

Undersøgelse af Adgangs- og Meldepligtsystemet

Foretaget af PricewaterhouseCoopers Statsautoriseret
Revisionspartnerselskab i 2021

Opdateret i 2023 med Bilag 4.7: Vurdering af gennemførte
ændringer

09.01.2023

Indholdsfortegnelse

1.0 Sammenfatning	3
2.0 Indledning	6
2.1 Formål	6
2.2 Metodisk rammeværk	6
2.3 Afgrænsning og begrebsdefinitioner	10
3.0 Undersøgelse	13
3.1 Opsummering af observationer	13
3.2 Proces	15
3.3 Adfærd	23
3.4 Validering og kontrol	27
3.5 Arkitektur og dataanalyser	33
3.6 Governance, risk og compliance	52
4. Bilag	58
4.1 Begrebsdefinitioner	59
4.2 Liste over afholdte møder, interviews og workshops	60
4.3 Materialeliste	62
4.4 Overblik over systemkomponenter	63
4.5 Observationsskema (simplificeret)	65
4.6 Vurdering af gennemførte ændringer	71
4.7 Vurdering af gennemførte ændringer (2023)	73

1.0 Sammenfatning

PriceWaterhouseCoopers (PwC) har på opdrag fra Udlændinge- og Integrationsministeriet (UIM) gennemført en undersøgelse af ministeriets system til kontrol af adgang og meldepligt (AMS) på udrejsecentre Kærshovedgård og Sjælsmark. Undersøgelsen er gennemført i perioden fra den 25. januar til den 16. april 2021 med forudgående dialog i januar 2021 om tilrettelæggelse af opgaven samt efterfølgende tilretning af rapporten. Undersøgelsen har været forankret i en projekt- og styregruppe med deltagelse i begge grupper af repræsentanter fra UIM's departement, UIM's Koncern It (KIT), Hjemrejsestyrelsen og Udlændingestyrelsen.

Baggrund

Undersøgelsen skal ses i lyset af, at Rigsadvokaten den 1. december 2020 besluttede midlertidig at suspendere brugen af oplysninger fra AMS under hovedforhandlinger eller retsmøder vedrørende opretholdelse af anholdelse og varetægtsfængsling ved manglende overholdelse af opholds-, underretnings- og meldepligt. Rigsadvokaten henviste til, at der ved behandlingen af et mindre antal straffesager var identificeret en række sager med uregelmæssige registreringer i AMS, som ikke var indgået i den undersøgelse, der var redegjort for i Udlændinge- og Integrationsministeriets orientering af 29. september 2020.

På baggrund af udmeldingen fra Rigsadvokaten om berosættelse af behandlingen af straffesager om opholds- og meldepligt besluttede Hjemrejsestyrelsen, at der fra torsdag den 10. december 2020 skulle ske manuel kontrol med udlændinges opholds- og meldepligt på Udrejsecenter Kærshovedgård og Udrejsecenter Sjælsmark. Det blev endvidere besluttet, at der var behov for en ekstern uvildig undersøgelse og validering af dels systemets tekniske funktion og dels den praktiske anvendelse af systemet. Dette med henblik på en vurdering af validiteten af data fra systemet og for at identificere eventuelle tiltag, der kan styrke/genoprette validiteten i data i nødvendigt omfang.

Fokus for undersøgelsen

Sigtet med undersøgelsen har været at afdække, om der er forhold omkring AMS, herunder den tekniske opbygning, dataflow og den praktiske anvendelse, der udgør risici for datatab, dataforvanskning eller forkerte eller manglende registreringer af data, så registreringerne ikke omfatter beboernes reelle færden og passager. Fokus har i undersøgelsen både været på henholdsvis online data (data fra standere på begge udrejsecentre) og offline data (data fra dørlåse på Kærshovedgård).

Genstandsfeltet for undersøgelsen er udgjort af de primære aktiviteter i AMS (se figur 1, delproces 2-7), herunder beboerregistrering, indgangsregistrering, meldepligtregistrering, øvrig hændelsesregistrering, udgangsregistrering samt undersøgelse af brud på pligter (melde-, opholds- og underretningspligt). Hertil kommer systemunderstøttelse på tværs af AMS-processen (delproces 8, figur 1). Selve håndteringen (oprettelsen) af pligter (melde-, opholds- og underretningspligt) (delproces 1) er udenfor denne undersøgelses genstandsfelt. Undersøgelsen tager udgangspunkt i en teknisk afgrænsning som defineret af UIM i forbindelse med opgavebeskrivelsen (se afsnit 2.3.2 for den konkrete tekniske afgrænsning).

Undersøgelsen skal ses som supplementet til allerede gennemførte interne redegørelser i UIM, herunder diverse faktaark for området. Undersøgelsen skal endvidere ses i sammenhæng med den undersøgelse af de fysiske forhold på centrene, som UIM gennemfører parallelt med denne undersøgelse, men som ligger uden for genstandsfeltet for denne undersøgelse.

Konklusion

Konklusionen på undersøgelsen skal ses i lyset af hovedaktiviteter, som er gennemført i undersøgelsen, herunder særligt en række observationer og dataanalyser i AMS. Der er i dataanalyserne *ikke* fundet nogen indikationer på hverken tab eller forvanskning af online data i dataflowet i AMS. Samtidig er der på online data *ikke* fundet en teknisk eller systemmæssige årsag til observationer omkring datatab eller -forvanskning i

AMS, herunder også dobbeltregistreringer på meldestandere og modstridende registreringer. Dataanalysernes resultater bidrager til forskellige observationer i afsnit i rapporten, fx i forhold til implementering af antipassback for stregkodekort (fejlmelding hvis en beboer laver to på hinanden følgende ind- eller udgangsregistreringer) samt forkert brug af datamodel, hvoraf ingen af observationerne vurderes at kunne indebære en direkte risiko for dataforvanskning (se også gennemgang af dataanalyser i afsnit 3.5.2.2).

Undersøgelsens tilgang har været at gennemgå alle tilfælde med observationer med betydning for dataforvanskning og/eller datatab. Der er i den forbindelse identificeret 2 observationer, som indebærer en direkte risiko for dataforvanskning og/eller datatab i AMS.

Samlet set har undersøgelsen ført til 25 observationer, der hver beskriver en problemstilling i relation til risiko ved registrering og databehandling i AMS-processen og det dertilhørende dataflow. Observationerne fordeler sig på tværs af AMS-processen, men er særligt centreret omkring ind- og udgangsregistrering samt den underliggende systemunderstøttelse. Observationerne er prioriteret efter væsentlighed. Der er identificeret to observationer med prioritet ”1”, hvilket betyder, at håndtering af disse er en forudsætning for at undgå risiko for dataforvanskning. Det drejer sig om 1) ”Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG” (se også afsnit 3.5) og 2) ”Uklar proces for tilmelding og tilkobling af nye registreringsenheder” (se også afsnit 3.6). Herudover vurderes fem prioritet 1-observationer og én prioritet 3-observation allerede at være afhjulpeth i tilstrækkelig grad. Af de fem prioritet 1-observationer er tre kategoriseret som ”valideret afhjulpeth” (det er valideret, at risikoen er afhjulpeth) og to kategoriseret som ”ingen problematik observeret” (det har i undersøgelsen ikke været muligt at genfinde problemstillinger, som fx er beskrevet i diverse faktaark).

