaS)-ydelse kaunt.

Beskrivelse af Enversion A/S

Enversion A/S er en it-virksomhed med base i Aarhus, DK. Vi har siden 2009 arbejdet med at udvikle intelligente assistenter, der hjælper vores kunder med at træffe de bedste beslutninger på baggrund af proaktiv brug af data. Vores faglige kompetencer inden for datamodellering, maskinlæring og kunstig intelligens er i verdensklasse, og vores ambitioner om at levere det bedste på markedet er tårnhøje. Vi vil til enhver tid hellere prøve en god ide af i praksis end slå den ihjel med regneark og businesscases, og vi insisterer på retten til at være lige dele idealister og opportunister i vores tilgang til verden. Hver dag går vi på arbejde med vores mission for øje: At levere markedets smarteste dataløsninger og bidrage til at gøre menneskers liv bedre, gladere og længere.

I den følgende gennemgang af kaunt™ henvises til nummereringen i nedenstående figur. Figuren beskriver det komplette daglige operationelle workflow.



Figur 1 – Beskrivelse af kaunt

kaunt™ er en SaaS (software as a service)-løsning, der udnytter en kombination af to teknologier:

- RPA (Robot Process Automation), dvs. software, der kan interagere med brugergrænsefladen i eksisterende it-systemer – i dette tilfælde it-systemer, der anvendes til at behandle og bogføre indkomne leverandørfakturaer.

- ML (Maskinlæring), dvs. algoritmer, der kan se mønstre i data – i dette tilfælde algoritmer, der kan udlede en korrekt kontering for en indgående faktura baseret på den læring, algoritmen har fået ved at kigge på den historiske kontering af indgående fakturaer.

0. Fokuspunktet for kaunt™ er kundens eksisterende workflowsystem til behandling af indkomne leverandørfakturaer. Ofte behandles indkomne fakturaer direkte i kundens økonomisystem, men i nogle tilfælde vælger kunden, at behandlingen skal ske i et indkøbssystem eller et dedikeret workflowsystem.

1. Kunden vil typisk oprette en række medarbejdere som brugere af økonomi- og/eller workflowsystemet. Disse medarbejdere har et ansvar for at behandle indkomne fakturaer (og kan derudover løse en lang række andre opgaver, afhængigt af hvilke rettigheder de tildeles). Ved oprettelse af brugeradgange til medarbejdere tager kunden stilling til, hvilke rettigheder disse medarbejdere skal have.

2. Kunden opretter kaunt™ som en helt almindelig bruger af økonomi- og/eller workflowsystemet. Kunden tildeler kaunt™ præcis de rettigheder, der er nødvendige for at kunne bogføre indkomne fakturaer. kaunt™ kan som RPA-robotbruger derfor ikke gøre noget, der ikke er givet tilladelse til. Derudover vil kaunt™, som alle andre oprettede bruger, blive genstand for systematisk logning. kaunt™ har dermed ingen mulighed for at udføre arbejde, der ligger ud over de tildelte privilegier eller unddrager sig almindeligt tilsyn. Specielt har kaunt™ ingen mulighed for at rette i logfiler, slette spor efter sig selv eller på anden vis unddrage sig opmærksomhed.

3. I daglig operationel drift kigger kaunt™ i dagens fakturaindbakke ved at logge sig ind i systemet (som enhver anden bruger). I indbakken ligger fakturaer, der er klar til behandling af kundens brugere. Da kaunt™ typisk arbejder om natten, vil der ligge mange ubehandlede fakturaer i indbakken. Hver faktura vurderes individuelt af kaunt™'s fakturabehandlingsalgoritmer (4, 5, 7 og 8).

4. Kunden har (via regler) mulighed for at frasortere fakturaer, som kaunt™-brugeren ikke skal/må behandle på nogen måde. Det kan fx være fakturaer, der ønskes behandlet i et andet projektstyringssystem eller i et indkøbsordresystem (P2P-system). Hvis reglen er opfyldt, stopper kaunt™ behandlingen af fakturaen og lader den ligge urørt i indbakken.

5. kaunt™ tjekker, om den pågældende faktura lever op til god skik for fakturaer. Dvs. det kontrolleres, om de elementer, der er nødvendige for at kunne behandle fakturaen automatisk, er til stede. Eksempelvis skal der være et gyldigt CVR-nummer på en leverandør og et gyldigt EAN-nummer på en fakturamodtager. Hvis formkravene ikke er opfyldt, overlades fakturabehandlingen til de almindelige brugere (1).

7. Baseret på historiske data og læring af konteringsmønstre (6) vurderer kaunt™, om det er muligt at identificere alle de konteringselementer, der er nødvendige for at kunne bogføre fakturaen. Dette kan fx være et kontonummer, ydelsesmodtager ift. registrantkontering samt et cost-center. Hvis dette er tilfældet, sendes fakturaen videre til næste skridt (8). Hvis ikke, overlades fakturabehandlingen til de almindelige brugere (1).

