Trafik-, Bygge- og Boligstyrelsen
Danish Transport, Construction and Housing Authority

It-instruks om krav til systemrevision af kørselskontorets systemanvendelse for håndtering af kørselsdata

Kort beskrivelse af emnet

Nedenstående krav skal rapporteres i en ISAE 3000 erklæring (eller tilsvarende) dækkende en 12 måneders periode og med høj grad af sikkerhed omfatte konklusioner på design, implementering og effektivitet.

Erklæringen skal udarbejdes af en uafhængig revisor med tilstrækkelig brancheindsigt og tekniske kompetencer til at vurdere risici og interne kontroller forbundet med kørselskontorets administrative kørselssystemer, forretningsgange og IT struktur.

Som udgangspunkt i nedenstående handlinger bør den uafhængige revisor anvende følgende revisionshandlinger.

Inspektion	Gennemlæst 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 udformet og implementeret, så de kan forventes at blive effektive. Vurdering, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Inspektion af parameter og konfiguration af teknisk udstyr for at sikre korrekt opsætning i henhold til kontrollen. Herunder udtræk af konfigurationer og analytiske handlinger på data for at sikre effektivitet af kontroller i erklæringsperioden.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres og dokumenteres.
Observation	Observere udførelsen af kontrollen.
Genudførelse	Genudførsel af kontrollens udførelse på baggrund af tilgængelig data og implementering med henblik på at verificere, at kontrollen har fungeret som forudsat.

Begreb	Beskrivelse
Kørselskontor	Juridisk enhed, der har fået udstedt en tilladelse til drift af kørselskontor af Trafik-, Bygge og Boligstyrelsen.
Kørselskontortilladelse	En kørselskontortilladelse giver en virksomhed ret til at drive et kørselskontor.
Vognmand	Den juridiske enhed, der har en tilladelse til erhvervsmæssig persontransport.
Erhvervsmæssig transporttilladelse	Tilladelse udstedt af Trafik-, Bygge og Boligstyrelsen til erhvervsmæssig persontransport, herunder taxikørsel, limousinekørsel og kørsel for offentlig myndighed. Tilladelse udstedes til en vognmandsvirksomhed.
Erhvervsmæssig persontransporttilladelse og relation mellem tilladelse og bil	For hver af sine tilladelser skal vognmandsvirksomheden indberette registreringsnummer på den bil, der anvendes.
Chauffør	Føreren af bilen, der udfører erhvervsmæssig persontransport. Chaufføren skal have førerkort/chaufførkort.
Førerkort/ Chaufførkort	Et førerkort er udstedt iht. den tidligere gældende taxilov af en kommune. Et chaufførkort udstedes af TBST og afløser førerkortet.
Vagt	En vagt er en sammenhængende periode (typisk 6-10 timer), hvor en chauffør udelukkende kører ture for kørselskontoret. Køres der for andre, skal chaufføren meddele dette til kørselskontoret, således at vagten kan registreres som afsluttet. En chauffør kan have flere vagter på samme arbejdsdag. Holdes der pauser, hvor chaufføren ikke er til rådighed for kørselskontoret anbefales det, at vagten afsluttes, og at der oprettes en ny, når kørslen starter igen. På samme vagt kan chaufføren køre både taxi- og kørsel for offentlig myndighed, blot alle ture køres i kørselskontorets regi. Alle ture under vagten skal registreres af kørselskontoret.
Tur	En tur er som udgangspunkt en kørselsopgave, hvor en passager køres fra startdestination til slutdestination. I visse tilfælde kan der også være tale om kørsel med laboratorieprøver mv. I andre tilfælde kan enkelt tur køres til/fra mange destinationer f.eks. kørsel for lægevagt – betingelsen er her, at turen betales samlet.
Løbende GPS koordinater	Koordinater for bilens position minimum hvert minut registreret for hver tur, der involverer erhvervsmæssig persontransport. GPS-koordinater registreres fra turens start til turens afslutning.

