NOVEMBER 2017

LINK MOBILITY A/S

ISAE 3402 TYPE 2 ERKLÆRING

Revisors erklæring vedrørende de generelle it-kontroller i tilknytning til driften af SMS-service.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR-nr. 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Erklæringsopbygning

Kapitel 1:
LINK Mobility A/S' ledelseserklæring.

Kapitel 2:
LINK Mobility A/S' beskrivelse af de generelle it-kontroller for driften af SMS-service.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de generelle it-kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf.

KAPITEL 1:

LINK Mobility A/S' ledelseserklæring

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

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af LINK Mobility SMS-service's generelle it-kontroller i hele perioden 1. juni 2016 - 31. oktober 2017. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:
- de typer af ydelser, der er leveret, når det er relevant
- de processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af LINK Mobility A/S, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller

(ii) indeholder relevante oplysninger om ændringer i LINK Mobility A/S' generelle it-kontroller foretaget i perioden 1. juni 2016 - 31. oktober 2017

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

(B) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. juni 2016 - 31. oktober 2017. Kriterierne for dette udsagn er, at:

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

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

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. juni 2016 - 31. oktober 2017

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

(i) IT-sikkerhedspolitik version 2016/03/23

(ii) Service Level Agreement for SMS-service version1

Kolding, den 14. November 2017

Mikkel Robin Nielsen
Adm. direktør

Christian Møller Hjelmager
Driftschef/ COO

LINK Mobility A/S, Birkemose Allé 37, DK-6000 Kolding, Tel (+45) 7026 1272, CVR: 30077520

KAPITEL 2:

LINK Mobility A/S' beskrivelse af de generelle it-kontroller for driften af SMS-service

Indledning

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

Beskrivelsen giver herudover information om de kontroller, der er anvendt for driften af LINK Mobility A/S' SMS-service i perioden 1. juni 2016 - 31. oktober 2017.

Beskrivelse af LINK Mobility A/S

LINK Mobility A/S beskæftiger i dag 8 medarbejdere ansat i selskabet, og har dernæst tilknyttet medarbejdere fra LINK Mobility ASA, Oslo

LINK Mobility A/S er SMS-aggregator, og leverer SMS-afsendelse og –modtagelse, primært til det danske marked.

Omfang for denne beskrivelse

LINK Mobility A/S er leverandør af services inden for informationsteknologi. Kerneaktiviteten i LINK Mobility A/S er levering og modtagelse af SMS-beskeder til de danske telenetværk samt drift af platformen hertil, men har tillige en stor udenlandsdækning. I dette dokument benævnes disse aktiviteter samlet SMS-services.

Overvågning og support sker centralt fra kontoret, og driften er placeret i floorrent faciliteter hos GlobalConnect.

LINK Mobility A/S har som leverandør ansvaret for at etablere og opretholde passende procedurer og kontroller med henblik på at finde og forebygge fejl, for således at overholde de i aftalerne stillede krav. Det er netop denne kerneaktivitet, SMS-håndtering samt vedligeholdelse af denne, der danner grundlag for nærværende beskrivelse.

Forretningsstrategi/ it-sikkerhedsstrategi

Det er LINK Mobility A/S' strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici.

LINK Mobility A/S har overordnede strategiske pejlepunkter:

- Vi ønsker at sikre de fortrolige oplysninger, kunderne sender gennem LINK Mobility koncernen.
- Vi ønsker at levere et produkt med den bedst mulige oppe-tid og fremkommelighed.
- Vi ønsker at give vores kunder et produkt, der er markedsledende.
- Vi ønsker, at vores medarbejdere har en relevant, opdateret viden.
- Vores mål skal være fælles på tværs af hele organisationen.

LINK Mobility A/S arbejder med IT-sikkerhed på et forretningsstrategisk niveau, og arbejder derfor løbende med at sikre et højt service- og kvalitetsniveau. Ledelsen prioriterer gennem selskabets sikkerhedspolitik, at IT-sikkerhed er en vigtig del af selskabets virksomhedskultur.