8. Før fakturaen sendes til bogføring, foretages en risikovurdering af fakturaen. Her vurderes, om der er forhold ved fakturaen, der gør den uegnet til automatisk behandling. Hvis fakturaen fx ligner en dobbeltfaktura, eller hvis fakturaens indhold giver anledning til bekymring, overlades fakturabehandlingen til de almindelige brugere (1). Hvis alt er o.k., er fakturaen klar til automatisk bogføring.

9. Kunden udvælger en superbruger, der via en brugergrænseflade kan opstille regler for, hvornår en faktura kan sendes automatisk til betaling (uden medarbejdergodkendelse, B), og hvornår en faktura skal godkendes af en medarbejder, før den betales (A). Al aktivitet i denne brugergrænseflade logges af kaunt™.

A./B.: kaunt™ RPA-brugeren (2) spørger ML-algoritmerne, hvordan den skal behandle den pågældende faktura, og vil herefter indtaste konteringsoplysningerne i brugergrænsefladen til økonomi- og/eller workflowsystemet og afhængigt af udfaldet (A eller B) sende fakturaen til betaling.

Omfang af denne beskrivelse

Enversion A/S er leverandør af software as a service inden for blandt andet automatisk fakturahåndtering (kaunt™).

Enversion A/S har ansvaret for at etablere og opretholde passende procedurer og kontroller med henblik på at adressere alle relevante it-sikkerhedsaspekter, herunder også overholdelse af krav fra GDPR.

Enversion A/S er certificeret inden for den internationale standard for informationssikkerhed, ISO 27001, samt den tekniske standard relateret til beskyttelse af persondata i overensstemmelse med GDPR (EU) 2016/679.

Forretningsstrategi/it-sikkerhedsstrategi

Det strategiske formål i Enversion A/S er at indbygge den nødvendige sikkerhed i vores forretning, så selskabet ikke påføres uacceptable risici til ulempe for os og – ikke mindst – vores kunder.

Hos Enversion er vi dedikerede til at hjælpe mennesker ved hjælp af data. Derfor er informationssikkerhed i fokus og en integreret del af hverdagen hos os. For yderligere information, besøg kaunt.com: https://kaunt.com/about/company/

Enversion A/S' organisation og organisering af it-sikkerhed

Overordnet ansvarlig er CEO, der har uddelegeret ansvaret for it-sikkerheden til Information Security Manager og Data Protection Officer.

Der udarbejdes altid en samarbejdsaftale og databehandleraftale med kunden, inden arbejdet påbegyndes.

Idet kaunt™-løsningen og antallet af kunder, der benytter kaunt, har udviklet sig med hastige skridt i løbet af 2020 er der foretaget en omstrukturering af virksomheden, således at kaunt™ og alle aktiviteter forbundet hermed er flyttet til Kaunt A/S i starten af 2021. I oktober 2020 tiltrådte Kaunt A/S' direktør Frank Aaquist. Kaunt A/S og Enversion A/S er søsterselskaber og begge en del af Enversion Holding Group ApS. Begge selskaber er omfattet af det informationssikkerhedsmæssige setup.

Risikostyring i Enversion A/S

Det er Enversions politik, at de risici, der følger selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde og tilbyde en tilfredsstillende SaaS-løsning til kunderne. Enversions kvalitetsledelsessystem (opbygget iht. krav i ISO 27001:2013) sikrer, at processer og procedurer er effektivt implementeret, hvilket monitoreres løbende.

Enversion har indarbejdet faste procedurer for risikovurdering af forretningen og de kunderelaterede løsninger. Vi sikrer dermed, at de risici, som er forbundet med de services, vi udbyder, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderingen ligger hos ledelsen.

Håndtering af it-sikkerhed

Information Security Manager (ISM) hos Enversion har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet Enversions struktur for it-sikkerhed. It-sikkerhedspolitikkerne revideres minimum én gang årligt.

Enversions kvalitetsledelsessystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker SaaS til kunderne. For at kunne gøre det er der indført politikker og procedurer, der sikrer, at Enversions leverancer er ensartede og gennemsigtige.

Enversions it-sikkerhedspolitikker er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere. It-sikkerhedspolitikkerne er udarbejdet, så Enversion har ét fælles regelsæt. Dermed opnås en høj kvalitet og et højt sikkerhedsniveau af SaaS. Der foretages løbende forbedringer af både politikker, procedurer og processer.

Kontroller og sikkerhedsforanstaltninger

Enversion har valgt at blive certificeret i henhold til ISO 27001:2013 og har dermed implementeret relevante sikkerhedsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitik
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhed
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse med lov- og kontraktkrav