Af de resterende 17 observationer er 12 observationer kategoriseret som prioritet ”2”, hvilket betyder, at observationerne ikke selv kan forårsage dataforvanskning eller -tab, men bør inkluderes i en længeresigtet plan for modning af AMS såvel som styringen af området. De sidste fem observationer er kategoriseret som prioritet ”3” og kan hermed ikke i sig selv have betydning for dataforvanskning og datatab, men de bør på linje med prioritet 2-observationer indgå i en generel modning af området.

Tværgående observationer

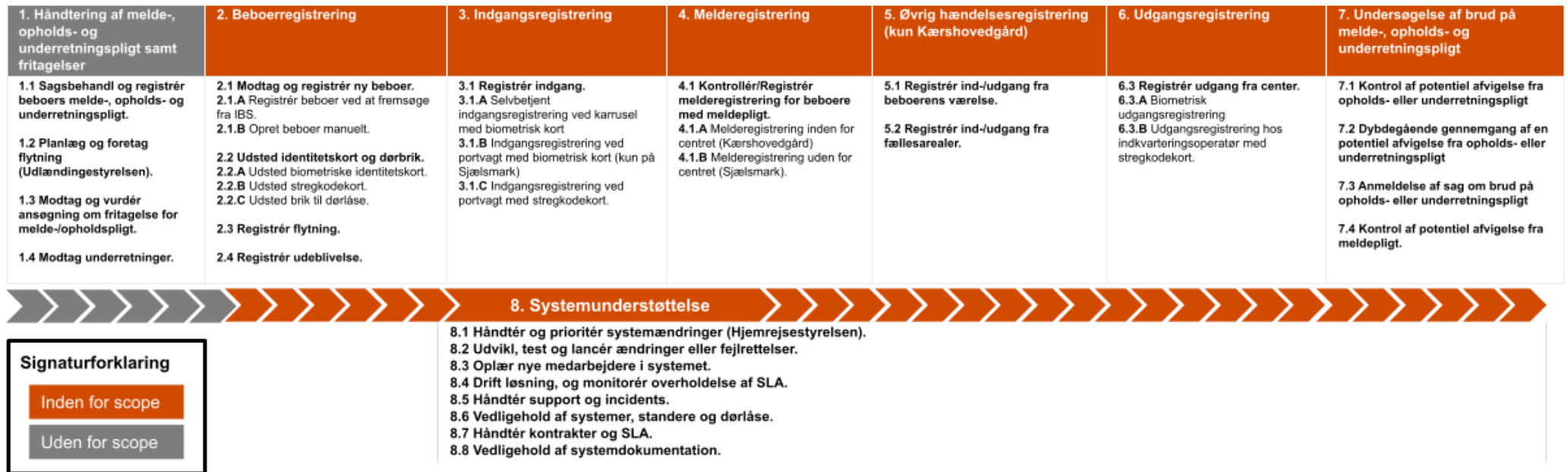
I forbindelse med undersøgelsen er der også gjort en række tværgående observationer med relevans for den samlede AMS-proces, som bør håndteres i forhold til risikoen for dataforvanskning og datatab i AMS.

Det drejer sig særligt om organisering og governance samt beboeradfærd ved brug af AMS samt betydningen af fysisk arkitektur:

- *Beboeradfærd ved brug af AMS:* Det er i forbindelse med undersøgelsen oplyst, at visse beboere aktivt forsøger at forhindre registrering af deres passager ind og ud af udrejsecentrene samt i det hele taget forsøger at stressteste og så mistillid til data i AMS. Dette sker ved, at beboerne bevidst undgår registreringer ved at hoppe over hegnet, sætte sko i døren (Kærshovedgård) mv. Beboeradfærden kan eksempelvis ses i dataanalyserne, hvor et stort omfang af dobbelte registreringer på meldestandere ikke kan teknisk begrundes, men snarere peger i retning af beboernes adfærd i forbindelse med meldepligtsregistrering (se kontrol 8 i afsnit 3.5.2).
- *Organisering og governance:* AMS-processen understøttes af en kompleks organisering og fordeling af opgaver og ansvarsområder på tværs af en række både interne aktører i UIM og eksterne leverandører. Der er ikke etableret en entydig placering af henholdsvis systemejerskab og procesejerskab, hvilket foreslås at indgå som led i den videre modernisering af området.
- *Fysisk arkitektur:* Validiteten af data i AMS er i høj grad afhængig af den fysiske arkitektur på udrejsecentrene, som dog ikke er inden for denne undersøgelses genstandsfelt, men håndteres i en særskilt analyse i UIM. Disse observationer er eksempelvis muligheden for at passere hegn og herved undgå passage via ind- og udgange. Observationerne er overleveret løbende til UIM og ikke inkluderet i denne rapport.

Som led i afslutningen af undersøgelsen har PwC gennemført en vurdering af UIM's håndtering af de to udestående prioritet 1-observationer. Resultaterne af vurderingen er for hver observation sammenfattet i bilag 4.6.

Figur 1. Procesdiagram for AMS med fokus på arbejdsgange i form af delprocesser



2.0 Indledning

2.1 Formål

Formålet med undersøgelsen er at give input til en vurdering af validiteten af Adgangs- og Meldepligtsystemet (AMS), herunder af de data, der registreres i systemet, med henblik på at:

- undersøge tilstedeværelsen af eventuelle risici relateret til forvanskning og tab af oplysninger i AMS i hele dataflowet fra registrering af data til opbevaring, filtrering og udstilling af data samt den praktiske anvendelse af systemet
- vurdere eksisterende kontrolforanstaltninger i forhold til håndtering af data i systemet, herunder både af datamæssig, systemmæssig og processuel karakter
- identificere anbefalinger, som kan nedbringe risikoen for forvanskning og tab af data i AMS, herunder både af datamæssig, systemmæssig og processuel karakter.

Undersøgelsen giver på denne baggrund et uvildigt input til og grundlag for en vurdering af, om der er risiko for forvanskning og tab af oplysninger i AMS – ud over de risici og årsager, der er fremhævet i UIM's faktaark og tidligere redegørelser til bl.a. Folketingets Udlændinge- og Integrationsudvalg. Hertil giver undersøgelsen anbefalinger, som ved implementering kan nedbringe risikoen for forvanskning og tab af data i AMS.

Endelig udgør undersøgelsen, sammen med UIM's faktaark, et faktuel grundlag i forhold til en vurdering af data i forbindelse med behandlingen af sager vedrørende opretholdelse af anholdelse og varetagtsfængsling ved manglende overholdelse af pligter.

2.2 Metodisk rammeværk

PwC anvender det metodiske rammeværk PAVA som struktur for undersøgelsen og ramme for de metoder, som anvendes til at gennemføre undersøgelsen af AMS.

PAVA er baseret på PwC's internationale metoderammeværk og er tilpasset de erfaringer, PwC har opnået ved tidligere gennemførte datahåndterings- og kontrolopgaver i centraladministrationen. På den måde sikrer anvendelsen af PAVA-rammeværket, at undersøgelsen forholder sig til alle relevante elementer i relation til AMS, uanset om de adresseres metodisk eller ligger uden for undersøgelsens afgrænsning af genstandsfeltet (se afsnit 2.3 for afgrænsning af genstandsfelt).

