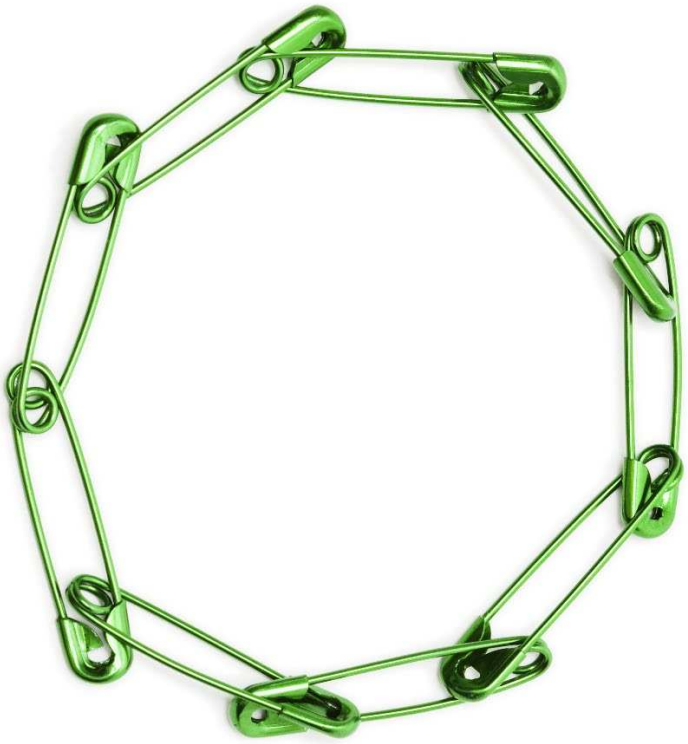
Deloitte.

Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk



Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

RelateIT

Uafhængig revisors ISAE 3402 type 1-erklæring pr. 15. maj 2023 om generelle IT-kontroller relateret til RelateIT's ydelser

Pr. 15. maj 2023

Deloitte Touche Tohmatsu Limited
Deloitte er en betegnelse for et eller flere af Deloitte Touche Tohmatsu Limiteds ("DTTL") medlemsfirmaer, dets netværk af medlemsfirmaer og deres tilknyttede virksomheder (der samlet betegnes "Deloitte-organisationen"). DTTL (der også omtales som "Deloitte Global") og alle dets medlemsfirmaer og tilknyttede virksomheder udgør selvstændige og uafhængige juridiske enheder, som ikke kan forpligte hinanden over for tredjemand. DTTL og de enkelte DTTL-medlemsfirmaer og tilknyttede virksomheder er kun ansvarlige for egne handlinger og/eller udeladelser. DTTL leverer ikke ydelser til kunder. Vi henviser til www.deloitte.com/about for nærmere oplysninger

Indholdsfortegnelse

1. Uafhængig revisors erklæring 1
2. Serviceleverandørs udtalelse 3
3. Serviceleverandørs systembeskrivelse 4
4. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf 9

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3402 type 1-erklæring om generelle IT-kontroller relateret til RelateIT's ydelser

Til ledelsen hos RelateIT, RelateIT's kunder og deres revisorer

Omfang

Vi har fået til opgave at afgive erklæring om RelateIT's beskrivelse i afsnit 3 af generelle IT-kontroller i forbindelse med konsulentydelser pr. 15. maj 2023 og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Erklæringen omfatter de generelle IT-kontroller, som varetages af RelateIT i forbindelse med IT-konsulentydelser.

Enkelte af de kontrolmål, der er anført i RelateIT's beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos RelateIT. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

RelateIT's ansvar

RelateIT er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i afsnit 2, "Serviceleverandørs udtalelse", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for levering af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

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

Deloitte Statsautoriseret Revisionspartnerselskab anvender International Standard on Quality Management (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.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om RelateIT's beskrivelse og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, *Erklæringer med sikkerhed om kontroller hos en serviceleverandør*, som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og implementering. 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. Vores handlinger har omfattet test af udformning og implementering af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2, "Serviceleverandørs udtalelse".

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

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

Begrænsninger i kontroller hos en serviceleverandør

RelateIT'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 systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen.

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 afsnit 2. Det er vores opfattelse,

(a) at beskrivelsen af RelateIT's ydelser og kontrolmiljø, således som det var udformet og implementeret pr. 15. maj 2023, i alle væsentlige henseender er retvisende
(b) at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 15. maj 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater 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 medlemsskoler, der har anvendt RelateIT's ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlig fejlinformation i deres regnskaber.

København, den 7. juli 2023

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

2. Serviceleverandørs udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt RelateIT's ydelser, 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, når de opnår en forståelse af kundernes informationssystemer, som er relevante. RelateIT bekræfter, at:

1. Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af de generelle IT-kontroller i tilknytning til RelateIT's serviceydelser, der er anvendt af kunder pr. 15. maj 2023. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

    a. redegør for, hvordan de generelle IT-kontroller var udformet og implementeret, herunder redegør for:
        i. De typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant
        ii. De processer i både IT- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til brugervirksomhederne
        iii. De tilhørende registreringer og underliggende information, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan information blev overført til de rapporter, der blev udarbejdet til brugervirksomhederne
        iv. Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
        v. Den proces, der blev anvendt til at udarbejde rapporter til brugervirksomhederne
        vi. Relevante kontrolmål og kontroller udformet til at nå disse mål
        vii. Kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementeret af RelateIT's kunder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
        viii. Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for applikationskontrollerne.
    b. indeholder relevante oplysninger om ændringer i de generelle IT-kontroller foretaget pr. 15. maj 2023.
    c. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte kunde måtte anse for vigtigt efter dennes særlige forhold.