Kørsel efter taxameter	Tur, hvor taxametret beregner prisen.
Taxikørsel efter fast pris	Tur, hvor prisen beror på en aftalt fast pris for kørslen.
Kundetype	1. Gadetur 2. Telefonbestillling 3. Online-bestilling (herunder app, web, mail) 4. Kontraktkørsel for offentlig myndighed, 5. Kontraktkørsel for øvrige.
Pris for turen	Den pris som vognmanden modtager for turen. Normalt den pris kunden betaler direkte til vognmandsvirksomheden, men hvis vognmandsvirksomheden modtager betalingen fra kørselskontoret, angives denne. Hvis prisen er rettet efter turen pga. ændrede oplysninger om f.eks. medtaget cykel, angives den rettede pris. I data skal der blot oplyses den pris, der kendes på indberetningstidspunktet, og der er ikke pligt til at indberette ændringer.

Punkt 0: Overvågning af regelgrundlag

Kørselskontoret skal dokumentere indsigt i taxilovgivningen og har initiativpligt til at følge med i ændringer i regelgrundlaget, således at systemer til stadighed er i overensstemmelse med gældende lovgivning.

Nr.	Kontrolmål
0.1	Kørselskontoret har etableret et beredskab, som løbende følger op på regelændringer.
0.2	Kørselskontoret har etableret processer, som sikrer, at de administrative systemer er i overensstemmelse med de til enhver tid gældende regler på området.

Punkt 1 Adgangsstyring og styring af adgang til kørselsdata (herunder turdata) i de administrative systemer

Adgang til kørselssystemer og til kørselsdata skal være styret på betryggende vis.

Nr.	Kontrolmål
1.1	Kørselskontoret har etableret passende kontroller for tildeling, opfølgning og vedligeholdelse af adgangsrettigheder til systemer og data, der underbygger den organisatoriske funktionsadskillelse.

	Kørselskontoret har implementeret kontroller, der sikrer, at: a) Brugerrettigheder for adgang til tilladelser og turdata skal tildeles ud fra et arbejdsbetinget behov og godkendes før ibrugtagen af godkendt bruger b) Brugere af systemerne skal have et unikt bruger-id c) Opfølgning og vedligehold af tildelte brugerrettigheder til kørselssystemer skal udføres periodisk af rette vedkommende.
1.2	Kørselskontoret har etableret fornødne logiske adgangskontroller til kørselssystemer. Kørselskontoret har implementeret kontroller, der sikrer, at: a) Nøglesikkerhedsindstillinger, herunder password indstillinger er af tilstrækkelig kvalitet, som beskytter imod uautoriseret adgang og ændringer b) Login og logout for systembrugere logges.
1.3	Kørselskontoret har etableret funktionalitet og kontroller til at forebygge og opdage fejl, herunder bevidste fejl. Kørselskontoret har implementeret kontroller, der sikrer, at: a) Ændringer til tilladelser og turdata logges b) Opfølgning på ændringer til tilladelser og turdata gennemføres periodisk og dokumenteres.

Punkt 2 Beskyttelse af data i den underliggende it-infrastruktur

Kørselskontoret skal sikre autenticitet, tilgængelighed og integritet af opbevaret data uanset, hvordan data opbevares.

Kørselskontoret træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller bevidst tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lovning.

Nr.	Kontrolmål
2.1	Kørselskontoret har implementeret kontroller, der sikrer, at data registreres og opbevares i bilen samt beskyttes tilfredsstillende.
2.2	Kørselskontoret har implementeret kontroller, der sikrer, at data under transport (fra bil til kørselskontor) beskyttes tilfredsstillende.
2.3	Data skal beskyttes tilstrækkeligt. Kørselskontoret har implementeret kontroller, der sikrer, at data i kørselssystemers databaser/filserver mv. beskyttes tilfredsstillende.
2.4	Kørselskontoret har implementeret kontroller, der sikrer, at programkørsler monitoreres for korrekt og fuldstændig eksekvering.
2.5	Det skal sikres, at programmer og data skrives til et backup medie mindst én gang ugentligt. Kørselskontoret har implementeret kontroller, der sikrer, at programmer og data skrives til et backup medie, og at backup kan genskabes.