PAVA har fem hovedområder, som er vist i figur 2. De fem hovedområder forholder sig til opgavens genstandsfelt, dvs. Adgangs- og Meldepligtsystemet, som vil være omdrejningspunktet for anvendelse af rammeværket (benævnt "AMS" i figuren). De fem hovedområder i PAVA indeholder alle en række underkategorier og delområder, som er med til at fokusere undersøgelsen af AMS, herunder:

- **Processer**, særligt af delprocesser og understøttende processer til AMS såvel som forskelle mellem udrejsecentrene (procesvarianter) (se også afsnit 3.2)
- **Adfærd**, særligt Kriminalforsorgens medarbejderes bevidsthed, kompetencer og efterlevelse af retningslinjer samt best practice for at opretholde kontroltrykket på udrejsecentrene ved brug af AMS (se også afsnit 3.3)
- **Validering (og kontrol)**, særligt etablerede kontrolforanstaltninger til at opretholde kontroltrykket såvel som kontrollernes praktiske udførelse og dokumentation (se også afsnit 3.4)
- **Arkitektur**, særligt de væsentligste tekniske komponenter i AMS samt relevante forhold omkring datas passage gennem AMS i forhold til risikoen for dataforvanskning og datatab (se også afsnit 3.5)
- **Governance, risk og compliance**, særligt de understøttende og rammesættende forhold for AMS, fx systemejerskab, procesejerskab,

håndtering af ændringer i AMS (incidents) og kontraktuel håndtering og klassificering (se også afsnit 3.6).

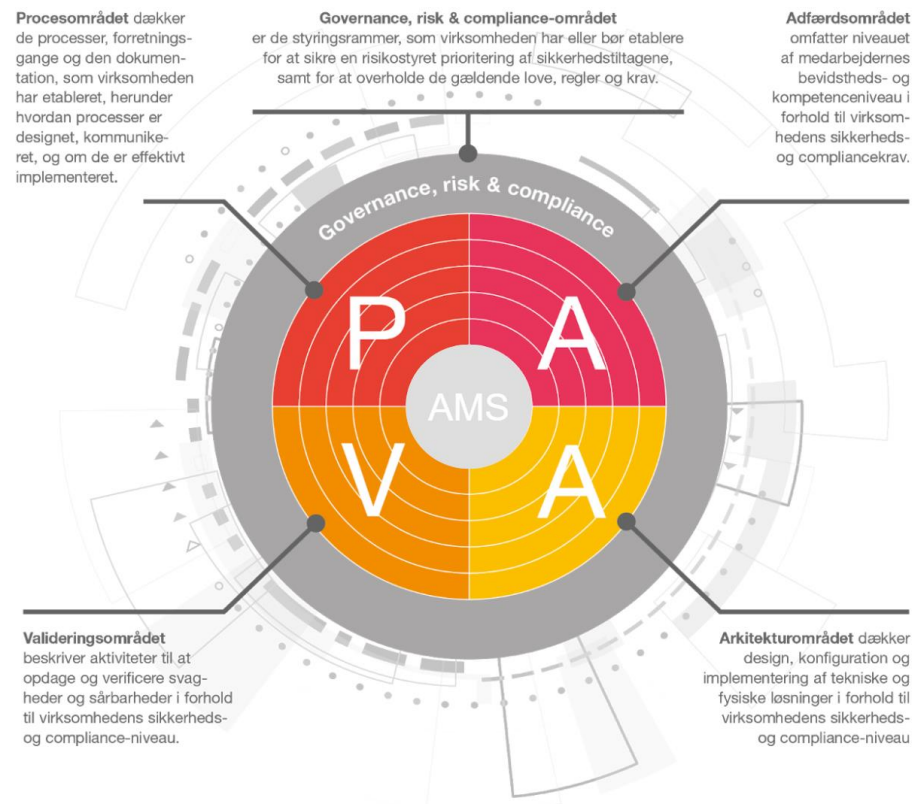
De nævnte fokusområder anvendes til at udvælge de metoder, der er relevante at inddrage i undersøgelsen inden for rammerne af PAVA-rammeverket. PwC har på baggrund af aktiviteterne inden for hvert af de fem områder i PAVA identificeret relevante observationer, deres afledte risici og anbefalinger, hvilket fremgår af de enkelte afsnit såvel som det vedlagte observationsskema.

Observationsskemaet opsummerer alle observationer identificeret i denne undersøgelse med angivelse og beskrivelse af de tilknyttede problemstillinger, afledte risici, eventuelt mitigerende kontroller og eventuelt mitigerende anbefalinger i forhold til risikoen. Af observationsskemaet fremgår også, hvilke udrejsecentre observationen er relevant for, samt prioriteringen i forhold til risikoen for dataforvanskning og observationens tilstand (fra tese til validering).

Endelig vurderes hver anbefaling i forhold til den forventede effekt på den givne risiko samt det afledte ressourcekrav, og der tilføjes en reference til kilden for observationen. Observationsskemaet indgår som bilag 4.5 (simplificeret format) og udgør den tværgående opsamling på alle observationer, som er identificeret inden for rammen af PAVA-modellen.

Det bemærkes, at afsnittet om processer (afsnit 3.2) ikke indeholder observationer, men i stedet sætter en ramme og struktur for beskrivelsen af observationer på de andre områder i PAVA-modellen. Hermed har afsnittet til formål at sætte konteksten for resten af undersøgelsen ved at beskrive AMS-processen i detaljer, hvorved aktørerne bag undersøgelsen opnår en fælles referenceramme for og forståelse af AMS-processen.

Figur 2. Illustration af PAVA-rammeverket (inklusive generiske beskrivelser af de fem områder i modellen i forhold til sikkerhed og compliance)



På baggrund af områderne i PAVA-rammeverket er der anvendt en række metoder for at foretage en fuldstændig undersøgelse af AMS. Metoderne kan kategoriseres i fem grupper:

- Workshops
- Dokumentationsgennemgang
- Interviews og besigtigelser
- Kontrolanalyse
- Dataanalyser.

Workshops til validering af centrale leverancer og genstandsfelt

Workshopformatet er i undersøgelsens opstart anvendt til at kvalificere og validere udkast til rammesættende leverancer omkring tilrettelæggelsen af opgaven samt kvalificering af værktøjer og metoder til gennemførelse af dataanalyser og kontrolanalyse samt senere i undersøgelsen til at strukturere viden (fx gennemgang af kontroller i kontrolanalysen). PwC har til disse workshops udarbejdet udkast til centrale leverancer (fx procesdiagram, systemoverblik og observationsskema), som på workshopperne er blevet anvendt til at afgrænse opgaven og være en ramme for opsamling af observationer. Endelig er der udarbejdet en aktivitets- og leveranceplan. Gennem workshops og projektgruppemøder har projektgruppen gennemgået leverancerne med fokus på validering, fuldstændighed og anvendelighed i forhold til områderne i PAVA-rammeverket samt undersøgelsen i det hele taget.

Dokumentgennemgang, så undersøgelsen bygger på eksisterende viden

Alle analyseelementer i PAVA-modellen inkluderer gennemgang af eksisterende dokumentation og materiale for at sikre, at undersøgelsen så vidt muligt bygger på eksisterende viden. Viden fra UIM's faktaark er blevet anvendt gennemgående i undersøgelsen sammen med forskellige typer af dokumenter, som er stillet til rådighed i løbet af undersøgelsen (fx operatørkontrakt mellem Udlændingestyrelsen og Kriminalforsorgen, systemdokumentation for AMS og dokumentation af tilsyn). Materialet er ikke indarbejdet direkte, men data fra materialet har ligget til grund for fx bruttolisten over observationer i denne undersøgelse og hermed også vurderingen af risikoeksponeringen i AMS i forhold til dataforvanskning og datatab (se også bilag 4.3 for materialeliste).