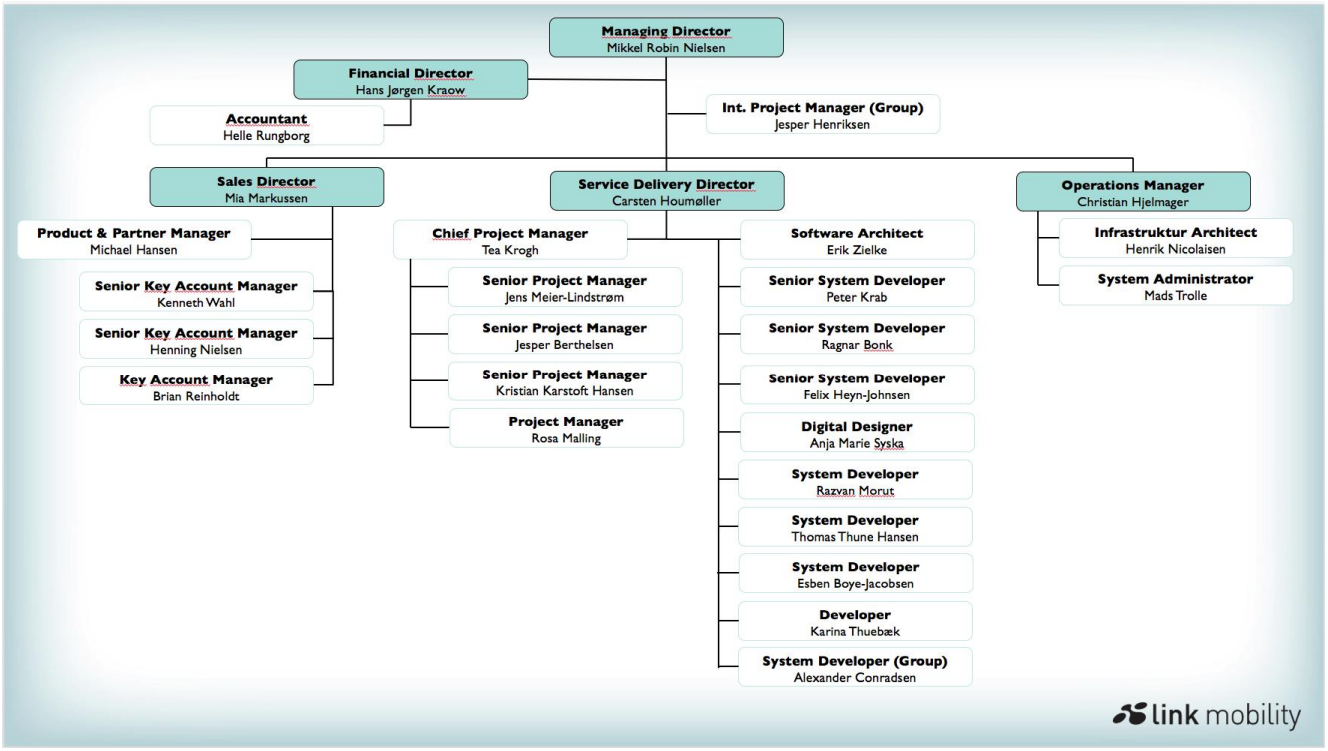
LINK Mobility A/S har omkring IT-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27002:2013, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitikker.
- Organisering af informationssikkerhed.
- Medarbejdersikkerhed.
- Styring af aktiver.
- Adgangsstyring.
- Fysisk sikring og miljøsikring.
- Driftssikkerhed.
- Leverandørsikkerhed.
- Kommunikationssikkerhed
- Styring af informationssikkerhedsbrud.
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring.

De implementerede sikringsforanstaltninger hos LINK Mobility A/S fremgår af bilag 1 til denne beskrivelse.

LINK Mobility A/S' organisation og organisering af IT-sikkerheden

LINK Mobility A/S beskæftiger 8 medarbejdere og har en flad organisationsstruktur. Virksomheden ledes dagligt af Adm. direktør, Mikkel Robin Nielsen, der samtidig har det overordnede ansvar for IT-sikkerhed. Driftschef Christian Møller Hjelmager har ansvaret for gennemførelse af revision samt kontrol og ajourføring af relevante procedurer.



Risikostyring i LINK Mobility A/S

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

LINK Mobility A/S har indarbejdet faste procedurer for risikovurdering af forretningen. Det sikres dermed, at de risici, som er forbundet med de services, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer, som vurderes. Ansvaret for risikovurderingen er en del af den IT-sikkerhedsansvarliges ansvar og skal efterfølgende accepteres og godkendes hos virksomhedens ledelse.

Som led i ovenstående IT-sikkerhedsstrategi, arbejder LINK Mobility A/S med standard for IT-sikkerhed, ISO27002:2013, som primær referenceramme for IT-sikkerheden. Arbejdsprocessen omkring IT-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at LINK Mobility A/S til hver en tid er i overensstemmelse med sine kunders krav og behov.