Punkt 3 Registrering af alle administrative brugeres brug af systemet

Kørselskontoret har implementeret kontroller, der sikrer, at adgang til privilegerede IT funktioner begrænses til autoriserede brugere.

Privilegeret adgang er defineret som adgang til systemkonfiguration, adgang til at udføre programændringer, muligheden for at tilføje eller ændre roller og adgangsrettigheder samt adgang til beskyttet data og logs.

Nr.	Kontrolmål
3.1	Adgang til privilegerede IT funktioner begrænses, logges og monitoreres. Kørselskontoret har implementeret kontroller, der sikrer, at:

	a) Adgang til privilegerede IT funktioner begrænses til autoriserede brugere b) Privilegeret brug af systemet logges, monitoreres og gennemgås månedligt c) Den månedlige gennemgang dokumenteres.

Punkt 4 Systemudvikling og vedligeholdelse

Udvikling og ændringshåndtering skal være styret på betryggende vis.

Nr.	Kontrolmål
4.1	Kørselskontoret sikrer, at systemudvikling og vedligeholdelse er en styret proces, der tager højde for krav om dokumentation, gældende målsætninger og gældende regelgrundlag. Kørselskontoret har implementeret kontroller, der sikrer, at: a) Systemleverandøren har etableret en procedure for udvikling og styring af applikationsændringer i kørselssystemer samt for overvågning af denne procedures effektivitet b) Ændringsanmodninger til kørselssystemer registreres, godkendes og prioriteres med henblik på at understøtte målsætninger c) Ændringer i kørselssystemer udvikles og implementeres med henblik på at understøtte systemets funktionalitet i forhold til gældende regelgrundlag.
4.2	Alle ændringer skal have udført nødvendige test, før de implementeres i produktionsmiljø. Kørselskontoret har implementeret kontroller, der sikrer, at der er etableret procedurer til at sikre, at de nødvendige test udføres med henblik på at afgøre, hvorvidt ændringer i kørselssystemer fungerer som ønsket, og at disse test medvirker til at understøtte systemets funktionalitet i forhold til det relevante regelgrundlag.
4.3	Alle ændringer skal godkendes af relevante medarbejdere, før de implementeres i produktionsmiljø. Kørselskontoret har implementeret kontroller, der sikrer, at der er etableret procedurer til at sikre, at ændringer implementeres i produktionsmiljøet, når tilstrækkelige test er gennemført, og at der foreligger behørig godkendelse af ændringerne fra relevante medarbejdere hos leverandøren.
4.4	For nye og ændrede systemer sikres, at dokumentation er opdateret. Kørselskontoret har implementeret kontroller, der sikrer, at dokumentation for kørselssystemer opdateres sideløbende med implementering af ændringer.

4.5	Funktionsadskillelse sikres i systemudviklingsprocessen. Kørselskontoret har implementeret kontroller, der sikrer, at roller og ansvar både i systemudviklingsprocessen og i change management processen er behørigt afgrænsede og adskilte.

Punkt 5 Systemdokumentation

Systemdokumentation skal være tilstrækkelig for kørselskontorets administrative system, der leverer kørselsdata og være tilgængelig for systembrugere.

Nr.	Kontrolmål
5.1	Kørselskontoret har implementeret kontroller, der sikrer, at: a) Kørselssystemer og øvrige applikationer har en tilstrækkelig systemdokumentation, som løbende opdateres ved ændringer. b) Systemdokumentation er tilgængelig for relevante systembrugere.

Punkt 6 Transaktions og kontrolspor

Registrerings- og indberetningsforløbet skal kunne dokumenteres.