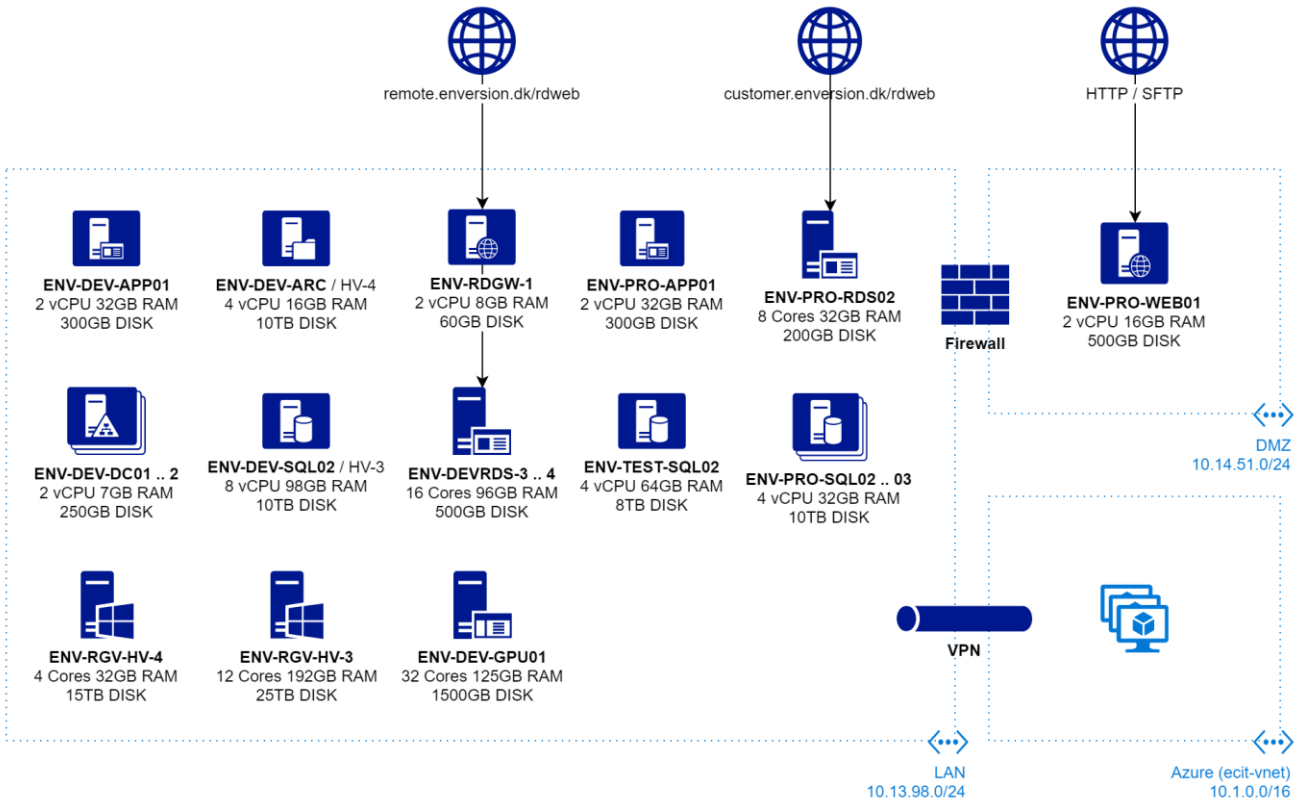
Scope for denne erklæring er:

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

Der henvises til afsnit 4 for uddybning af kontrolmål og kontrolaktiviteter i relation til ovenstående.

Teknisk setup af kaunt

Nedenstående figur viser det tekniske setup mellem ECIT/Enversion. På figuren ses, hvilke servere der findes hos ECIT, og at miljøet er sikret og kun kan tilgås med specifikke rettigheder og tofaktorgodkendelse.



Figur 2 – Teknisk setup ECIT/Enversion

Hosting ved ECIT

ECIT er godkendt hostingleverandør hos Enversion. Leverandøren sikrer den højeste driftsstabilitet og sikkerhed i forbindelse med hele Enversions it-infrastruktur.

Beskrivelse af ydelse ved ECIT

ECIT's hosting-miljø er dækket ind med eget nødstrømsanlæg bestående af nødstrømsakkumulator (UPS).

Hosting-miljøet er sikret mod brand med et automatisk brandbekæmpelsessystem.

Alle rackskabe er forsynet med to stk. 32 ampere (A)-grupper i separat fremførte kabelforsyninger. Disse fordeles til otte undersikringer af hver maks. 10 ampere (A). Alle fremføringer sidder parvist på hver sin hovedsikring.

ECIT's kølingsanlæg består af et fuldt ud redundant system, hvor de enkelte kølingsenheder overvåges centralt.

For at sikre mod tyveri er ECIT's datacenter sikret med nyeste alarmteknologi med adgangskontrol på samme sikkerhedsniveau som terrorsikring. Eksternt bliver hele bygningen overvåget via IP-kameraer med bevægelsesdetektorer. Inde i datacentret er der konstant måling af temperatur, røg og brand.

Der er hundepatrulje tilknyttet datacentret 24 timer i døgnet. Sikkerhedsvagten tilkaldes med strakskørsel i tilfælde af alarm.

ECIT tilstræber at have serverkapacitet efter følgende princip for delte miljøer: At udstyret er kraftigt nok til at afvikle den aftalte drift hos Enversion.

Der anvendes serverhardware fra markedsledende producenter såsom HP C-class blade infrastructure, Proliant servere m.v.