Interviews og besigtigelser, så undersøgelsen bygger på forretningsmæssig indsigt

Et bærende element i undersøgelsen har været gennemførelse af besigtigelser på både KHG og SJM samt interviews med Kriminalforsorgens medarbejdere på centrene såvel som leverandører og aktørerne bag AMS. Formålet var at opnå dyb forretningsmæssig viden om og forståelse af problemstillinger i forhold til datatab og dataforvanskning samt at skabe grundlaget for konkrete og handlingsorienterede anbefalinger. Der er gennemført ti interviews og tre besigtigelser (inklusive tillægsbesigtigelse på KHG) samt håndteret en række opfølgende mails og henvendelser om særskilte problemstillinger. Alle observationer fra interviews og besigtigelser er dokumenteret særskilt i interviewskabeloner, som er valideret og

kommenteret efterfølgende af interviewpersonerne. Interviewene har også ligget til grund for løbende udvikling af procesdiagram, systemoverblik, observationsskema, kontrolmatrice mv. Der er desuden indhentet data fra dataflowet i AMS (Salto-rådataloggen, som giver mulighed for at se en enkelt beboers registreringer) til at tjekke, hvor præcise registreringerne på udrejsecentre er i forhold til data i AMS.

Kontrolanalyse til vurdering af design og udførelse af kontroller

På baggrund af workshops, besigtigelser, interviews og dokumentgennemgang er der opsamlet en bruttoliste over kontroller, der skal forhindre dataforvanskning og datatab i AMS. Kontrollerne er indsat i PwC's kontrolmatrice, som sammenholder kontrollerne med konkrete risici for dataforvanskning, med henblik på en vurdering af hver kontrol og beskrivelse af konkrete anbefalinger, som kan reducere eventuelle risici.

Kontrollerne i AMS er vurderet på to overordnede parametre:

1. *Kontrollernes designeffektivitet*, dvs. deres tilstrækkelighed og behov i forhold til risikoen for dataforvanskning og/eller datatab i AMS
2. *Kontrollernes funktionelle effektivitet*, dvs. hvorvidt de etablerede kontroller faktisk udføres og fungerer. Kontrollernes funktionelle effektivitet er blevet testet via besigtigelserne, hvor det vurderes, om kontrollerne udføres som beskrevet, og efterfølgende om kontrollerne er dokumenteret på behørig vis.

Dataanalyser til undersøgelse af risiko for datatab og -forvanskning i AMS

Dataanalyserne er dels gennemført hypotesedrevet, hvor det søges at be- eller afkræfte hypoteser (fx tidsforskydninger mellem beboernes passager og registrering i Salto-loggen), kontrollere akkuratheden af registreringer (dvs. om data afspejler det rigtige tidspunkt og sted for registreringen) og en struktureret gennemgå generelle datakvalitetsparametre baseret på PwC's rammeverk for vurdering af datakvalitet, jf. figur 3. Hertil er data sammenlignet på tværs af dataflowet, og der er gennemført review af kodeelementer, som bidrager til udtræk, transformation og indlejring af data i løbet af dataflowet (se også afsnit 3.5 i forhold til dataanalyser). Formålet har været at belyse datakvaliteten i systemkomplekset med forskellige perspektiver på datakvalitet, herunder akkurathed, fuldstændighed, konsistens, unikhed og validitet på tværs af komponenter i AMS (jf. figur 3). Som det fremgår af figuren er henholdsvis "Integritet" og "Tilgængelighed" ikke i fokus, da de henholdsvis er ude af scope og ikke relevant som selvstændig risiko for dataforvanskning og/eller datatab.

Figur 3. PwC's rammeværk for undersøgelse af datakvalitet (inklusive datakvalitetsparametre)

Datakvalitetsparametre		I fokus
	Akkurathed: Sammenligning af data med det faktiske objekt, som data repræsenterer, for at sikre at data er en nøjagtig repræsentation af "virkeligheden".	Ja
	Fuldstændighed: Kontrol af, at de forventede oplysninger er til stede i data, såsom de forventede attributter eller antallet af rækker i et datasæt.	Ja
	Konsistens: Kontrol af, at der ikke er variation i data på tværs af fx systemer, tabeller og processer.	Ja
	Integritet: Sikring af, at uvedkommende ikke kan kompromittere datas integritet, herunder om it-sikkerheden tilstrækkeligt beskytter mod bevidste forsøg på at kompromittere datas integritet (fx hacking).	Nej
	Tilgængelighed: Kontrol af, at data er tilgængelige på det nødvendige tidspunkt til et specifikt brugerbehov.	Nej
	Unikhed: Kontrol af, at data er unikke, eller om der er dubletter, hvor der ikke burde være det.	Ja
	Validitet: Måling af, at data overholder et sæt forretningsregler for, hvordan data forventes at se ud.	Ja

Der er især anvendt følgende metoder til at gennemføre dataanalyserne:

- *Manuelle stikprøver* er anvendt til at kontrollere, om data bliver forvansket gennem dataflowet, fx ved at sammenligne data fra før

overførsel fra Salto loggen (Salto-hændelsesjobs) med data i Salto-databasen (Salto BI DB), med henblik på at vurdere om data har ændret sig. Et eksempel på en konkret ændring, som undersøges via stikprøven, er, om tidsstempler forbliver korrekte gennem dataflowet.

- *Fysiske stikprøver* er anvendt til at teste, om registreringerne på udrejsecentrene er præcise. Dvs. om data korrekt afspejler tid og sted for beboerens registrering. Dette er gjort ved at notere tidspunktet og stedet for registreringen i forbindelse med besigtigelse og efterfølgende at sammenholde disse noter med data fra dataflowet i AMS med fokus på særlige risici (fx tidsforskydning).
- *Review af kode og forretningslogik:* En gennemgang af den kode og logik, som potentielt kan ændre data, fx i forbindelse med daglige overførsler af data fra én database til en anden. En ændring af data kan i den forbindelse være, om datatyper følger forventede formater (fx formater for dato som "dd-mm-åååå").

Metoderne er baseret på adgang til data i AMS, herunder Salto-applikationen (både webapplikation på de enkelte centre og den bagvedliggende database), jobserver hos Statens It (SIT), som håndterer overførsler af data fra Salto-applikationen til HJEMSTs BI-database, og QlikView, som anvendes af HJEMST til at undersøge eventuelle brud på pligter hos beboerne på udrejsecentrene (se også afsnit 3.5 for beskrivelse af systemkomplekset).

2.3 Afgrænsning og begrebsdefinitioner

I det følgende vil de mest relevante afgrænsninger for denne undersøgelse blive gennemgået, herunder afgrænsning i forhold til processen for adgangs- og meldepligt samt afgrænsning af den tekniske systemunderstøttelse. Herefter beskrives de mest centrale begrebsdefinitioner for at kunne forstå rapporten. Afslutningsvis afgrænses publikationen og genstandsfeltet.

2.3.1 Afgrænsning af processen

Undersøgelsen afgrænses til at inkludere visse delprocesser og aktiviteter i processen for adgangs- og meldepligtsystemet på udrejsecentrene KHG og SJM. Den inkluderer også forskelle i processen (procesvarianter) mellem de to centre. Fx er indgangsregistrering ved portvagten med biometrisk kort kun muligt på SJM, hvorfor dette behandles som en selvstændig procesvariant. *Figur 4* gengiver de otte trin i processen, herunder også it-understøttelsen. De primære aktiviteter i processen inden for genstandsfeltet (delproces 2-7) er beboerregistrering, indgangsregistrering, meldepligtregistrering, øvrig hændelsesregistrering, udgangsregistrering samt undersøgelse af brud på pligter (melde-, opholds- og underretningspligt). Hertil kommer systemunderstøttelse på tværs af AMS-processen (delproces 8). Selve håndteringen (oprettelsen) af pligter (melde-, opholds- og underretningspligt) (delproces 1) er udenfor denne undersøgelses genstandsfelt.