2. De kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 15. maj 2023.

Kriterierne for denne udtalelse var, at:

a) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
b) de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

København, den 7. juli 2023

RelateIT A/S

_____	----------
Simon Berthelsen	Carsten Andersen
Managing Director and Partner	Managing Partner

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

3. Serviceleverandørs systembeskrivelse

3.1. Beskrivelse af RelateIT

RelateIT er en af landets største NAV-/Business Central-partnere, som leverer ambitiøse ERP-konsulentydelser til virksomheder med både nationale og internationale udviklingsbehov. RelateIT leverer også løsninger til IT-infrastruktur, som sikrer fremtidig drift og indfrier kravene til moderne IT. RelateIT er en rådgivende virksomhed, der har til formål at levere IT-ydelser til kunder baseret på Microsofts løsninger. RelateIT er en af Danmarks største Microsoft Dynamics 365 Business Central-/NAV-partnere, som leverer ERP-løsninger til virksomheder med både nationale og internationale udviklingsbehov. Derudover leverer RelateIT løsninger indenfor Business Intelligence, Power Automate, e-commerce, web, IT-infrastruktur og IT-sikkerhed, så kunderne får en integreret løsning, der sikrer fremtidig drift og indfrier kravene til moderne IT.

3.2. RelateIT's kerneydelser

RelateIT leverer services relateret primært til rådgivning og assistance til kunden, hvor vi udfører opsætning, migrering, test, udvikling mv. Typerne af aktiviteter vil typisk være følgende:

- Udførelse af tests af udviklede software- eller hardwareløsninger for Kunden
- Analyser og fejlfinding i Kundens IT-systemer
- Migrering af data mellem Kundens IT-systemer.

For at levere ovenstående ydelser og udføre IT-arbejdet eller yde support har de medarbejdere, der arbejder på den enkelte kunde, adgang til kundens platform.

3.3. RelateIT's kontrolmål

Der er i informationssikkerhedspolitikken beskrevet en række kontroller, som skal sikre en høj informationssikkerhed hos RelateIT.

Informationssikkerhedspolitikken kan ikke fraviges af medarbejdere eller samarbejdspartnere uden ansættelsesretlige konsekvenser og/eller ophør af samarbejde, medmindre der undtagelsesvis er givet tilladelse til dette. Informationssikkerhedspolitikken gennemgås og godkendes hvert år.

3.4. Implementerede kontroller

Der er implementeret kontroller med henblik på at kvalitetssikre og dokumentere RelateIT's ydelser. Alle kontroller, hvad enten de relaterer sig til en processuel eller teknisk handling, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender.

Kontrollerne er baseret på rammeværket ISO 27002 og omfatter følgende områder (til inspiration)

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved ned-, beredskabs- og reetablering
- Overensstemmelse (overholdelse af aftaler).

3.5. Implementerede kontroller

Der er udarbejdet en Informationssikkerhedspolitik med tilhørende underpolitikker, der er gældende for alle medarbejdere og samarbejdspartnere. De udarbejdede politikker er:

- IT Security Policy med følgende underpolitikker
    - Backup Policy
    - Account Management & Access Control Policy

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

- Awareness Policy
- Cryptography Policy
- Password Policy
- Physical Security Policy
- Policy for Maintenance, Repair, Disposal and re-use of Hardware
- Shadow IT Policy

- Andre informationssikkerhedsplaner og procedurer
  - Business Continuity Plan
  - Attack Classifications
  - Patch Management Procedure
  - Security Incident Management process.

3.6. Informationssikkerhedspolitikker

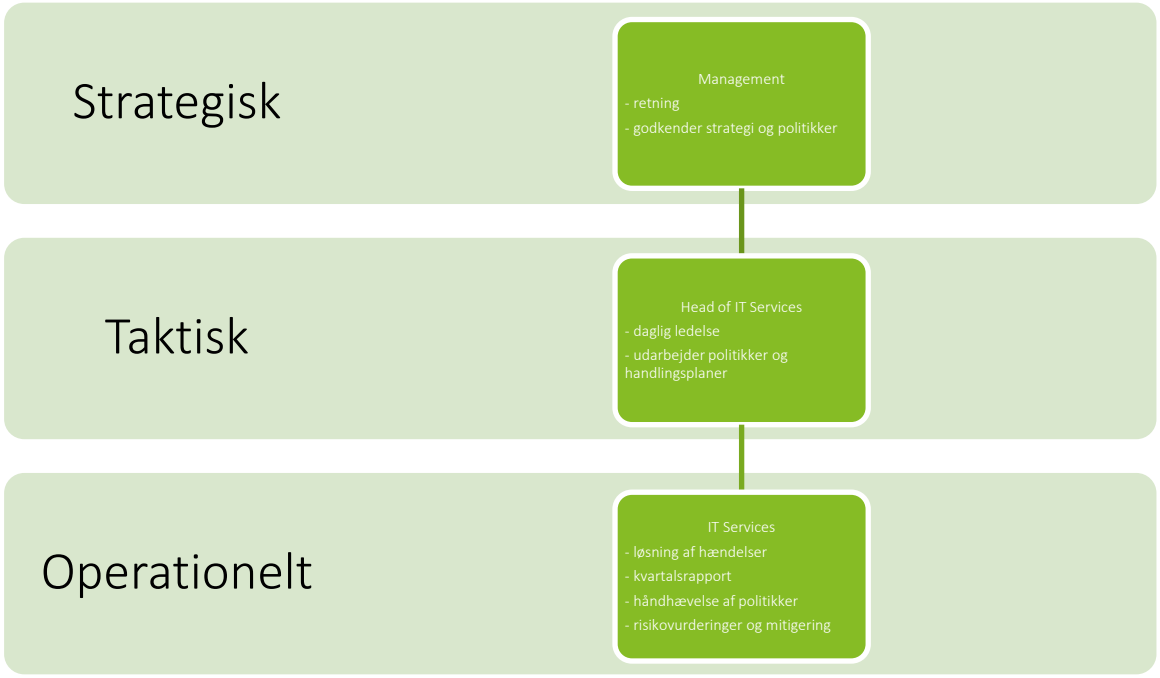
Informationssikkerhedspolitikkerne udarbejdes af IT Services med Head of IT som ansvarlig, og medarbejderne får ved ansættelse udleveret information om IT-sikkerhed. Politikkerne revideres som minimum årligt og godkendes af koncernledelsen.
Det overordnede ansvar for informationssikkerhed ligger hos koncernledelsen. Herfra udstikkes overordnede instrukser.

Den daglige ledelse af informationssikkerhedsarbejdet varetages af Head of IT Services. Overordnede instrukser omsættes til konkrete handlingsplaner og politikker, som godkendes af koncernledelsen. Prioritering af handlingsplan og konkrete opgaver.