Til storage-system anvendes markedsledende SAN/Storage-teknologi som eksempelvis HP enterprise class dedikeret storage. Desuden anvendes andres SAN-systemer. Den tekniske opbygning af SAN-systemerne er sådan, at der er fysisk separation af dels controllere og dels storage enclosures. Sådan garanteres, at spejling af data sker som mirror, og at data findes på to harddiske på to forskellige fysiske enclosures bag ved to fysisk separate controllere. SAN-systemerne er SSD/Flash Storage-accelererede.

Der tages daglig backup af alle servere på datacentret.

ECIT overvåger hvert 5. minut linjer, switche, routere og driftsanlægget generelt, herunder røg, brand og temperatur via alarmcentral.

Firewall: BSD- og Linux-baserede security appliances for afgrænsning mod internettet i redundant setup. Systemet anvender intrusion detection og stateful packet inspection.

Kontroller udført hos ECIT er ikke indeholdt i denne erklæring. Her henvises til ECIT 3402-erklæring.

Hosting hos Microsoft Ireland Operations Ltd.

Der anvendes Microsoft Azure infrastruktur og services som en del af løsningen til at fremme databehandlingen og lette integrationer, samt sikre skalerbarhed ift. udvidelse af løsningen efter behov.

Microsoft Azure miljøet er forbundet via site2site vpn med whitelisting af IP'er til ECIT miljøet.

Kontroller udført hos Microsoft Ireland Operations Ltd er ikke indeholdt i denne erklæring. Her henvises til 3402-erklæring vedrørende Microsoft Azure.

Komplementerende kontroller

Kunder er ansvarlige for brugeradministration i egne systemer, samt at meddele kaunt™ hvilke af kundens brugere, der skal tildeles/fratages adgange til platformen. Øvrige kontroller fremgår af aftalen med kunden.

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 2020 til 31. december 2020. Dette omfatter bl.a. vurdering af patching-niveau, segmentering, passwordkompleksitet mv..
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

A.5 Kontrolmål: Der er etableret passende overordnede retningslinjer

Enversion-kontrol	PwC-test	Resultat af test
5.1.1 Politikker for informationssikkerhed *Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.* Sikkerhedspolitikken er dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken er godkendt af ledelsen. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere via Enversion Management System (EMS).	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har ved inspektion observeret, at der eksisterer en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har ved inspektion konstateret, at sikkerhedspolitikken gennemgås mindst én gang årligt.	Ingen væsentlige svagheder noteret.
5.1.2 Gennemgang af politikker for informationssikkerhed *Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Informationssikkerhed og tiltag herunder varetages af QA, ISM, DPO og ledelsen.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har ved inspektion observeret, at politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i forbindelse med væsentlige ændringer.	Ingen væsentlige svagheder noteret.

A.6 Kontrolmål: Der er etableret passende forretningsgange og kontroller for organisering af informationssikkerhed		
Enversion-kontrol	**PwC-test**	**Resultat af test**
6.1.1 Roller og ansvarsområder for informationssikkerhed *Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.* Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer. Vi har observeret, at informationssikkerhed og tiltag herunder varetages af afdelingsledelsen og støttes af en stabsfunktion.	Ingen væsentlige svagheder noteret.
6.1.2 Funktionsadskillelse *Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.* Enversions ledelse har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse. Dette sikrer, at udviklings- og driftsaktiviteter er adskilt, medmindre der eksisterer et arbejdsbetinget behov for andet.	Vi har overordnet drøftet proceduren/kontrolaktiviteterne, der udføres, med ledelsen. Vi har observeret, at der er implementeret politikker og procedurer, der sikrer et passende niveau af funktionsadskillelse. Vi har inspiceret, at der er funktionsadskillelse på miljøer ved ECIT.	Ingen væsentlige svagheder noteret.

A.7 Kontrolmål: Der er etableret passende forretningsgange og kontroller for styring af medarbejdersikkerhed

Enversion-kontrol	PwC-test	Resultat af test
7.1.1 Screening *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.* Ledelsen skal sikre, at der udføres en screening af ansøgere inden en ansættelse.	Vi har overordnet drøftet procedurer/kontrolaktiviteter, der udføres, med ledelsen og gennemgået proceduren for screening af jobkandidater.	Ingen væsentlige svagheder noteret.
7.1.2 Ansættelsesvilkår og -betingelser *Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.* Enversion har fastlagt regler for fortrolighedsaftaler, som medarbejdere underskriver ved ansættelse, og erklæringer, som eksterne konsulenter underskriver forud for deres arbejde, såfremt relevant.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Ved stikprøver har vi observeret, at fortrolighedsaftaler anvendes i henhold til retningslinjerne, herunder: • at medarbejdere underskriver fortrolighedsaftaler ved ansættelsen • at eksterne konsulenter med adgang til fortrolige data underskriver fortrolighedsaftaler forud for det aftalte arbejde.	Ingen væsentlige svagheder noteret.
7.2.1 Ledelsesansvar *Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.* Enversion har for både medarbejdere og leverandører fremsat krav gennem kontrakter, som sikrer, at organisationens fastlagte politikker og procedurer opretholdes.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der foreligger underskrevne kontrakter for både medarbejdere og leverandører, så organisationens krav til informationssikkerhed opretholdes.	Ingen væsentlige svagheder noteret.