Nr.	Kontrolmål
6.1	Kørselskontoret har etableret et tilstrækkeligt og dokumenteret transaktions- og kontrolspor fra registrering til arkivering af kørselsdata, herunder turdata og dokumentation for de kontroller, der er udført fra datafangst til endelig registrering. Transaktions- og kontrolsporet skal som minimum omfatte: a. Unik identifikation af transaktioner, der muliggør sporbarhed (transaktionsspor) b. Dokumenteret dataflow på tværs (transaktionssporet) c. Beskrivelse af implementerede interne kontroller til sikring af fuldstændighed og nøjagtighed (kontrolsporet) d. Detaljeret redegørelse for eventuelle ændringer til transaktioner i processen uden om den almindelige proces e. Detaljeret redegørelse for eventuel manuel håndtering af fejl i dataflow.

Punkt 7 Registrering af stamoplysninger om vognmand, bil og chauffør

Stamoplysninger skal registreres forsvarligt. Der skal kun registreres nødvendige oplysninger, og der skal løbende føres kontrol over oplysninger. Der skal sikres overensstemmelse med gældende persondatalovgivning.

Nr.	Kontrolmål
7.1	Kørselskontoret har implementeret kontroller, der sikrer, at stamoplysninger om vognmand, bil og chauffør registreres fuldstændigt og nøjagtigt. Kørselskontoret har interne forretningsgange og interne kontroller, der sikrer: a) En klar definition af, hvilke stamoplysninger der er registreret b) At der kun registreres nødvendige stamoplysninger c) At der er etableret tilstrækkelige kontroller til validering af stamdata d) At databehandleraftaler indgås i overensstemmelse med gældende lovgivning vedr. persondata.

Punkt 8 Registrering af chauffør vagt login og log-ud

Nr.	Kontrolmål
8.1	Kørselskontoret har implementeret kontroller, der sikrer, at login og log-ud for en chaufførs vagt registreres fuldstændigt og nøjagtigt og straks efter indtastning i kørselssystemet.

Punkt 9 Registrering af turdata (GPS-koordinater for turen, længden af turen og betaling for turen)

Nr.	Kontrolmål
9.1	Data opsamles fuldstændigt og nøjagtigt, og de kommunikeres fra bil til kørselskontor løbende i det interval, der er defineret i indledningen af denne instruks. Kørselskontoret har implementeret kontroller, der sikrer: a) Korrekt registrering af turdata, herunder a. Alle registreringer for turdata skal have et unikt ID b. Udstyr opsamler korrekt beregningsgrundlag (begyndelse- og sluttidspunkt, takster, GPS startpunkt, GPS slutpunkt, afstand og betaling) c. Registrering af kundens betaling er fuldstændig.

Punkt 10 Kontroller til sikring af, at indrapporterede turdata er fuldstændige og nøjagtige og vedrører den korrekte periode/vognmand/bil/chauffør

Nr.	Kontrolmål
10.1	Indrapporterede turdata er fuldstændige (alle ture for alle kørselskontorets vognmænd for alle dage er medtaget) og nøjagtige (turene er medtaget med korrekt erhvervsmæssig persontransporttilladelse, vognmand, bil, chauffør, begyndelses- og sluttidspunkt, GPS start punkt, GPS slut punkt, længde og betaling) og vedrører den korrekte periode/vognmand/bil/chauffør. Kørselskontoret har implementeret kontroller, der sikrer, at turdata valideres senest ved overførelse til kørselskontoret.

Punkt 11 Kontroller til sikring af, at data opsamles fuldstændigt og nøjagtigt løbende, og at de kommunikeres fra bil til kørselskontor løbende

Nr.	Kontrolmål
11.1	Kørselskontoret har implementeret kontroller, der sikrer, at: a) Der ikke er huller i nummerserien for turdata registreringer b) Der kommunikeres fra bil til kørselskontor løbende.