IT Services har det generelle ansvar for procedurer og processer i forbindelse med informationssikkerhed. Eksempelvis:

- Løsning af IT-sikkerhedshændelser
- Kvartalsvis IT-sikkerhedsrapport til koncernledelsen
- Data Loss Prevention
- Håndhævelse af informationssikkerhedspolitikker
- Risikovurderinger og udarbejdelse af mitigerende tiltag

IT Services har ligeledes til opgave at sikre en prioritering og operationalisering af de opgaver, som ligger i årshjul for informationssikkerhed, samt varetage de decentrale informationssikkerhedsproblematikker.



3.7. Informationssikkerhedspolitikker

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

Der er faste procedurer for ansættelse, omrokering og afskedigelse af medarbejdere. HR foretager sammen med lokationscheferne ansættelser og afskedigelser. Medarbejdere instrueres i Informationssikkerhedspolitikken, retningslinjer for informationssikkerhed, håndtering af personoplysninger, jf. GDPR, håndtering af fortrolige oplysninger og fortrolighed i forbindelse med ansættelse og undervejs i dedikerede awareness-tiltag. Ved ansættelsesophør gøres medarbejdere opmærksomme på fortsat fortrolighedsbinding.

3.8. Styring af aktiver

IT-udstyr håndteres af IT-Services, der håndterer lister over alle aktiver. Herudover er services, programmel og data nedfældet, og alle aktiver har udpeget en ejer.

Der forefindes procedurer for returnering af udstyr i forbindelse med udskiftning eller ophør af ansættelse, og bortskaffelse af udstyr sker på forsvarlig vis.

3.9. Adgangsstyring

Der er etableret processer for tildeling af systemroller og rettigheder ved ansættelse baseret på medarbejderens rolle. Der er ligeledes etableret processer, der sikrer, at alle autorisationer fratages medarbejderen ved afskedigelse.

Hvis der er behov for adgang til data eller systemer, som ikke er beskrevet i rollen, tildeles dette efter princippet om mindste niveau af adgang i forhold til behov og fordrer godkendelse, afhængigt af niveau.

Hvis en medarbejder skifter rolle, skiftes de rollebaserede adgange også, således at medarbejderen fratages rettigheder på den gamle rolle, samtidig med at der tildeles rettigheder passende til den nye rolle. Privilegerede ad hoc-adgange sikres ved periodisk gennemgang af adgange. Perioden afhænger af typen af adgang.

For at få adgang til kunders lokale systemer skal der etableres adgang via VPN, hvis den pågældende medarbejder ikke er på RelateIT's kontor. For adgang til Cloud-systemer (såvel egne som kunders) fordres Multi-fator Authentication, hvis der ikke arbejdes på RelateIT's kontor.

3.10. Kryptografi

Kryptering af data, mens de er gemt, giver effektiv beskyttelse mod uautoriseret adgang og tyveri. Kryptering bruges til at beskytte RelateIT's digitale data i hvile.

Alle virksomhedsejede enheder og lagersystemer har fuld diskkryptering aktiveret, og hvor det er muligt, skal overvågning være på plads for at sikre, at dette fortsat er aktiveret og effektivt.

Kryptering af data under transit giver effektiv beskyttelse mod uautoriseret aflytning og adgang. Kryptering bruges til at beskytte RelateIT's digitale data i transit.

Kryptering implementeres ved hjælp af godkendte metoder og teknologier. Krypteringsstandarder, algoritmer, protokoller, nøglelængde, og krypteringspakker opfylder de nuværende acceptable standarder. Systemer, infrastruktur, applikationer og tjenester skal konfigureres til kun at acceptere forbindelser, der overholder dette krav.

Krypteringsalgoritmer og specifikke implementeringer af algoritmer kan indeholde sårbarheder. Brugen af algoritmer og krypteringssoftware overvåges og styres gennem sårbarhedshåndteringsprocessen.

3.11. Fysisk sikring og miljøsikring

Servere og infrastruktur er placeret hos eksterne hosting-partnere, som kontrolleres årligt.
Det er kun muligt at tilgå kontorlokaler i åbningstiden, mens adgang kræver nøgle eller kort, afhængigt af lokation.
Regler for adgang til virksomhedens lokaler er i øvrigt beskrevet i retningslinjer for informationssikkerhed.

Medarbejderne er instrueret i at holde deres skrivebord i virksomhedens lokaler ryddeligt.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

3.12. Driftssikkerhed

RelateIT har dokumenterede driftsprocedurer, som er tilgængelige for alle brugere, der har brug for dem. Der er etableret en Change Management-proces, således at standardiserede metoder og procedurer anvendes til effektiv og hurtig håndtering af alle ændringer for at minimere indvirkningen af ændringsrelaterede hændelser på servicekvaliteten. Enhver foreslået ændring skal gennem Change Management-processen

Drift og opdatering af infrastruktur foregår ligeledes jævnligt og ensartet med digital understøttelse for at sikre udførelse og dokumentation.

Ændringer i miljøer testes så vidt muligt i et dedikeret testmiljø, før det implementeres i produktionsmiljøet.

Backup foretages efter gældende politik, afhængigt af system.

Servere og computere opdateres løbende med opdateringer til beskyttelse mod malware, og der foretages løbende overvågning af systemernes tilgængelighed og logs.

Der er implementeret procedurer for hændelseslogning til sikring af registrering af brugeraktiviteter, undtagelser og fejl, og informationssikkerhedshændelser registreres og opbevares.

Der er etableret procedurer for opdatering af operativsystemer og software, og der er etableret kontroller, der sikrer foranstaltninger mod kendte trusler og sårbarheder.

3.13. Kommunikationssikkerhed

Al kommunikation til åbne, offentlige netværk sker via firewalls driftet af RelateIT og en samarbejdspartner.

Der er etableret en Zero Trust-arkitektur, hvor det vigtigste er at passe på de enheder, der er på netværket og internettet.

Netværkene er opdelt, så gæster og ikke-styrede enheder ikke blandes med firmaets styrede enheder.

Der er etableret markedsstandardfirewallregler for at forhindre medarbejderne i at tilgå kendte ondsindede domæner. Denne kontrol findes også direkte på medarbejdernes computere, så dette også sikres udenfor kontoret.

3.14. Leverandørforhold

Der er udarbejdet en liste over alle eksterne leverandører, og der følges op på de leverede ydelser – både økonomisk og sikkerhedsmæssigt.