A.7 Kontrolmål: Der er etableret passende forretningsgange og kontroller for styring af medarbejdersikkerhed

Enversion-kontrol	PwC-test	Resultat af test
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed *Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.* Enversion introducerer medarbejderne til informationssikkerheden i forbindelse med ansættelse via både menneskelig introduktion og krav til gennemlæsning af sikkerhedspolitikkerne og relevante dele af EMS. Der laves også yderligere awareness-tiltag i løbet af forretningsåret. Enversion har, hvor det er relevant, fastsatte krav med leverandører vedrørende informationssikkerhed, som er i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at medarbejderne periodisk skal gennemføre et undervisningsforløb for at opretholde organisationens sikkerhedskrav. Vi har for leverandørerne observeret, at der er udarbejdet kontrakter, som sikrer, at organisationens krav vedrørende informationssikkerheden opretholdes.	Ingen væsentlige svagheder noteret.
7.3.1 Ansættelsesforholdets ophør eller ændring *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.* Enversion sikrer, at brugerrettigheder til operativsystemer, netværk, databaser mv. vedrørende fratrådte medarbejdere inaktiveres rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at medarbejdernes rettigheder til operativsystemer, netværk, databaser, mv. nedlægges i forbindelse med fratrædelse.	Ingen væsentlige svagheder noteret.

A.8 Kontrolmål: Der er etableret passende forretningsgange og kontroller for styring af informationsrelaterede aktiver		
Enversion-kontrol	**PwC-test**	**Resultat af test**
8.1.1 Fortegnelse over aktiver *Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.* Enversion har udarbejdet en fortegnelse over kritiske aktiver og implementeret procedurer, der sikrer løbende vedligeholdelse heraf.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er etableret kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver ejet af Enversion.	Ingen væsentlige svagheder noteret.
8.2.1 Klassifikation af information *Information skal klassificeres efter lovmæssige krav efter værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.* Enversion har etableret retningslinjer, som sikrer, at medarbejderne er informeret om organisationens krav til klassificering af information.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er etableret kontroller i relation til klassifikation af information.	Ingen væsentlige svagheder noteret.

A.9 Kontrolmål: Der er etableret passende forretningsgange og kontroller for adgangsstyring

Enversion-kontrol	PwC-test	Resultat af test
9.1.1 Politik for adgangsstyring *En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.* Enversion har etableret retningslinjer, som sikrer, at medarbejderne tildeles rettigheder ud fra et arbejdsbetinget behov, og som opfylder organisationen krav til informationssikkerhedskrav.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er etableret retningslinjer for adgangskontroller.	Ingen væsentlige svagheder noteret.
9.1.2 Adgang til netværk og netværkstjenester *Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.* Enversion gennemgår alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler for at sikre overensstemmelse med virksomhedens politikker og dermed sikre, at rettigheder er tildelt ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved stikprøvevis inspektion gennemgået udvalgte sikkerhedsgrupper, der giver rettigheder til kaunt-systemer, og klarlagt, hvorvidt medarbejderne oprettes ud fra et arbejdsbetinget behov. Vi har observeret, at der hos Enversion findes dokumentation for, hvilke medarbejdere der har hvilke rettigheder i forbindelse med kaunt.	Ingen væsentlige svagheder noteret.
9.2.1 Brugerregistrering og -afmelding *Der skal implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.* Enversion har etableret en politik for adgangskontrol, der beskriver relevante aspekter af brugerrettighed. Endvidere er der oprettet en procedure for on- og offboarding af medarbejdere, som netop beskriver registrering og afmelding af brugere.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er procedurer for brugeradministrationen, og ved stikprøvevis inspektion observeret, at der findes en formel procedure for brugerregistrering- og afmelding.	Ingen væsentlige svagheder noteret.

A.9 Kontrolmål: Der er etableret passende forretningsgange og kontroller for adgangsstyring

Enversion-kontrol	PwC-test	Resultat af test
9.2.2 Tildeling af brugeradgang *Der skal implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.* Enversion har tilrettelagt processer, som sikrer, at tildelte brugeradgange er i overensstemmelse med et arbejdsbetinget behov. Alle tekniske autorisationer hos Enversion, der har berøring med kundemiljøer, godkendes løbende af den systemansvarlige. De implementerede autorisationsprocedurer hos Enversion sikrer, at oprettelse af brugere og tildeling af rettigheder sker efter godkendelse fra en bemyndiget person (den systemansvarlige for det respektive system). Alle adgange hos Enversion er personlige og behandles fortroligt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Enversion har tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring. Vi har ved stikprøvevis inspektion observeret, at tildeling af adgange godkendes samt tildeles ud fra et arbejdsbetinget behov.	Ingen væsentlige svagheder noteret.
9.2.3 Styring af privilegerede adgangsrettigheder *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* Enversion har tilrettelagt formaliserede processer, som sikrer, at tildelte brugeradgange, inklusive brugere med privilegerede rettigheder, er i overensstemmelse med et arbejdsbetinget behov. Alle brugerkonti hos Enversion er personlige og behandles fortroligt, ligesom der foretages verificering af brugers identitet, inden denne autoriseres. Anvendelse af privilegerede rettigheder overvåges løbende. Afvigende forhold undersøges og løses rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Enversion har tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring, som tillige omfatter brugere med privilegerede rettigheder. Vi har observeret, at tildelte privilegerede autorisationer er tildelt ud fra et arbejdsbetinget behov.	Ingen væsentlige svagheder noteret.