Figur 4 Processen for adgangs- og meldepligt



Processen anvendes som struktur og referenceramme for rapportering af observationer i denne rapport. Processen foldes ud og beskrives i større dybde i afsnit 3.2 (Procesbeskrivelse).

2.3.2 Afgrænsning af den teknisk systemunderstøttelse

Undersøgelsen tager udgangspunkt i en teknisk afgrænsning som defineret af UIM i forbindelse med opgavebeskrivelsen. På den baggrund og som led i de løbende afklaringer i undersøgelsen afgrænses den tekniske systemunderstøttelse til følgende elementer:

- Ind- og udgangsstandere samt meldepligtstandere på KHG og SJM koblet op til systemet
- Offline registreringsenheder (beboerdørlåse og låse til fællesarealer) på KHG
- Salto ProAccess Space (herunder både applikationskoden og databasen)
- Pc-opsætning, kortstationer og kontrolstandere til brugeroprettelse på KHG og SJM samt til manuel registrering
- Håndscannere til stregkoder til brug ved manuelle registreringer
- Registreringsenheder til nulstilling/genaktivering af kort
- Forbindelse fra enheder og pc på KHG og SJM til servere på UIM's domæne hos SIT
- Udvalgte jobs, der bidrager til udtræk, transformation og indlæsning af data i løbet af dataflowet
- Databaser, der bidrager til lagring af data i løbet af dataflowet (ud over den oprindelige Salto-database)
- Løsning til visning og sortering af data til at understøtte sagsbehandling i HJEMST.

Et samlet overblik over det systemmæssige genstandsfelt for undersøgelsen fremgår af figur 5 på næste side.

Det bemærkes, at der i undersøgelsen indgår fysiske elementer (fx ind- og udgangsstandere, registreringsenheder, kontrolstandere og håndscannere), som angivet i figur 5. Nærværende undersøgelse er dog afgrænset fra den fysiske arkitektur som hegn, mure, opsætning af sluser mv. Disse elementer håndteres i en særskilt analyse af de fysiske forhold på centrene, som ikke gennemføres af PwC. PwC har i forbindelse med besigtigelserne, interviews med Kriminalforsorgens medarbejdere og HJEMST gjort observationer med relevans for den fysiske arkitektur. Disse observationer er overleveret uden for genstandsfeltet af denne undersøgelse.

Figur 5: Overblik over den systemmæssige afgrænsning af opgavens genstandsfelt

Tekniske komponenter uden for scope: Følgende komponenter er relevante for den overordnede forståelse af AMS-komplekset, men er uden for undersøgelsens scope.

UIM's systemer
CARL2 og IBS

**Automatisk
oprettelses-
applikation**

Stored procedures
Kode og
forretningslogik til
dannelse af
QlikView-anmeldels
esliste

**QlikView-
anmeldelsesliste**
Potentielle
anmeldelser for
brud på opholds- og
underretningspligt

**Sagsbehandlings-
systemer**
Fx Public 360

Tekniske komponenter inden for scope

**Ind- og udgangsstandere
samt meldepligtstandere**

Fx registreringsenheder ved
karruseller, biometriske kort-
samt stregekodekortscannere

Salto-applikationen

Herunder frontend, backend,
database og udtræk af
hændelseslog

**Netværksforbindelse og
integrationsmønstre**

Forbindelse fra enheder og
pc'er på KHG og SJM til
servere på UIM's domæne
hos Statens It

QlikView-rådatalog

Oversigt over registreringer
med mulighed for at
fremsøge pr. Beboer.
Indgår i datagrundlag, der
fremsendes til
Anklagemyndigheden i
tilfælde af en anmeldelse for
brud på opholds-, melde- og
underretningspligt

**Offline
registreringsenheder**

Beboerdørlåse og låse til
fællesarealer

**Enheder til
brugeroprettelse**

Fx biometriske kort, pc'er
med adgang til AMS,
bordkoder og
førstegangslæsere

Udvalgte jobs

Jobs, der bidrager til udtræk,
transformation og indlæsning
af data i løbet af dataflowet
(programmeret i MS
PowerShell)

Udvalgte mellemlagre

Databaser, der bidrager til
lagring af data i løbet af
dataflowet (udover den
oprindelige Salto-database)

2.3.3 Afgrænsning af undersøgelsens genstandsfelt

Dette afsnit præciserer en række perspektiver, som potentielt kunne have været afdækket i undersøgelsen, men som efter aftale med opdragsgiver ikke er en del af genstandsfeltet.

Sikkerhedsniveauet i hardware og software, herunder fx kryptering af data, autentificeringsmekanismer, beskyttelse mod malware og lignende, er efter aftale med opdragsgiver ikke en del af genstandsfeltet. Det er således uden for opgavens afgrænsning fx at vurdere risikoen for, at en beboer eller anden aktør har mulighed for at kompromittere dataintegriteten i det samlede systemkompleks (mulighed for at forvanske data, som systemet opbevarer), fortroligheden (mulighed for at få adgang til at se data, som man ikke skal kunne se) eller tilgængeligheden (mulighed for at gøre systemet ubrugeligt eller utilgængeligt).

En videre undersøgelse og besigtigelse af beboernes adfærd ved brug af AMS er ikke inden for genstandsfeltet af denne analyse, og da observationer i relation til konkret beboeradfærd alene er overleveret via interviews og ikke selvstændigt undersøgt og besigtiget, leder dette ikke til videre observationer, til trods for deres potentielt dataforvanskende karakter.

2.3.4 Publikationens afgrænsning

Denne rapport er udarbejdet til intern brug i UIM samt til dialogen med Anklagemyndigheden. Rapporten er udtryk for PwC's vurdering af processerne omkring AMS-systemet og giver alene en vurdering af risikoen for, om data, der registreres i systemet, kan forvanskes. Rapportens dataanalyser er efter sædvanlig praksis funderet på stikprøver vedrørende risikoen for forvanskning og/eller tab af data i AMS. Denne rapport er ikke en egentlig revisionsmæssig udtalelse eller vurdering, da fokus for undersøgelsen har været at gennemføre en detaljeret gennemgang af systemet for at identificere eventuelle risici for dataforvanskning og datatab samt anbefalinger til håndtering af samme, jf. afsnit 2.1.

3.0 Undersøgelse

3.1 Opsummering af observationer

Undersøgelsens tilgang har været at gennemgå alle tilfælde med observationer med betydning for dataforvanskning og/eller database. Der er i den forbindelse identificeret 2 observationer, som indebærer en direkte risiko for dataforvanskning og/eller database i AMS.