Der er indgået en række databehandleraftaler med alle underleverandører, der enten behandler, indsamler eller videresender personlige oplysninger.

RelateIT vedligeholder løbende en oversigt over anvendte underleverandører. RelateIT sikrer, at der er indgået underdatabehandleraftaler med underdatabehandlere, og at underdatabehandlere underlægges de samme tekniske sikringsforanstaltninger som RelateIT. Endvidere udføres der løbende kontrol med underleverandører. Gennemgangen af databehandleraftaler og underdatabehandlere udføres mindst én gang årligt.

3.15. Styring af sikkerhedsbrud

Der er udarbejdet en proces for håndtering af sikkerhedsbrud i RelateIT. Sikkerhedsbrud er brud på persondatasikkerhed og udnyttelse af sårbarheder på enheder eller servere. Det fremgår tillige af databehandleraftaler, at databehandlere skal bistå dataansvarlige i forbindelse med sikkerhedsbrud.

Der er udarbejdet en Business Continuity Policy med beredskabsplan for forretningsrelaterede emner samt for IT-systemer (systembreakdown), procedure for genetablering af væsentlige systemer samt procedure for genetablering af medarbejdernes evne til at udføre arbejde ved manglende adgang til netværk på virksomhedens faciliteter. Dette således, at det påvirker forretningen, kunderne og forsikringstagere mindst muligt.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

3.16. Overensstemmelse (overholdelse af aftaler)

Alle vores aftaler er reguleret og indeholder krav om fortrolighed. Der indhentes revisorerklæringer på væsentlige områder, fx ISAE 3000 vedrørende overholdelse af EU GDPR, ISAE 3402 vedrørende generelle IT-kontroller.

Der er udarbejdet et årshjul, der oplister tidspunkter for væsentlige opgaver for IT-compliance-aktiviteter og kontroller.

3.17. Komplementerende kontroller hos kunderne

For at kontrolmålene i erklæringen kan nås, er det vigtigt, at kunderne udfører de opgaver, som de er ansvarlige for. Det drejer sig om:

- **Opsætning af infrastruktur**

For at sikre stabil og sikker afvikling af applikationen er det vigtigt, at infrastrukturen er sat korrekt op og løbende vedligeholdes og patches.

- **Overvågning af servere og infrastruktur**

Kunderne er ansvarlige for driftsovervågning af deres infrastruktur. Dette indebærer, at der reageres rettidigt og iværksættes mitigerende tiltag, såfremt driftsovervågningen afslører udfordringer med infrastruktur, servere og/eller applikationerne.

- **Brugerstyring**

Kunderne er ansvarlige for tildeling af brugerrettigheder på alle servere, herunder den valgte løsning til sikker adgang til serverne for eksterne konsulenter.

- **Test i forbindelse med ny og ændret funktionalitet**

Det er kundernes ansvar, at der bliver defineret og foretaget passende tests af nye ændringer, før disse bliver released til produktion.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

4. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf

4.1. Introduktion

Denne erklæring er udformet med henblik på at informere RelateIT's kunder om RelateIT's systemer og kontroller, som kan påvirke behandlingen af data, og samtidig informere om udvalgte kontroller, vi har efterprøvet, og resultatet af vores handlinger. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i kundernes forretningsprocesser, har til hensigt at hjælpe kundernes revisor med at vurdere risici for fejl, som muligvis påvirkes af kontroller hos RelateIT.

Vores test af RelateIT's kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle IT-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene. Det er hver brugerorganisations revisors ansvar at evaluere denne information i forhold til de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan RelateIT's kontroller muligvis ikke kompensere for sådanne svagheder.

4.2. Test af kontroller

De udførte test i forbindelse med fastlæggelsen af kontrollers funktionalitet består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos RelateIT
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3. Test af udformning og implementering

Vores test af kontrollernes udformning og implementering inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelig til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået pr. 15. maj 2023.