A.9 Kontrolmål: Der er etableret passende forretningsgange og kontroller for adgangsstyring

Enversion-kontrol	PwC-test	Resultat af test
9.2.4 Styring af hemmelig autentifikationsinformation om brugere *Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af en formel administrationsproces.* Ved brugeroprettelse eller nulstilling af password skal brugere tildeles et sikkert, midlertidigt password, som skal ændres umiddelbart efter første anvendelse. IT skal etablere og vedligeholde en procedure for, hvordan en brugers identitet fastslås, før et nyt midlertidigt password må udleveres. Midlertidige passwords skal være unikke, må ikke genbruges og skal opfylde de almindelige krav til passwords. Passwords må ikke bruges privat eller deles.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har inspiceret Enversions retningslinjer for passwords.	Ingen væsentlige svagheder noteret.
9.2.5 Gennemgang af brugeradgangsrettigheder *Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.* Medarbejdere tildeles rettigheder ud fra et arbejdsbetinget behov for interne systemer. Disse standardrettigheder tilføjes og fjernes ved enten ansættelse, flytning eller fratrædelse hos Enversion. Enversion foretager løbende gennemgang af medarbejdernes rettigheder. Dermed sikres overensstemmelse med medarbejderens arbejdsbetingede behov.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at systemejere hver tredje måned opfordres til at revurdere adgange til deres systemer.	Ingen væsentlige svagheder noteret.
9.2.6 Inddragelse eller justering af 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.* Enversion sikrer, at brugerrettigheder til operativsystemer, netværk, databaser mv. vedrørende fratrådte medarbejdere inaktiveres rettidigt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved stikprøvevis inspektion kontrolleret, at brugerrettigheder til systemer i forbindelse med kaunt vedrørende fratrådte medarbejdere inaktiveres rettidigt.	Ingen væsentlige svagheder noteret.

A.9 Kontrolmål: Der er etableret passende forretningsgange og kontroller for adgangsstyring

Enversion-kontrol	PwC-test	Resultat af test
9.3.1 Brug af hemmelig autentifikationsinformation *Det bør være et krav, at brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.* Enversion har udarbejdet retningslinjer for passwords samt oprettelse og opbevaring af disse.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har inspektion observeret, at Enversion har udarbejdet en passwordpolitik samt guidelines, der beskriver oprettelse samt opbevaring af passwords. Vi har ved inspektion observeret, at passwordpolitikken på AD ved ECIT lever op til Enversions guidelines.	Ingen væsentlige svagheder noteret.
9.4.1 Begrænset adgang til informationer *Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring.* Enversion har udarbejdet retningslinjer for administration af, og kontrol med, autorisationer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Enversion har udarbejdet retningslinjer for administration af, og kontrol med, autorisationer.	Ingen væsentlige svagheder noteret.
9.4.2 Procedurer for sikker log-on *Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker log-on.* Enversion anvender tofaktorautentifikation, hvor det er relevant (baseret på risiko).	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at der er anvendes tofaktorautentifikation ved adgang til kundemiljøer via RDS ved ECIT.	Ingen væsentlige svagheder noteret.
9.4.3 System for administration af passwords *Systemer til administration af passwords skal være interaktive og skal sikre passwords af god kvalitet.* Enversion har etableret en politik for oprettelse, ændring og beskyttelse af passwords. Herunder anbefales brugen af password managers.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at Enversion har implementeret en passende passwordpolitik samt retningslinjer for passwords.	Ingen væsentlige svagheder noteret.
9.4.4 Brug af privilegerede systemprogrammer *Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.* Enversion har formelle politikker for software på sine enheder, der beskriver retningslinjer for installation af programmer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der findes en politik for installation af software.	Ingen væsentlige svagheder noteret.
9.4.5 Styring af adgang kildekoder til programmer *Adgang til kildekoder til programmer bør begrænses.* Enversion har etableret en procedure, således at kun medarbejdere med et arbejdsbetinget behov har adgang til kildekode.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion påset, at kun medarbejdere med et arbejdsbetinget behov har adgang til kildekode.	Ingen væsentlige svagheder noteret.

A.11 Kontrolmål: Der er etableret passende forretningsgange og kontroller for fysisk sikkerhed

Enversion-kontrol	PwC-test	Resultat af test
11.1.1 Fysisk perimetersikring *Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.* Enversion har udarbejdet retningslinjer for fysisk perimetersikring af kontorfaciliteter.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har påset, at Enversion har udarbejdet retningslinjer for fysisk perimetersikring af kontorfaciliteterne. Vi har inspiceret, at adgange til kontoret logges i syv dage.	Ingen væsentlige svagheder noteret.