Håndtering af IT-sikkerhed

Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet LINK Mobility A/S' struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

LINK Mobility A/S' overordnede målsætning er at levere en stabil og sikker SMS-service til kunderne ud fra den til enhver tid gældende SLA. Til at understøtte dette er indført politikker og procedurer, der sikrer, at leverancer er ensartede og gennemsigtige.

LINK Mobility A/S' it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedsbristen omgående.

Alle servere og netværksenheder er dokumenteret i LINK Mobility A/S' dokumentationssystem. Her logges alle ændringer af driftsmiljøet. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger automatisk gemt i overvågningssystemet.

Sikkerhedspolitikken er udarbejdet, så LINK Mobility A/S har ét fælles regelsæt. Dermed opnås et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

På det generelle IT-sikkerhedsområde har LINK Mobility A/S implementeret de nødvendige procedurer og kontroller i forhold til de enkelte områder inden for ISO27002:2013, der er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, der er implementeret hos LINK Mobility A/S.

Medarbejdere og uddannelse

Alle udførende driftsmedarbejdere har kompetencer inden for de områder, de beskæftiger sig med. Dette sikres ved f.eks. rekruttering gennem netværk og evt. kontrol mod relevante referencer.

Dernæst sikres der indhentning af digital straffeattest af alle medarbejdere én gang årligt. Denne kontrol udføres i forbindelse med en årlig "IT-sikkerhedsdag", hvor den gældende IT-sikkerhedspolitik gennemgås med alle medarbejdere, dernæst er denne dag en uddannelsesdag, hvor der undervises i relevante emner relateret til IT-sikkerhed.

Fysisk sikkerhed og miljøsikring

LINK Mobility A/S' driftsmiljø er placeret i to (2) GlobalConnect datacentre, der er geografisk adskilt. Datacentrene har redundans på alle væsentlige infrastrukturkomponenter, som strøm, UPS, nødgeneratorer, netværk samt internetforbindelse.

Adgang hos GlobalConnect sker med adgangskort og personlig numerisk kode. Dernæst meldes indgang til et datacenter altid til GlobalConnect, og når et datacenter forlades, meldes dette også, så det sikres, at alle alarmer mv. er aktive. Alene autoriserede personer får adgang til datacentrene via den etablerede procedure, og der følges periodisk, minimum årligt, op på hvilke personer, der har denne adgang.

Eksterne personer (leverandører eller kunder) får kun adgang til lokalet i følge med en autoriseret medarbejder.

I datacenteret er driftsmiljøet placeret i låste skabe, hvortil kun autoriserede personer har adgang.

Levering af internetforbindelse er redundant både i leveringen fra GlobalConnect, men også fra alternativ leverandør Nianet.

Brugerstyring/ adgangssikkerhed

Adgang til driftsmiljøet kan ske ved fysisk opkobling i et datacenter eller eksternt alene via SSL VPN opkobling. Denne opkobling sker udelukkende til autoriserede personer og er rolleopdelt, med reference til den relevante medarbejders jobbeskrivelse. Disse adgange revideres mindst årligt.
Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

Ud fra IT-sikkerhedspolitikken er der følgende krav:

- Krav til password - alle brugere oprettet i LINK Mobility A/S' centrale brugerdatabase skal skifte password hver 120. dag. Password skal være på mindst 8 tal eller bogstaver, og de seneste 4 passwords kan ikke bruges igen.
- Klienter skal være opdateret med seneste sikkerhedspatches
- Der er kun adgang til driftsmiljøet via SSL krypteret VPN adgang.

Overvågning

LINK Mobility A/S har etableret automatisk overvågning af driftsmiljøet, herunder selve SMS-leverancen og har supportpersonale på vagt 24/7/365, hvorved der altid er de nødvendige kompetencer til rådighed.

Hvis en fejl konstateres, afsendes alarm både visuelt på en overvågningsskærm og på SMS. Opstår en situation, hvor der konstateres en fejl på en komponent, der ikke er en del den automatiske overvågning, tages der skridt til, at den fremover registreres i systemet. Hvis der sker hændelser, som kan påvirke driften, vil overvågningssystemet automatisk alarmere vagtberedskabet, og der forefindes en indarbejdet procedure for eskalation sluttende med, at den IT-sikkerhedsansvarlige involveres.

Backup

Formålet med backup er at sikre, at data i LINK Mobility A/S' driftsmiljø kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig nedetid.

Der tages dagligt et komplet billede af hvert datacenter, og dette lagres i det modsatte center. Dette sikrer, at der ved større nedbrud kan retableres et helt datacenter på få minutter.