4.4. Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
5.1 Sikkerhedspolitik **Kontrolmål: At levere midler til styring af og støtte for IT-sikkerhed i overensstemmelse med forretningens krav og med relevante bestemmelser.**				
5.1.1	Informationssikker-hedspolitik	Ledelsen fastlægger og godkender politikker for IT-sikkerhed, som offentliggøres og kommunikeres til medarbejdere og relevante kontrahenter.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt. Deloitte har inspiceret, at der er udarbejdet følgende relevante politikker relateret til informationssikkerhed: • Account Management & Access Control • Awareness policy • Password policy • Policy for maintenance, repair, disposal and re-use of hardware • Shadow IT policy. Deloitte har inspiceret relevant dokumentation, hvoraf det fremgår, at informationssikkerhedspolitikkerne er kommunikeret til medarbejdere.	Ingen afvigelser konstateret.
5.1.2	Evaluering af informationssikker-hedspolitikken	IT-sikkerhedspolitikken evalueres årligt eller i tilfælde af væsentlige ændringer for at sikre dens fortsatte egnethed og tilstrækkelighed.	Deloitte har forespurgt udvalgt personale hos RelateIT om kontrollen. Deloitte har inspiceret IT-sikkerhedspolitikken og observeret, at denne er godkendt af ledelsen i februar 2023.	Ingen afvigelser konstateret.
6.1 Intern organisering **Kontrolmål: At styre IT-sikkerheden internt i organisationen.**				
6.1.1	Roller og ansvarsområder for informationssikker-hed	Alle ansvarsområder for IT-sikkerheden er klart defineret og fordelt.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret 'IT-strategi' og observeret, at der er beskrevet de overordnede rammer for anvendelse og styring af IT. Deloitte har inspiceret relevant dokumentation, hvori intern organisering er beskrevet.	Det er konstateret, at der ikke foreligger en særskilt IT-sikkerhedsstrategi. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
			Deloitte har foretaget interview af én medarbejder og verificeret, at medarbejderens beskrivelser er i overensstemmelse med beskrivelsen af de faktiske roller og ansvarsområder.	
6.1.2	Funktionsadskillelse	Der er etableret funktionsadskillelse via rettighedsstyring.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret dokumentation for adgangsstyring, hvori funktionsadskillelse via rettighedsstyring er beskrevet. Deloitte har inspiceret relevant dokumentation og observeret, at der er et overblik over, hvilke adgangsrettigheder der tildeles medarbejdere med forskellige jobfunktioner.	Ingen afvigelser konstateret.
6.1.5	Informationssikker-hed ved projektstyring	Der udarbejdes kvartalsvise rapporter med status til ledelsen.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret relevant dokumentation for én stikprøve vedrørende kvartalsvis sikkerhedsrapportering til ledelsen og observeret, at den bl.a. omfatter status vedrørende IT-sikkerhed, informationssikkerhedshændelser og evt. fremtidige initiativer.	Ingen afvigelser konstateret.
6.2 Mobilt udstyr og fjernarbejdspladser **Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.**				
6.2.1	Politik for mobilt udstyr	Der er udarbejdet politik relateret til anvendelse af mobilt udstyr. Der er etableret sikkerhedsforanstaltninger relateret til anvendelse af mobilt udstyr.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret politikken relateret til anvendelse af mobilt udstyr og observeret, at politikken er godkendt af ledelsen i februar 2023. Deloitte har stikprøvevis inspiceret relevant dokumentation og observeret, at der er etableret tekniske sikkerhedsforanstaltninger relateret til anvendelse af mobilt udstyr.	Ingen afvigelser konstateret.
6.2.2	Fjernarbejdspladser	Der er udarbejdet politik relateret til anvendelse af fjernarbejdspladser. Der er etableret sikkerhedsforanstaltninger relateret til anvendelse af fjernarbejdspladser, herunder krav ang. MFA og VPN.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret politikken relateret til anvendelse af mobilt udstyr og observeret, at politikken er godkendt af ledelsen i februar 2023.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
			Deloitte har stikprøvevis inspiceret relevant dokumentation og observeret, at der er etableret sikkerhedsforanstaltninger relateret til fjernearbejdspladser. Deloitte har stikprøvevis inspiceret relevant dokumentation for indstillinger for VPN og MFA.	
7.1 Før ansættelsen **Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.**				
7.1.1	Screening	Der foretages screening af alle jobkandidater før ansættelsen. Kandidatens CV og referencer indhentes, og der udføres en profiltest.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har for én stikprøve på en nyansat medarbejder forespurgt om processen for efterprøvning i forbindelse med ansættelse og har fået oplyst, at der blev indhentet referencer fra tidligere ansættelser samt straffeattest. Deloitte har endvidere fået oplyst, at der ikke opbevares dokumentation for referencer og straffeattest.	Ingen afvigelser konstateret.
7.1.2	Ansættelsesvilkår og -betingelser	Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og RelateIT's ansvar for IT-sikkerhed.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har ved én stikprøve på en nyansat medarbejder inspiceret ansættelseskontrakt og observeret, at den pågældende medarbejder har underskrevet en fortrolighedsaftale. Deloitte har for én stikprøve på en nyansat medarbejder inspiceret relevant dokumentation og observeret, at den pågældende medarbejder er blevet introduceret til: • Medarbejderhåndbogen • Intro til Team Infrastruktur.	Ingen afvigelser konstateret.
7.2 Under ansættelsen **Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.**				
7.2.2	Bevidsthed om uddannelse og træning i informationssikker-hed	Alle medarbejdere skal gennemføre awareness-træning.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedure for awareness-træning samt relevant dokumentation, hvoraf det fremgår, at der udbydes awareness-træning til alle medarbejdere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
7.3 Ansættelsesforholdets ophør eller ændring **Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.**				
7.3.1	Ansættelsesforholdets ophør eller ændring	Ved fratrædelse gøres medarbejdere opmærksomme på fortsat tavshedspligt. Herudover modtager afgående medarbejdere et brev indeholdende diverse formalia, herunder fortsat tavsheds- og loyalitetsforpligtigelse.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret 'Medarbejderhåndbogen' og observeret, at der er beskrevet krav relateret til opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret relevant dokumentation og observeret, at medarbejderen blev gjort opmærksom på krav angående opretholdelse af fortrolighedsaftale, herunder fortsat tavsheds- og loyalitetsforpligtigelse.	Ingen afvigelser konstateret.
8.1 Ansvar for aktiver **Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.**				
8.1.1	Fortegnelse over aktiver	Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres. Der er udarbejdet en samlet fortegnelse over alle aktiver, som vedligeholdes.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har forespurgt om procedure for styring af aktiver. Deloitte har inspiceret relevant dokumentation og observeret, at aktiver er identificeret i følgende applikationer: • Microsoft Intune, hvor der sker registrering af fysisk udstyr, dvs. bærbare computere, servere m.m. Hver enhed har tildelt en ejer. • FortiCloud, hvor der sker en registrering af netværksudstyr, herunder servere, klienter og switches. Deloitte har forespurgt om en samlet fortegnelse over alle aktiver samt procedure for vedligeholdelse af fortegnelsen.	Det er konstateret, at der ikke er en samlet fortegnelse over alle aktiver. Deloitte har fået oplyst, at på revisionstidspunktet er arbejdet vedrørende udarbejdelse af en samlet fortegnelse over alle aktiver igangsæt. Ingen yderligere afvigelser konstateret.
8.1.2	Ejerskab af aktiver	Der er udpeget en ejer for hvert aktiv.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret relevant dokumentation og observeret, at aktiver er identificeret i følgende applikationer hhv. Microsoft Intune og FortiCloud. Deloitte har forespurgt, om RelateIT har dokumenteret ejerskab for hvert aktiv.	Det er konstateret, at der ikke er dokumenteret ejerskab for alle aktiver, herunder netværksudstyr og servere. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
8.1.4	Tilbagelevering af aktiver	Aktiver returneres ved ophør af ansættelse, kontrakt med eksterne eller når aftaler med kunder ophører. Medarbejdere får en rekvisition med angivet udstyr, som kvitteres for, når udstyret er afleveret.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer for tilbagelevering af aktiver ved ophør af ansættelse, kontrakt med eksterne, eller når aftaler med kunder ophører. Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret, at aktiver er inddraget.	Ingen afvigelser konstateret.
8.2 Klassifikation af information **Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.**				