Punkt 12 Kontroller til sikring af, at data opbevares fuldstændigt og nøjagtigt uden mulighed for uautoriseret eller udokumenteret ændring

Nr.	Kontrolmål
12.1	Data opbevares fuldstændigt og nøjagtigt uden mulighed for uautoriseret eller udokumenteret ændring. Kørselskontoret har implementeret kontroller, der sikrer, at: a) Adgang til turdata begrænses til autoriserede brugere b) Direkte ændringer til registeret turdata kræver godkendelse af en anden autoriseret bruger og disse ændringer logges og monitoreres.

Punkt 13 Kontroller til sikring af den løbende afstemning af turdata, til sikring af, at al data leveres per chauffør, per bil, per vagt og at disse data rapporteres per vognmand, per dag og der etableres hensigtsmæssige kontroller (eksempelvis kørselsprocent, indkørt omsætning per dag etc.)

Nr.	Kontrolmål
13.1	Kørselskontoret har implementeret kontroller, der sikrer, at: a) Alt al data indrapporteres periodisk og afstemmes for fuldstændighed og nøjagtighed b) Data valideres ved indrapportering c) Der følges systematisk op på: a. Kørselsprocent b. Indkørt omsætning pr dag c. Manglende chaufførlogin/logud d. Manglende turdata jf. transaktionslogs.

Punkt 14 Eksterne grænseflader imod myndigheder

Kørselskontoret stiller stamdata og kørselsdata til rådighed for relevante myndigheder. Data stilles til rådighed via en fast defineret grænseflade indeholdende syntaks, semantik og protokol, og øvrige specificerede krav i de tilhørende grænsefladebeskrivelser overholdes.

Nr.	Kontrolmål
14.1	Kørselskontoret har implementeret kontroller, der sikrer, at: a) Data vil som minimum indeholder de oplysninger, som kræves i den tilhørende gældende vejledning b) Der foretages validering i henhold til krav beskrevet i den pågældende vejledning, inden data stilles til rådighed c) Data indberettes i rette formater krævet i den pågældende vejledning d) Der kommunikeres med kommunikationsstandard i henhold til vejledningen.

Punkt 15 Kommunikation mellem kørselskontoret og eksterne interessenter (myndigheder)

Kommunikation mellem kørselssystemer og eksterne interessenter skal være styret, således at der kan følges op på alle hændelser, og således at der er historik på modtagne og afsendte data. Kontrolmålene gælder al kommunikation med den eksterne part.

Nr.	Kontrolmål
15.1	Kørselskontoret har etableret: a) Passende kontroller vedrørende drift, herunder overvågning, registrering og opfølgning på relevante hændelser b) Fuld historik på afsendte og modtagne data c) Passende funktionalitet og kontroller til at understøtte følgende scenarier:

	a. Godkendelsesprocedurer uden transaktionsspor b. Godkendelsesprocedurer med transaktionsspor c. Godkendelsesprocedurer med transaktionsspor og versionering d. Godkendelsesprocedurer for elektronisk modtagne transaktionsdata d) Passende procedurer og metode vedrørende versionsstyring og –kontrol e) Passende procedurer for orientering om versioner og indhold heraf f) Passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift og brugerfunktioner g) Passende kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed og fortrolighed h) Passende procedurer til sikring af passende bruger- og driftsvejledninger i) Passende procedurer, der sikrer, at brugere løbende orienteres om eventuelle fejl ved eller manglende tilgængelighed til systemet.

Punkt 16 Kørselskontoret har funktionalitet og kontroller til sikring af, at aftalt data kan leveres til forespørgende myndighed på forlangende

Nr.	Kontrolmål
16.1	Kontroller skal sikre, at aftalt data kan leveres til forespørgende myndighed via: a) Tilladelser til udførelse af erhvervsmæssig persontransport for samtlige tilknyttede vognmænd b) Tilladelsen til udførelse af erhvervsmæssig persontransport er koblet til det enkelte bil og førerkort til den enkelte chauffør c) Chauffør login ved vagt start d) Tur data (GPS koordinator for turen, begyndelses- og sluttidspunkt, længden af turen og betaling af turen) e) Chauffør logout ved vagt slut.