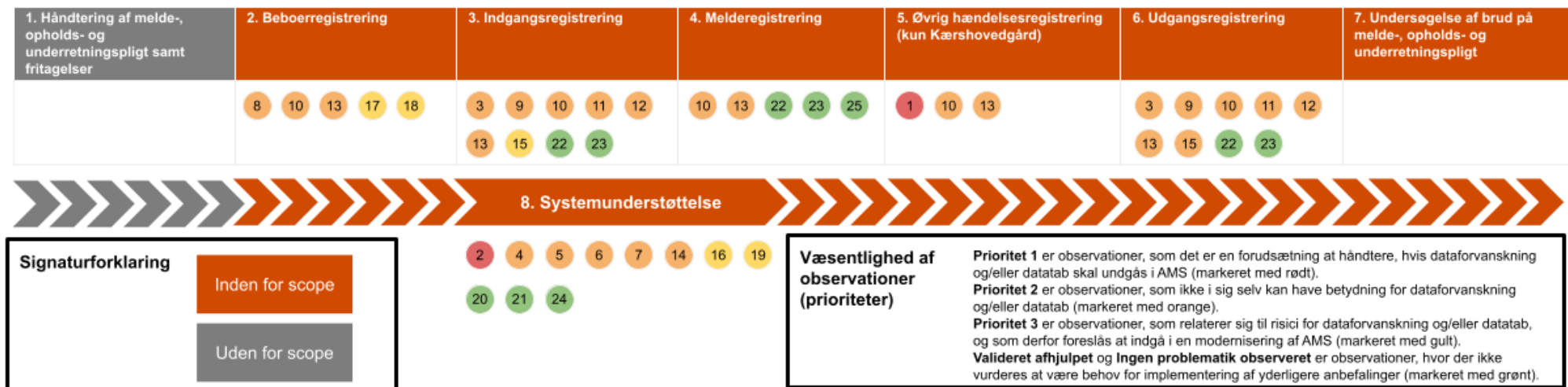
Samlet set har undersøgelsen ført til 25 observationer, der hver beskriver en problemstilling i relation til risiko ved registrering og databehandling i AMS-processen og det dertilhørende dataflow. Observationerne fordeler sig på tværs af AMS-processen, men er særligt centreret omkring ind- og udgangsregistrering samt den underliggende systemunderstøttelse. Observationerne er prioriteret efter væsentlighed. Der er identificeret to observationer med prioritet "1", hvilket betyder, at håndtering af disse er en forudsætning for at undgå dataforvanskning. Det drejer sig om 1) "Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG" (se også afsnit 3.5) og 2) "Uklar proces for tilmelding og tilkobling af nye

registreringsenheder" (se også afsnit 3.6). Herudover vurderes fem prioritet 1-observationer og én prioritet 3-observation allerede at være afhjulpeth i tilstrækkelig grad.

Af de resterende 18 observationer er 12 observationer kategoriseret som prioritet "2", hvilket betyder, at observationerne ikke selv kan forårsage dataforvanskning eller -tab, men bør inkluderes i en længeresigtet plan for modning af AMS såvel som styringen af området. De sidste seks observationer er kategoriseret som prioritet "3" og kan hermed ikke i sig selv have betydning for dataforvanskning og database, men de bør på linje med prioritet 2-observationer indgå i en generel modning af området.

Tabel 1 opgør alle observationer fra undersøgelsen af AMS med angivelse af relevans for udrejsecentrene, tilstand (niveau af validering), prioritet samt indplacering i forhold til PAVA-modellen (Proces, Adfærd, Validering og Arkitektur). Figur 6 illustrerer fordelingen af observationer på tværs af AMS.

Figur 6. Observationer på tværs af AMS-processen



Tabel 1. Overblik over observationer identificeret i forbindelse med undersøgelsen af AMS

#	Titel	Udrejsecenter	Tilstand*	Prioritet (1-3)**	PAVA (delområde)
1	Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG	KHG	3. Valideret	1	Arkitektur
2	Uklar proces for tilmelding og tilkobling af nye registreringsenheder	KHG og SJM	3. Valideret	1	Governance
3	Uhensigtsmæssig placering af streghedescanner (uden biometri)	KHG	3. Valideret	2	Arkitektur
4	Manglende organisatorisk forankring af proces for håndtering af incidents	KHG og SJM	3. Valideret	2	Governance
5	Lav kritikalitetsscore	KHG og SJM	3. Valideret	2	Governance
6	Uklart procesejerskab for AMS-processen	KHG og SJM	3. Valideret	2	Governance
7	Uklart systemejerskab for AMS-komplekset	KHG og SJM	3. Valideret	2	Governance
8	Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere	KHG og SJM	3. Valideret	2	Adfærd
9	Anti-passback ikke implementeret for streghedekort	KHG og SJM	3. Valideret	2	Validering/Kontrol
10	Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentre	KHG og SJM	3. Valideret	2	Adfærd
11	Periodevist åbne døre ved personsłuse	SJM	3. Valideret	2	Adfærd
12	Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre	KHG og SJM	3. Valideret	2	Validering/Kontrol
13	Mangelfuld automatisk advisering ved driftsproblemer	KHG og SJM	2. Dokumenteret	2	Arkitektur
14	Anti-passback ikke aktiveret for biometriske kort	KHG	3. Valideret	2	Validering/Kontrol
15	Fejlregistreringer ved bruger meldt som udeblevet	SJM	3. Valideret	3	Validering/Kontrol
16	Kort slettefrist for øvrige logoplysninger i driftsmiljøet	KHG og SJM	2. Dokumenteret	3	Arkitektur
17	Forkert brug af datamodel (fx brug af statuskoder i beboers navnefelt)	KHG	3. Valideret	3	Adfærd
18	Uhensigtsmæssige roller og adgange i relation til ændring af stamdata	KHG	3. Valideret	3	Validering/Kontrol
19	Mangelfuldt testmiljø	KHG og SJM	3. Valideret	3	Arkitektur
20	Datatab ved nedbrud eller menneskelige fejl	KHG og SJM	0. Valideret afhjulpet	1	Arkitektur
21	Problemer ved systemopdatering og genstart	KHG og SJM	0. Valideret afhjulpet	1	Arkitektur
22	Risiko for datatab, når serveren er utilgængelig for online registreringsenheder	KHG og SJM	0. Valideret afhjulpet	1	Arkitektur
23	Manglende bekræftelse på beskedmodtagelse	KHG og SJM	0. Ingen problematik observeret	1	Arkitektur
24	Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data	KHG og SJM	0. Ingen problematik observeret	1	Arkitektur
25	Dobbeltregistreringer på meldestandere	KHG og SJM	0. Ingen problematik observeret	3	Adfærd

*) "Tilstand" angiver, i hvilken grad observationen er underbygget. 1. "Tese" angiver, at observationen ikke er underbygget, udover anekdotisk niveau, i forbindelse med de anvendte metoder på området. 2. "Dokumenteret" angiver, at observationen er blevet underbygget gennem undersøgelsen, fx via interview, besigtigelse, analyse eller anden aktivitet. 3. "Valideret" angiver, at observationen er dokumenteret og valideret gennem metoderne i denne undersøgelse, fx via interview, besigtigelse, analyse eller anden aktivitet. 0. "Valideret afhjulpet" angiver, at observationen er valideret, og at der er foretaget en aktivitet til afhjælpning af risiko for dataforvanskning. 0. "Ingen problematik observeret" angiver, at observationer tidligere nævnt (fx i faktaark) ikke har kunnet genfindes i undersøgelsen **Prioritet er opgjort i en skala i forhold til væsentligheden i at håndtere den tilknyttede risiko for dataforvanskning.

3.2 Proces

Dette afsnit præsenterer og beskriver den samlede proces, som AMS understøtter. Procesrammen (figur 7) udgør et samlet overblik og en struktur, som opdeler AMS i delprocesser. På den måde er procesdiagrammet både en overordnet struktur og en referenceramme for de enkelte afsnit i rapporten.