8.2.1	Klassifikation af information	RelateIT har implementeret politik relateret til klassificering af information.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har forespurgt, om RelateIT har udarbejdet og implementeret politik og procedurer for klassificering af information og har fået oplyst, at information klassificeres baseret på Microsoft anbefalinger og håndteres på baggrund heraf.	Ingen afvigelser konstateret.
8.3 Mediehåndtering **Kontrolmål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.**				
8.3.1	Styring af bærbare enheder	Der er udarbejdet en politik for styring og bortskaffelse af medier.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret de udarbejdede politikker og procedurer for styring og bortskaffelse af bærbare enheder.	Ingen afvigelser konstateret.
8.3.2	Bortskaffelse af medier	Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer udarbejdet af RelateIT for bortskaffelse af udstyr. Deloitte har forespurgt om bortskaffelse af media og har fået oplyst, at der på revisionstidspunktet ikke har været bortskaffelse af media.	Ingen afvigelser konstateret.
9.1 Forretningsmæssige krav til adgangsstyring **Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.**				
9.1.1	Politik for adgangsstyring	RelateIT har defineret politikken for adgangsstyring, der er beskrevet i den til enhver tid gældende sikkerhedspolitik.	Deloitte har forespurgt udvalgt personale om kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
			Deloitte har inspiceret politikken for adgangsstyring og observeret, at bl.a. proceduren for brugergennemgang er beskrevet, og at brugerens begrænsninger beskrives.	
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.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedure relateret til sikring af, at brugere kun har adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte. Deloitte har inspiceret den etablerede rolle-/rettighedsmatrix og observeret, at den giver et overblik over, hvilke adgangsrettigheder der tildeles medarbejdere med forskellige jobfunktioner. Vi har ved én stikprøve på en medarbejder inspiceret relevant dokumentation og observeret, at brugeren har fået tildelt adgang efter et arbejdsbetinget behov.	Ingen afvigelser konstateret.
9.2 Administration af brugeradgang **Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.**				
9.2.1	Brugerregistrering og -afmelding	RelateIT har implementeret formelle procedurer for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder. Deloitte har ved én stikprøve på en nyansat medarbejder inspiceret relevant dokumentation for, at registrering af bruger har fulgt de fastsatte procedurer. Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret relevant dokumentation for, at adgangsrettigheder er inaktiveret.	Ingen afvigelser konstateret.
9.2.2	Tildeling af brugeradgang	RelateIT har implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedure for tildeling af brugeradgang.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
			Deloitte har ved én stikprøve på en tildeling af nye adgangsrettigheder inspiceret, at den blev udført i overensstemmelse med udarbejdede procedurer.	
9.2.3	Styring af privilegerede adgangsrettigheder	Tildeling og brug af privilegerede adgangsrettigheder er begrænset og kontrolleres.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret proceduren for tildeling og brug af privilegerede adgangsrettigheder. Deloitte har inspiceret et udtræk af brugere med tildelte privilegerede adgangsrettigheder på Azure Active Directory-niveau. Deloitte har på forespørgsel fået oplyst, at privilegerede adgangsrettigheder kun er tildelt medarbejdere med et arbejdsbetinget behov.	Ingen afvigelser konstateret.
9.2.5	Gennemgang af brugeradgangs-rettigheder	Brugernes adgangsrettigheder gennemgås med jævne mellemrum.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har forespurgt om proceduren for gennemgang af brugernes adgangsrettigheder. Deloitte har for en stikprøve inspiceret relevant dokumentation for den senest udførte brugergennemgang af brugernes adgangsrettigheder.	Det er konstateret, at en formel, skriftlig procedure for gennemgang af brugernes adgangsrettigheder ikke er færdigudarbejdet. Ingen yderligere afvigelser konstateret.
9.2.6	Inddragelse eller justering af adgangsrettigheder	Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører eller tilpasses efter en ændring.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer for inddragelse eller justering af adgangsrettigheder. Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret relevant dokumentation for, at nedlæggelse af brugeradgange og rettigheder er sket uden unødigt ophold.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
9.4 Styring af system- og applikationsadgang **Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.**				
9.4.1	Begrænset adgang til informationer	RelateIT har en politik for adgangsstyring samt etableret en rolle-/rettighedsmatrix, der angiver, hvilke rettigheder der følger med hvilke roller i organisationen.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedure for adgangsstyring. Deloitte har inspiceret den etablerede rolle-/rettighedsmatrix og observeret, at den giver et overblik over, hvilke adgangsrettigheder der tildeles medarbejdere med forskellige jobfunktioner. Deloitte har inspiceret relevant dokumentation, hvoraf opsætning af én dynamisk gruppe i Azure Active Directory fremgår, og har fået bekræftet, at medarbejderne kun får tildelt adgange, som svarer til medarbejderens arbejdsbetingende behov.	Ingen afvigelser konstateret.
9.4.2	Procedurer for sikker logon	Adgang til systemer og applikationer styres af en procedure for sikker logon.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer for sikker logon hos RelateIT. Deloitte har inspiceret relevant dokumentation, hvoraf opsætning for sikker logon indstillinger fremgår.	Ingen afvigelser konstateret.
9.4.3	System for administration af adgangskoder	Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet.	Deloitte har forespurgt udvalgt personale om kontrollen. Vi har inspiceret passwordpolitikken og observeret, at der er defineret krav til password. Deloitte har inspiceret relevant dokumentation, hvoraf det fremgår, at Azure AD-passwordkrav følges.	Ingen afvigelser konstateret.
9.4.5	Styring af adgang til kildekoder til programmer	Adgang til kildekoder til programmer er begrænset.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har stikprøvevist inspiceret relevant dokumentation for, hvorvidt brugere med adgang til kildekode er begrænset. Deloitte har indhentet bekræftelse på, at brugerne har et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
10.1 Kryptografiske kontroller **Kontrolmål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**				
10.1.1	Politik for anvendelse af kryptografi	Der er udarbejdet en politik for anvendelse af kryptografi til beskyttelse af information. Data ved opbevaring og/eller overførsel er krypteret.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret politikken for kryptering. Deloitte har stikprøvevis inspiceret relevant dokumentation relateret til anvendelse af krypteringsalgoritmer. Deloitte har ved udtagelse af én stikprøve inspiceret relevant dokumentation og observeret, at data ved opbevaring og/eller overførsel er krypteret.	Ingen afvigelser konstateret.
11.1 Sikre områder **Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.**				
11.1.1	Fysisk perimetersikring	Der er implementeret fysisk sikring af kontorer, lokaler og faciliteter i RelateIT.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret 'Medarbejderhåndbogen' og observeret, at der er beskrevet procedurer for adgang til kontorer og lokaler. Deloitte har i forbindelse med revisionen observeret, at der er etableret sikkerhedsforanstaltninger, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til kontorer og lokaler hos RelateIT.	Ingen afvigelser konstateret.
11.2 Udstyr **Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.**				
11.2.9	Politik for ryddeligt skriveborg og blank skærm	RelateIT har implementeret en politik om ryddelige skriveborde, anvendelse af flytbare lagringsmedier og blank skærm.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret en politik relateret til et ryddeligt skrivebord, anvendelse af flytbare lagringsmedier og blank skærm.	Ingen afvigelser konstateret.
12.1 Driftsprocedurer og ansvarsområder **Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.**				
12.1.1	Dokumenterede driftsprocedurer	RelateIT har udarbejdet driftsprocedurer, som er tilgængelige for alle brugere.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at driftsprocedurer foreligger på RelateIT's intranet og er tilgængelige for alle medarbejdere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
12.1.2	Ændringsstyring	RelateIT har implementeret procedurer, som sikrer, at ændringer af informationsbehandlingsfaciliteter og -systemer, som påvirker IT-sikkerheden, styres.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret skriftlige procedurer for håndtering af ændringer. Deloitte har ved én stikprøve på en foretaget ændring inspiceret dokumentation for, at formelle procedurer følges ved implementering af ændringen.	Ingen afvigelser konstateret.