Styring af IT-sikkerhedshændelser

Sikkerhedshændelser og svagheder i LINK Mobility A/S' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i LINK Mobility A/S er bekendt med procedurer og rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af LINK Mobility A/S' drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til ledelsen. Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Beredskabsstyring

Formålet med beredskabsstyring hos LINK Mobility A/S er at sikre forretningskontinuitet, kritiske informationsaktiver samt sikre kunder en hurtig og valid genetablering i tilfælde af katastrofe eller større systemnedbrud i driftsmiljøet, eller andre faktorer der resulterer i manglende leverance af services.

Ved større nedbrud informeres kunder, der benytter de påvirkede services, via mailliste-systemet samt på LINK Mobility A/S' website. Denne besked indeholder en foreløbig status, fejlbeskrivelse, samt, hvis

muligt, et estimat for, hvornår fejlen er udbedret. Kunder holdes gennem mailliste-systemet og LINK Mobility A/S' website løbende orienteret, indtil fejlen er udbedret.

Der er udarbejdet intern eskalationsprocedure med beskrivelse af beredskabet, ud fra omfanget af nedbrud eller katastrofe. Den komplette dokumentation for beredskabsstyring gennemgås og revideres årligt af driftsteamet.

Patch Management

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

Interne maskiner, der er kritiske for driften, kører ikke automatiske opdateringer. Alle lokale maskiner samt testservere sikkerhedspatches mellem kl 03:00 & 04:00 dagligt.

Servere, der indgår i produktionen, sikkerhedspatches hver søndag mellem kl. 20:00 & 21:00. Kritiske sikkerhedspatches installeres efter Link Mobiles A/S´ politik for styring af driftssoftware. Link Mobile A/S udfører dagligt backup. Formålet med backup er bl.a. at sikre, at systemerne kan komme tilbage i normal drift, hvis opdateringen ikke virker efter hensigten.

Change Management

Formålet med change management er at sikre, at ændringer testes og afprøves, inden en reel produktion igangsættes og sendes i drift.

Software i Link Mobile A/S, der skal indgå i direkte drift af SMS, underlægges retningslinjer, hvor en fast procedure følges jf. gældende bestemmelser. Kildekoder placeres i sikkert testmiljø og underlægges versionskontrol. Testmiljøet skal være så tæt på realbilledet som muligt uden at overskride sikkerhedspolitikker.

Væsentlige ændringer i forhold til IT-sikkerhed

For erklæringsperioden har der ikke været væsentlige it-sikkerhedsmæssige ændringer.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Kunder med direkte adgang til administrationssystem bærer selv det fulde ansvar for beskyttelse af denne adgang, da den giver adgang til evt. fortrolig information i form af f.eks. track & trace og dertilhørende beskedindhold. Dette betyder, at LINK Mobility A/S ikke er ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til SMS-service. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunderne er ansvarlige for datatransmission til LINK Mobility A/S' driftsmiljø, og det er kundernes ansvar at skabe den nødvendige datatransmission til LINK Mobility A/S' driftsmiljø. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

LINK Mobility A/S' beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af LINK Mobility A/S' SMS leverance. Der er ikke taget højde for faktorer, der vedrører kunders installationer eller miljøer.

BILAG 1:

LINK Mobility A/S har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2013

5. Informationssikkerhedspolitik
- 5.1. Retningslinjer for styring af informationssikkerhed

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

7. Medarbejdersikkerhed
- 7.1. Før ansættelsen
- 7.2. Under ansættelsen
- 7.3. Ansættelsesforholdets ophør eller ændring

8. Styring af aktiver
- 8.1. Ansvar for aktiver
- 8.3. Mediehåndtering

9. Adgangsstyring
- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar

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

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

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

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

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

KAPITEL 3:

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

Til kunder af LINK Mobility A/S' SMS-service og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om LINK Mobility A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af de generelle it-kontroller, som udføres i forbindelse med driften af LINK Mobility A/S' SMS-service til behandling af kunders transaktioner i perioden 1. juni 2016 - 31. oktober 2017, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. LINK Mobility A/S anvender eksterne samarbejdspartnere i forbindelse med driften af deres SMS-service på følgende områder: co-location/ datacenter – den fysiske sikkerhed omkring LINK Mobility A/S' produktionsudstyr.

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

LINK Mobility A/S' ansvar

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

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR's Etiske Regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd. Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om LINK Mobility A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt. En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelse, udformning og funktionalitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som LINK Mobility A/S har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

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

Begrænsninger i kontroller hos LINK Mobility A/S

LINK Mobility A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtig efter deres særlige forhold. Endvidere vil kontroller hos LINK Mobility A/S, som følge af deres art, muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos serviceleverandører kan blive utilstrækkelige eller svigte.