3.2.1 Overordnet overblik over processen

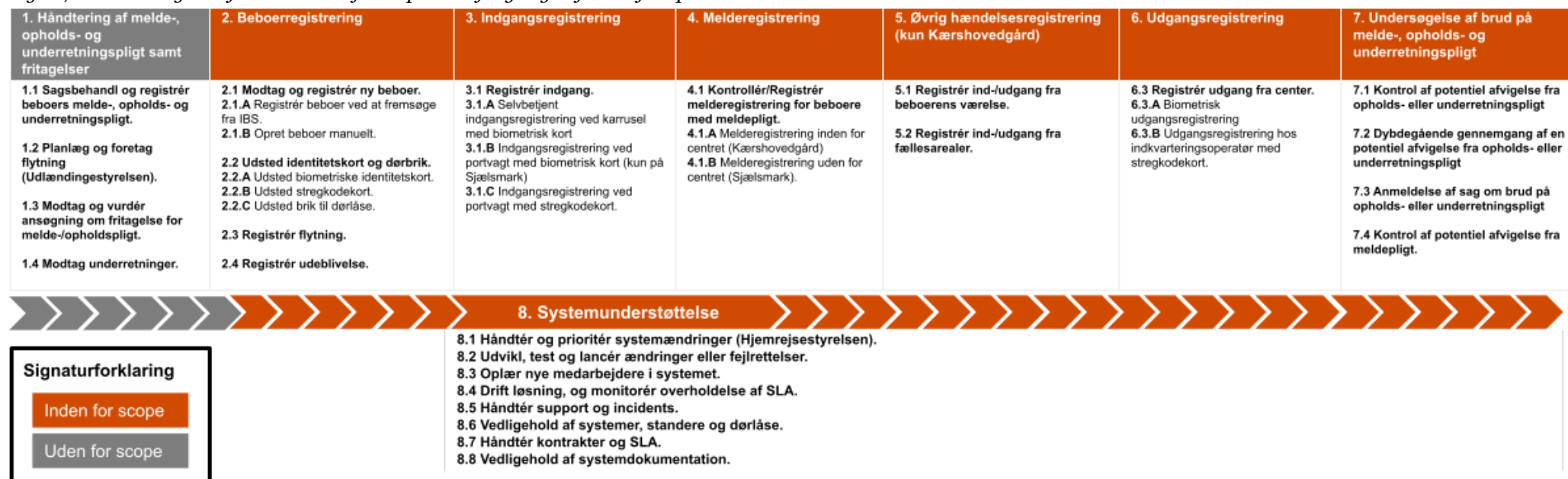
AMS kan inddeles i grupper af delprocesser, som hver fremgår af figur 7:

- Én delproces relateret til, men ikke direkte understøttet af, AMS (se delproces 1), som omhandler håndtering af melde-, opholds- og underretningspligt samt fritagelser herfra. Denne delproces er uden for analysens genstandsfelt og beskrives kun overordnet med det formål at give kontekst til de øvrige delprocesser, som er inden for genstandsfeltet.

- Seks delprocesser, der relaterer sig til arbejdsgangene, som er direkte understøttet af AMS (se delproces 2-7).
- En gruppe understøttende aktiviteter, der relaterer sig til selve systemunderstøttelsen af AMS, og som er samlet under én delproces (se delproces 8).

Procesrammen gennemgås i separate underafsnit, som hver især beskriver en delproces i AMS eller en samling aktiviteter relateret til systemunderstøttelsen. Procesrammen, som præsenteres i dette afsnit, vil også blive benyttet i senere afsnit i rapporten til at gennemgå de andre elementer i PAVA-rammeverket (Adfærd, Validering, Arkitektur og til sidst Governance).

Figur 7. Procesdiagram for AMS med fokus på arbejdsgange i form af delprocesser



3.2.2 Delproces 1. Håndtering af melde-, opholds- og underretningspligt

Delproces 1 er ikke en del af genstandsfeltet for undersøgelsen, idet processen relaterer sig til forberedende aktiviteter for den enkelte beboer, der ikke har direkte relevans for risikoen for dataforvanskning i AMS. Delprocessen gennemgås dog her som indgang til og kontekst for at forstå arbejdsgangene i de efterfølgende delprocesser.

Procestrin 1.1 Sagsbehandl og registrér beboers melde-, opholds- og underretningspligt

HJEMSTs sagsbehandlere i teamet for ”Motivationsfremmende foranstaltninger” (MOT) står for at behandle sager om kommende beboere for at træffe afgørelse om, hvorvidt den kommende beboer skal have henholdsvis melde-, opholds- og underretningspligt. Stort set alle beboere tildeles melde- og opholdspligt, mens underretningspligt kun tildeles udlændinge, der er udvist ved dom, udlændinge, der er på tålt ophold samt fremmedkrigere og udlændinge, der anses for at være til fare for statens sikkerhed.

Når der er truffet afgørelse om beboerens pligter, forkyndes denne for beboeren, og afgørelserne registreres i sagsbehandlingssystemet ”Public 360”.

Procestrin 1.2 Planlæg og foretag flytning (US)

Når medarbejdere i MOT hos HJEMST har truffet afgørelse om beboerens pligter, står US' medarbejdere i kontoret for indkvarteringsvilkår for at planlægge flytning til et udrejsecenter, herunder lavpraktisk planlægning af beboerens transport til centret. Informationer om flytningen og tidspunktet for flytningen registreres i Indkvarterings- og ydelsesBeregningsSystemet (IBS). Indflytningsdagen markerer startdatoen for beboerens opholdspligt. Kriminalforsorgen driver udrejsecentre KHG og SJM på baggrund af en operatørkontrakt med US. Kriminalforsorgen har adgang til IBS, hvorfra medarbejderne kan trække oplysninger på beboere, der skal bo på centret.

Procestrin 1.3 Modtag og vurdér ansøgning om fritagelse for melde-/opholdspligt

Beboere kan i forskellige tilfælde få fritagelse for melde- og opholdspligten, hvis de forinden har bedt om lov til dette. Eksempelvis beder beboerne om fritagelse, hvis de skal overnatte hos familie. Hvis en beboer er fritaget for sin melde-/opholdspligt, vil denne ikke blive anmeldt for overtrædelse af pligten i fritagelsesperioden.

Procestrin 1.4 Modtag underretninger

Beboere med underretningspligt skal give underretning, hvis de er uden for centret mellem kl. 23 og 06. Underretningen gives via et særligt telefonnummer, hvor beboeren skal indtaste sit PersonID, via hjemmesiden ”nyidanmark.dk” eller personlig underretning til centeret.

3.2.2 Delproces 2. Beboerregistrering

Beboerregistreringen foregår på udrejsecentre. Denne opgave varetages af Kriminalforsorgen på det enkelte udrejsecenter i henhold til den indgåede operatørkontrakt.

Procestrin 2.1 Modtag og registrér ny beboer

Der er to forskellige tilgange til at modtage og registrere beboere på udrejsecentre. Tilgangene er beskrevet nedenfor under punkt 2.1.A og 2.1.B. Afsnit 3.4 beskriver graden af kontroltryk i forhold til beboeroprettelsen på henholdsvis SJM og KHG.

Procestrin 2.1.A Registrér beboer ved at fremsøge fra IBS

Hvis der inden modtagelsen af en beboer er foretaget en korrekt oprettelse af beboeren i kontoret for indkvarteringsvilkår i Udlændingestyrelsen (jf. trin 1.2), vil beboerens oplysninger i IBS kunne fremsøges via et særskilt skærmbillede i AMS i forbindelse med modtagelse af beboeren på centret. Ved denne type oprettelse indhentes der stamoplysninger på personen fra IBS. IBS henter stamoplysningerne fra personregisteret om udlændinge, CARL2. Medarbejderen skal herefter supplere med yderligere oplysninger i AMS (fx beboerens værelsesnummer), inden beboeren er færdigregistreret.