12.1.3	Kapacitetsstyring	Der anvendes Azure Monitor til kapacitetsstyring.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret relevant dokumentation, hvoraf de opsatte parametre for overvågning i Azure Monitor fremgår.	Ingen afvigelser konstateret.
12.1.4	Adskillelse af udviklings-, test- og driftsmiljøer	Der er implementeret adskillelse mellem udviklings-, test- og driftsmiljøer.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer for beskyttelse af informationer i det testmiljø, der anvendes til test/udvikling. Deloitte har stikprøvevis inspiceret relevant dokumentation og observeret, at der er etableret separate miljøer til udvikling, test og drift.	Ingen afvigelser konstateret.
12.2 Beskyttelse mod malware **Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.**				
12.2.1	Kontroller mod malware	RelateIT har implementeret procedurer til detektering og forhindring af samt beskyttelse mod malware.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedurer til detektering og forhindring af samt beskyttelse mod malware. Deloitte har inspiceret relevant dokumentation, hvoraf en oversigt over aktive klienter fremgår, og at antivirus er installeret.	Deloitte har fået oplyst, at RelateIT siden februar 2023 har været i gang med at udskifte antivirusløsningen fra Cylance til Microsoft Defender. Ingen yderligere afvigelser konstateret.
12.3 Backup **Kontrolmål: At beskytte mod tab af data.**				
12.3.1	Backup af information	Der tages backupkopier af databaser, software og filer.	Deloitte har forespurgt udvalgt personale om kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
		Der foretages regelmæssigt restoretest.	Deloitte har inspiceret politikken for backup. Deloitte har inspiceret relevant dokumentation, hvoraf konfiguration af opsætning af backup fremgår. Deloitte har inspiceret relevant dokumentation for udførte backup-jobs. Deloitte har ved én stikprøve på et backupjob inspiceret dokumentation for, at backup blev udført uden fejl. Deloitte har inspiceret relevant dokumentation for opfølgning på månedlig backuprestoretesttjek.	
12.4 Logning og overvågning **Målsætning: At registrere hændelser og tilvejebringe bevis.**				
12.4.1	Hændelseslogning	RelateIT har implementeret procedurer for hændelseslogning til sikring af registrering af brugeraktiviteter, undtagelser og fejl, og informationssikkerhedshændelser registreres og opbevares.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret politikken for logning og observeret, at der er beskrevet opsatte logmekanismer og procedurer vedrørende sikkerhedslogning generelt. Deloitte har stikprøvevis inspiceret relevant dokumentation, hvoraf følgende fremgår: • opsætte indstillinger for logning • servere opsat til logning af Azure Monitor • overvågning og logning af hændelser i Microsoft Defender.	Ingen afvigelser konstateret.
12.4.2	Beskyttelse af logoplysninger	RelateIT's logfaciliteter og logoplysninger er beskyttet mod manipulation og uautoriseret adgang.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret politikken for logning og observeret, at der er beskrevet procedurer rettet mod manipulation og uautoriseret adgang til logs. Deloitte har inspiceret et udtræk over brugere med adgang til logoplysninger og har på forespørgsel fået bekræftet, at brugerne har et arbejdsbetinget behov.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
12.5 Styring af driftssoftware **Kontrolmål: At sikre integriteten af driftssystemer.**				
12.5.1	Softwareinstallation på driftssoftware	RelateIT har implementeret procedurer til styring af softwareinstallation på driftssystemer.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret procedure til styring af softwareinstallationer på driftssystemer. Deloitte har stikprøvevis inspiceret relevant dokumentation, som viser status for løbende softwareopdatering på RelateIT's enheder. Deloitte har inspiceret relevant dokumentation for, at der foretages løbende patching af RelateIT's enheder for udvalgte stikprøver.	Ingen afvigelser konstateret.
12.6 Styring af tekniske sårbarheder **Målsætning: At forhindre, at tekniske sårbarheder udnyttes.**				
12.6.1	Styring af tekniske sårbarheder	RelateIT indhenter løbende informationer om tekniske sårbarheder i anvendte informationssystemer, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har stikprøvevis inspiceret relevant dokumentation, hvoraf opsætning af Microsoft Defender for udførelse af løbende scanninger fremgår. Deloitte har stikprøvevis inspiceret relevant dokumentation for regelmæssig opfølgning på status relateret til tekniske sårbarheder.	Ingen afvigelser konstateret.
12.6.2	Begrænsninger på softwareinstallation	RelateIT har opsat regler for softwareinstallation, som styres via opsatte virksomhedspolitikker og blacklisting af software og hjemmesider.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret relevante politikker og procedurer og observeret, at der er beskrevet regler for softwareinstallation. Deloitte har inspiceret en liste, hvoraf ikke-godkendt software fremgår. Deloitte har på forespørgsel fået oplyst, at listen over ikke-godkendt software vedligeholdes i Endpoint Central.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
13.1 Styring af netværkssikkerhed **Målsætning: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.**				
13.1.1	Netværksstyring	RelateIT's netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har stikprøvevis inspiceret relevant dokumentation for det overordnede netværk. Deloitte har stikprøvevis inspiceret relevant dokumentation relateret til de etablerede firewallregler samt opsætning for overvågning af netværket.	Ingen afvigelser konstateret.
13.1.3	Opdeling af netværk	RelateIT's netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har stikprøvevis inspiceret relevant dokumentation og observeret, at netværk er segmenteret, herunder at netværket er opdelt til private og offentlige netværk i hvert af RelateIT's kontorer.	Ingen afvigelser konstateret.
13.1 Styring af netværkssikkerhed **Målsætning: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.**				
13.2.1	Politikker og procedurer for informations-overførsel	RelateIT har implementeret formelle procedurer for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret proceduren for kryptering og proceduren for sikker e-mail. Deloitte har stikprøvevis inspiceret relevant dokumentation relateret til anvendelse af krypteringsalgoritmer. Deloitte har ved udtagelse af én stikprøve inspiceret relevant dokumentation og observeret, at data ved opbevaring og/eller overførsel er krypteret.	Ingen afvigelser konstateret.
15.1 Informationssikkerhed i leverandørforhold **Kontrolmål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.**				
15.1	Informationssikker-hedspolitik for leverandørforhold	Alle adgangsberettigede kontrahenter med adgang til RelateIT's systemer, informationer og bygninger skal gøres bevidste om de relevante dele af RelateIT's informationssikkerhedspolitik og	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har på forespørgsel fået oplyst, at informationssikkerhedskravene til at minimere risici forbundet med	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
		underliggende politikker forud for etablering af den fornødne adgang.	leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres i samarbejdsaftaler. Deloitte har inspiceret et bilag til samarbejdsaftalen mellem RelateIT og IT Relations og observeret, at den beskriver kravene om de tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det aftalte sikkerhedsniveau.	
15.2 Styring af leverandørydelser **Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.**				
15.2.1	Overvågning og gennemgang af leverandørydelser	RelateIT monitorerer eksterne leverandører ved gennemgang af revisionserklæringer, tilsyn og møder.	Deloitte har forespurgt ansvarlige RelateIT-medarbejdere om kontrollen. Deloitte har forespurgt, om RelateIT har indhentet og gennemgået relevant rapportering fra leverandøren IT Relations og har vurderet indhold og konklusion.	Deloitte har ikke modtaget dokumentation for, at RelateIT har indhentet og gennemgået relevant rapportering fra leverandøren IT Relations og har vurderet indhold og konklusion. Ingen yderligere afvigelser konstateret.
16.1 Styring af informationssikkerhedsbrud og forbedringer **Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.**				
16.1.1	Ansvar og procedurer	Ledelsesansvar og procedurer er fastlagt for at sikre en hurtigt, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Deloitte har forespurgt ansvarlige RelateIT-medarbejdere om kontrollen. Deloitte har inspiceret proceduren for håndtering af informationssikkerhedsbrud og informationssikkerhedshændelser.	Ingen afvigelser konstateret.
16.1.2	Rapportering af informationssikker-hedshændelser	Informationssikkerhedshændelser skal rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Deloitte har forespurgt ansvarlige RelateIT-medarbejdere om kontrollen. Deloitte har inspiceret proceduren for håndtering af informationssikkerhedsbrud og informationssikkerhedshændelser. Deloitte har inspiceret, at RelateIT har en oversigt over sikkerhedshændelser.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