Konklusion

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

a) at beskrivelsen af LINK Mobility A/S' generelle it-kontroller til SMS-service, således som de var udformet og implementeret i hele perioden 1. juni 2016 - 31. oktober 2017, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. juni 2016 - 31. oktober 2017, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. juni 2016 - 31. oktober 2017.

Beskrivelse af test kontroller

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

Tiltænkte brugere og formål

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

Søborg, den 14. november 2017

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT auditor, Manager

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

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

Hvad angår periode har vi i vores test forholdt os til, om LINK Mobility A/S har levet op til kontrolmålene i perioden 1. juni 2016 - 31. oktober 2017.

Under feltet med resuméet af kontrolmålet er der tre kolonner:

- Første kolonne viser de aktiviteter, som LINK Mobility A/S jf. sin dokumentation har iværksat for at leve op til kravene.
- Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.
- Tredje kolonne viser resultatet af vores test.

De udføre tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring 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 blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale hos LINK Mobility A/S. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

INDLEDENDE KONTROLMÅL:

Risikovurdering og – håndtering

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

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

KONTROLMÅL 5:

Informationssikkerhedspolitikker

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

LINK Mobility A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes iht. planlagte intervaller.	Vi har indhentet og revideret LINK Mobility A/S' seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrollet, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via LINK Mobility A/S' intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

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

LINK Mobility A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer. Der foreligger passende forretningsgange for medarbejdere omkring angivelse af tavshedserklæring.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til SMS-service. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder. Gennem forespørgsler og stikprøve på ansættelsesaftale har vi kontrolleret, at medarbejdere i LINK Mobility A/S' er bekendte med deres tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og håndteretingen af sikkerhedsforholdene er passende.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos LINK Mobility A/S har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

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

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

KONTROLMÅL 8:

Styring af aktiver

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

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

KONTROLMÅL 9:

Adgangsstyring

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

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

Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer, at der sker skift af standardpassword.	Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i LINK Mobility A/S. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login. • at standard password ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (8 tegn), ingen krav til kompleksitet, maksimal løbetid (max 120 dage), ligesom password-opsætninger medfører, at password ikke kan genbruges (husker de seneste 4 versioner). Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i LINK Mobility. Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for: • minimum længde for password • maksimal levetid for password • minimum historik for password • lockout efter fejlede login forsøg	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftsikkerhed

Kontrolmål: Driftsprocedure og ansvarsområder

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

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

Kontrolmål: Malwarebeskyttelse

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

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

Kontrolmål: Backup

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

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

Kontrolmål: Logning og overvågning

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

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

Kontrolmål: Styring af driftssoftware samt Sårbarhedsstyring

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

LINK Mobility A/S' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etableret procedurer for change management i LINK Mobility A/S. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til LINK Mobility A/S' produktionsmiljøer. • at ændringer til driftsmiljøer i LINK Mobility A/S følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. Vi har stikprøvevis inspiceret, at styresystemerne er opdateret efter gældende procedurer, samt at status herpå registreres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringer i styresystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i LINK Mobility A/S. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til patch management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at alle ændringer er underlagt formel godkendelse inden idriftsætning • at ændringer er underlagt formelle konsekvensvurderinger • at der beskrives fall-back-planer • at der sker identifikation af systemer, der påvirkes af ændringer • at der sker en dokumenteret test af ændringer inden idriftsætning • at dokumentationen opdateres så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination i et "change board"	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

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

LINK Mobility A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data. Produktionsmiljøet skal være sikret mod forsyningssvigt i forhold til redundans til netværksforbindelse til internettet. Netværkstrafikken/ adgange fra produktionsmiljøet ud til omverdenen kan opnås ved hjælp af flere forsyningsindgange eller adgang fra mere end ét forsyningsselskab.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • Der er etableret passende procedurer for styring af netværksudstyr. • Der er funktionsadskillelse mellem brugerfunktioner. • Der er etableret passende procedurer og løbende opfølgning på logs og overvågning. • Styring af virksomhedens netværk er koordineret for at sikre en optimal udnyttelse af ressourcer og et sammenhængende sikkerhedsniveau. • Påset, at der etableret forbindelser for datakommunikation mod internettet via mere end én ISP-leverandør. • Stikprøvevist gennemgået dokumentationen fra leverandøren i forhold til skriftligt aftalegrundlag samt løbende afregning af ydelser hos ISP-leverandøren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.

LINK Mobility A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevis inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende anerkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører. Vi har kontrolleret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

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

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

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

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

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