A.12 Kontrolmål: Der er etableret passende forretningsgange for styring og overvågning af drift

Enversion-kontrol	PwC-test	Resultat af test
12.1.2 Ændringsstyring *Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres.* Enversion har formaliserede interne retningslinjer, forretningsgange og beskrivelser, der omfatter change management.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har observeret, at Enversion har udarbejdet formaliserede interne retningslinjer, forretningsgange og beskrivelser relateret til change management.	Ingen væsentlige svagheder noteret.
12.1.4 Adskillelse af udviklings-, test- og driftsmiljøer *Udviklings-, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.* Enversion har etableret separate it-miljøer for udvikling, test og produktion. Kun personale med funktionsadskilte rettigheder kan migrere ændringer mellem miljøerne.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og observeret, at der, jf. retningslinjerne, er etableret separate miljøer til udvikling, test og drift. Vi har ligeledes observeret, at autorisation til at migrere ændringer mellem miljøerne er baseret på funktionsadskillelse.	Ingen væsentlige svagheder noteret.

A.13 Kontrolmål: Der er etableret passende forretningsgange for styring og overvågning af netværk og datakommunikation

Enversion-kontrol	PwC-test	Resultat af test
13.2.4 Fortroligheds- og hemmeligholdelsesaftaler *Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, gennemgås regelmæssigt og dokumenteres.* Enversion har standardiserede kontrakter, der tager højde for fortrolighed og hemmeligholdelse, som benyttes til medarbejdere og visse leverandører.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at der foreligger underskrevne kontrakter for både medarbejdere og leverandører, så organisationens krav til informationssikkerhed opretholdes.	Ingen væsentlige svagheder noteret.

A.14 Kontrolmål: Der er etableret passende forretningsgange og kontroller for anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer

Enversion-kontrol	PwC-test	Resultat af test
14.2.1 Sikker udviklingspolitik *Der bør fastlægges og anvendes regler for udvikling af software i organisationer.* Enversion anvender en scrum-baseret udviklingsmodel, hvor udviklingsopgaverne deles op i mindre dele over en fastlagt periode (to uger). Hver opgave følger "definition of ready" og "definition of done", hvormed alle opgaver er vurderet på kundeværdi, tidsperspektiv, risiko og teststrategi. Der er indbyggede kontroller til sikring af, at alle krav er opfyldt.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har inspiceret, at Enversion har udarbejdet politikker for sikker udvikling.	Ingen væsentlige svagheder noteret.
14.2.2 Procedurer for styring af systemændringer *Ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af formelle procedurer for ændringsstyring.* Enversion anvender en scrum-baseret udviklingsmodel, hvilket medfører, at der foretages mindre ændringer til systemet hele tiden. Dette dokumenteres ved hjælp af beskrivelsen af opgaven i Microsoft Azure, hvor der er fuld sporbarhed. Derudover er der etableret en change management-politik, som benyttes ved større ændringer.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har inspiceret, at der er udarbejdet en politik for change management, samt at der benyttes en scrum-baseret udviklingsmodel. Vi har inspiceret, at ændringer til kaunt dokumenteres i Microsoft Azure.	Ingen væsentlige svagheder noteret.
14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme *Ved ændring at driftsplatforme skal forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.* Ændringer verificeres i udviklingsmiljøet, før det flyttes til produktionsserveren.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at udviklingsopgaver testes, samt at der bliver foretaget et "code review" af koden, inden den flyttes til produktionsmiljøet.	Ingen væsentlige svagheder noteret.
14.2.8 Systemsikkerhedstest *Test af sikkerhedsfunktionalitet skal udføres ved udvikling.* En del af Enversions scrum-baserede udviklingsmodel er at teste systemet. Når alle opgaver oprettes, defineres der også en teststrategi, der skal være gennemført, inden en opgave kan defineres som "done". Desuden udføres der løbende penetreringstests.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at udviklingsopgaver testes, inden de bliver flyttet til produktionsmiljøet og defineres som "done". Vi har ved inspektion observeret, at der er udført skanning og sikkerhedstest af dele af Enversions systemer.	Ingen væsentlige svagheder noteret.