ID	Kontrolaktivitet	Etableret kontrol hos RelateIT	Udførte revisionshandlinger	Testresultat
			Deloitte har stikprøvevis inspiceret relevant dokumentation, hvoraf det fremgår, at sikkerhedshændelser er blevet oprettet, dokumenteret og håndteret. Deloitte har forespurgt RelateIT, om der har været konstateret nogen informationssikkerhedsbrud, og har fået oplyst, at der ikke har været sikkerhedsbrud.	
17.1 Informationssikkerhedskontinuitet **Kontrolmål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.**				
17.1.2	Implementering af informationssikker-hedskontinuitet	RelateIT har fastlagte, dokumenterede og opdaterede procedurer og kontroller til at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret IT-beredskabsplan og dokumentation for, at den er godkendt af ledelsen. Deloitte har forespurgt, om der blev udført test af IT-beredskabsplanen.	Deloitte har fået oplyst, at der på revisionstidspunktet ikke har været udført test af beredskabsplanen. Ingen yderligere afvigelser konstateret.
18.1 Overensstemmelse med lov- og kontraktkrav **Kontrolmål: At forhindre overtrædelse af lov-, myndigheds- eller kontaktkrav i relation til informationssikkerhed og andre sikkerhedskrav.**				
18.1.4	Privatlivets fred og beskyttelse af personoplysninger	RelateIT indgår databehandleraftaler med kunder vedrørende behandling af personoplysninger.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret proceduren "Databehandlerprocedure" og observeret, at det fremgår, at der alene foretages behandling, når der foreligger en databehandleraftale, og at enhver behandling udføres i overensstemmelse med denne databehandleraftale. Deloitte har ved én stikprøve på en kunde inspiceret, at RelateIT har indgået en databehandleraftale med kunden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

PENNEO

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."

Carsten Andersen
Intern underskriver
Serienummer: 48beff95-a05a-4a66-b244-8d287171b676
IP: 193.88.xxx.xxx
2023-07-07 11:17:32 UTC

Simon Eglin Berthelsen
Intern underskriver
Serienummer: 68265612-d69a-4f42-8fd5-2f8979c41897
IP: 152.115.xxx.xxx
2023-07-07 11:21:41 UTC

Thomas Kühn
Ekstern underskriver
Serienummer: d1fc228f-48ef-4abe-abad-efe9492b4894
IP: 93.164.xxx.xxx
2023-07-07 11:42:55 UTC

Penneo dokumentnøgle: 4PIOY-OHE16-HJ0GY-J6VQQ-LE4ON-2MT23

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske s igneringsbeviser i ndlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**