A.14 Kontrolmål: Der er etableret passende forretningsgange og kontroller for anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer

Enversion-kontrol	PwC-test	Resultat af test
14.2.9 Systemgodkendelsestest *Der skal etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.* En del af Enversions scrum-baserede udviklingsmodel er at teste systemet. Når alle opgaver oprettes, defineres der også en teststrategi, der skal være gennemført, inden en opgave kan defineres som "done". Ydermere skal koden valideres og godkendes af en anden part, inden den kan implementeres.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen. Vi har ved inspektion observeret, at udviklingsopgaver testes, samt at der bliver foretaget et "code review" af koden, inden den flyttes til produktionsmiljøet.	Ingen væsentlige svagheder noteret.
14.3.1 Sikring af testdata *Testdata skal udvælges omhyggeligt og skal beskyttes og styres.* Der er fuld sporbarhed på alle data, som benyttes på Enversions test- og produktionsmiljø. Data på Enversions testmaskine er en delmængde af data fra Enversions produktionsmaskine. Der er samme sikring af data på både test- og produktionsmaskinen. Følgende servere udgør henholdsvis test- og produktionsmiljøet: ENV-TEST-SQL02 og ENV-PRO-SQL02. 03-serverne ligger inden for ECIT's beskyttede miljø, og kun specifikke sikkerhedsgrupper kan tilgå maskinerne. Disse maskiner kan kun tilgås af personer i sikkerhedsgruppen SecEnvEconomic.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og observeret, at der, jf. retningslinjerne, er etableret separate miljøer til udvikling, test og drift. Vi har observeret, at adgangen til miljøer ved ECIT styres via sikkerhedsgrupper, og stikprøvevis inspiceret medlemmer af grupper relateret til kaunt.	Ingen væsentlige svagheder noteret.

A.15 Kontrolmål: Der er etableret passende forretningsgange for beskyttelsen af Enversions og Enversions kunders aktiver, som leverandører har adgang til

Enversion-kontrol	PwC-test	Resultat af test
15.1.1 Informationssikkerhedspolitik for leverandørforhold *Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørens adgang til organisationens aktiver bør aftales med leverandøren og dokumenteres.* Enversion har etableret en procedure for vurdering af hver enkelt leverandør i forhold til kravspecifikation og herunder informationssikkerhed. Leverandøren evalueres ud fra et fast skema, og evalueringen sker minimum en gang årligt. Hvis en leverandør har adgang til organisationens aktiver, er det en del af den skriftlige aftale.	Vi har overordnet drøftet leverandørforholdene med ledelsen. Vi har ved stikprøvevis inspektion påset, at aftaler med relevante leverandører indeholder krav til sikkerhed, herunder adgang.	Ingen væsentlige svagheder noteret.
15.2.1 Overvågning og gennemgang af leverandørydelser *Organisationen bør regelmæssigt overvåge, gennemgå og auditere leverandørydelser.* Enversion har etableret en procedure for vurdering af hver enkelt leverandør. Denne vurdering foretages ud fra et fast skema og sker minimum en gang årligt. Desuden har Enversion etableret et system til håndtering af afvigelser. Hvis der opleves afvigelser hos en leverandør, registreres dette i systemet. En del af proceduren for afvigelseshåndtering er at udarbejde en årsagsanalyse og tage stilling til, hvordan afvigelsen skal korrigeres. Enversion følger løbende op på status på backup og incidents.	Vi har overordnet drøftet leverandørforholdene med ledelsen. Vi har ved stikprøvevis inspektion påset, at leverandørydelser overvåges og gennemgås tilstrækkeligt, herunder at relevante erklæringer gennemgås. Vi har observeret, at Enversion har et monitoreringsværktøj til backup, samt at der følges op på incidents.	Ingen væsentlige svagheder noteret.

A.16 Kontrolmål: Der er etableret passende forretningsgange og kontroller for styring af sikkerhedshændelser

Enversion-kontrol	PwC-test	Resultat af test
16.1.1 Ansvar og procedurer *Ledelsesansvar og procedurer skal fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.* Enversion har etableret et system til håndtering af afvigelser. Hvis der opleves en teknisk afvigelse (fx informationssikkerhedsbrud), registreres dette i systemet. En del af proceduren for afvigelseshåndtering er at udarbejde en årsagsanalyse og tage stilling til, hvordan afvigelsen skal korrigeres. Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret hos Enversion. Ved mistanke om informationssikkerhedsbrud, vil information security manageren altid være med inde over årsagsanalysen.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har kontrolleret, at der eksisterer en procedure, der beskriver håndtering af sikkerhedsbrud. Vi har observeret, at proceduren er i anvendelse, og at informationssikkerhedsbrud registreres og håndteres.	Ingen væsentlige svagheder noteret.

A.17 Kontrolmål: Der er etableret passende forretningsgange og kontroller for beredskabsstyring

Enversion-kontrol	PwC-test	Resultat af test
17.1.1 Planlægning af informationssikkerhedskontinuitet *Organisationen skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.* Enversion har taget de nødvendige forholdsregler og etableret beredskabsplaner, hvis en katastrofesituation måtte indtræffe. Beredskabsplanen beskriver etablering af katastrofeorganisationen, herunder lokaler og adgangsforhold, retningslinjer for beredskabsledelsen, beredskabsbemanding, systemlister, reetablering/katastrofedrift, instrukskort for aktiviteter og kommunikation, kontaktlister mv.	Vi har overordnet drøftet de procedurer/kontrolaktiviteter, der udføres, med ledelsen og ved inspektion kontrolleret, at der, jf. retningslinjerne, er udarbejdet en passende business continuity-plan. Vi har ved inspektion observeret, at business continuity-planen testes løbende.	Ingen væsentlige svagheder noteret.