Procestrin 2.1.B Opret beboer manuelt

Hvis der ikke inden modtagelsen af en ny beboer er oprettet stamdata på beboeren i IBS, er det muligt at oprette beboeren manuelt, ved at medarbejderen selv indtaster de relevante stamoplysninger. Disse oplysninger inkluderer bl.a. beboerens fornavn, efternavn og nationalitet. Herudover skal der manuelt sættes kryds ved funktionerne ”anti-passback” og ”hændelser på nøglen” (sidstnævnte kun på KHG). Hvis hændelser på nøglen er aktiveret, vil brugen af nøglebrikken på offline døråbner på KHG også fremgå i loggen. Anti-passback er en kontrolmekanisme til passager ud og ind af udrejsecentre (nærmere beskrevet i afsnit 3.4).

Procestrin 2.2 Udsted identitetskort og dørbrik

I forbindelse med modtagelse af beboeren udstedes der identitetskort og eventuel dørbrik til beboeren. Der udstedes både et identitetskort baseret på biometri og et stregekodekort.

Procestrin 2.2.A Udsted biometriske identitetskort

Biometriske identitetskort udstedes på både KHG og SJM som udgangspunkt til alle beboere med et læsbart fingeraftryk, og det er samtidig den foretrukne måde at identificere beboerne på i de senere delprocesser ”3. Indgangsregistrering”, ”4. Melderegistrering” og ”6. Udgangsregistrering”. I nogle tilfælde har udstedelsen af de biometriske kort dog været sat på pause, hvis et udrejsecenter er løbet tør for biometriske kort i en kort periode. Det biometriske identitetskort oprettes ved at registrere beboerens fingeraftryk med en fingeraftrykslæser, der sidder på selve kortet. Herefter kodes de biometriske data ind på kortet med en særskilt ”bordkoder” til de biometriske kort, hvorefter beboerens stamdata indlæses fra AMS på selve kortet med en særskilt bordkoder til dette. Sluttelig testes med en ”førstegangsscanner” for at sikre, at data er oprettet korrekt på det nye kort. Når beboerne flytter, og der kommer nye til, kan kortene genbruges, men det kræver, at de bliver sendt til ”rens” af data hos kortleverandøren, hvilket kan være en tidskrævende proces.

Procestrin 2.2.B Udsted strekkodekort

Strekkodekort oprettes og udstedes også til beboerne på både KHG og SJM. Strekkodekortene fungerer som et alternativ, hvis de biometriske identitetskort ikke kan anvendes. (Fx kan det være svært at aflæse fingeraftryk i regnvejr). Desuden er der en meget lille gruppe af beboere, som af forskellige årsager ikke kan få aflæst deres fingeraftryk (fx hvis fingeraftrykket er nedslidt). Ved udstedelse af strekkodekort tages et billede af beboeren. Billedet printes på beboerens kort sammen med en unik strekkode. Strekkodekortene kan også renses og genbruges, og dette tager kortere tid, end tilfældet er for de biometriske kort, da det kan ske på selve udrejsecentret.

Procestrin 2.2.C Udsted brik til dørlåse

På både KHG og SJM udstedes der elektroniske ”brikker” til åbning af dørlåsene på beboernes værelser. På KHG kan disse brikker også anvendes til elektroniske dørlåse ved døre i fællesarealerne. Disse brikker kan sammenlignes med fysiske nøgler. Dog kan en brik omkodes meget nemt, alt efter hvilke adgange beboeren skal have, hvorimod der både skal laves nye fysiske nøgler og skiftes lås, hvis en fysisk nøgle mistes. Det er kun på KHG, at brikker til dørlåse er integreret med AMS. På SJM anvendes et andet og fra AMS afkoblet system til kodning af brikkerne.

Procestrin 2.3 Registrér flytning

Når en beboer skal flytte fra et udrejsecenter, afleverer beboeren sine identitetskort og brik til dørlåse. Beboeren registreres herefter som fraflyttet i AMS.

Procestrin 2.4 Registrér udeblivelse

Hvis en beboer har opholdt sig uden for udrejsecentret i mere end 72 timer, registreres en beboeren automatisk som udeblevet, og beboeren vil ikke længere være registreret som indkvarteret på udrejsecentret. Beboeren vil således heller ikke efterfølgende kunne foretage en indgangsregistrering. Hvis beboeren ikke oplever at kunne komme ind på udrejsecentret, vil beboeren skulle tage kontakt til portvagten.

3.2.2 Delproces 3. Indgangsregistrering

Indgangsregistrering foregår på udrejsecentrene, og opgaven er enten selvbetjent eller betjent af Kriminalforsorgens medarbejdere på KHG og SJM.

3.1 Registrér indgang

Ved indgangsregistrering til centrene er der tre forskellige muligheder: selvbetjent indgang med biometrisk kort og indgang ved medarbejderen med enten biometrisk kort eller strekkodekort:

Procestrin 3.1.A Selvbetjent indgangsregistrering ved karrusel med biometrisk kort

På både KHG og SJM kan beboerne foretage indgangsregistrering gennem en ubemandet karrusel ved anvendelse af deres biometriske kort. En beboer skal bruge sit kort ad to omgange ved indgang: Først registrerer beboeren sit kort og får via karrusellen adgang til et lille ”mellemrum” under manuelt opsyn, hvor der er plads til maks. 1-2 personer (se også afsnit 3.4.1 om validerings- og kontrolmæssige observationer på tværs af AMS-processen). Herefter skal beboeren igen registrere sit kort for at komme ind på selve udrejsecentret og hermed ud af ”mellemrummet”. Hvis beboerens kort er løbet tør for strøm i ydertimerne, hvor porten ikke er bemanded, er det planen, at beboeren i fremtiden skal kunne lave en lynopladning ved en oplader direkte i porten. Dette er dog ikke muligt i dag, hvor beboeren i dette tilfælde må vente på en medarbejder.

Procestrin 3.1.B Indgangsregistrering ved portvagt med biometrisk kort (kun på SJM)

Hvis indgangskarrusellen ikke virker, kan beboeren også foretage en indgangsregistrering hos portvagten. På SJM kan denne alternative indgangsregistrering både ske ved biometrisk kort og med strekkodekort, mens der på KHG kun kan anvendes strekkodekort ved portvagten (se procestrin 3.1.C for indgangsregistreringen med strekkodekort). Indgangsregistreringen ved portvagten med biometrisk kort på SJM foregår, ved at beboeren giver portvagten sit biometriske kort, hvorefter portvagten scanner kortet med en biometrisk håndscanner, og porten

åbner for beboeren. Hvis beboerens kort er løbet tør for strøm, kan beboeren lægge sit kort til opladning hos portvagten.

Procestrin 3.1.C Indgangsregistrering ved portvagt med stregkodekort

Hvis beboeren ikke har et biometrisk kort, hvis det ikke virker, eller hvis det er løbet tør for strøm, kan beboeren også foretage en indgangsregistrering hos portvagten med sit stregkodekort. Dette foregår ved, at beboeren giver portvagten sit stregkodekort, hvorefter portvagten kontrollerer billedet af beboeren på kortet og sammenligner med beboerens ansigt. Herefter scanner portvagten beboerens kort med en håndscanner til stregkodekort og lukker beboeren ind på udrejsecentret.

3.2.2 Delproces 4. Melderegistrering

Procestrin 4.1 Kontrollér/Registrér melderegistrering for beboere med meldepligt

Melderegistreringen varetages af HJEMSTs medarbejdere på KHG og SJM. Meldepligten betyder, at en udlænding skal møde hos HJEMST på nærmere angivne tidspunkter med henblik på løbende at sikre, at myndighederne har kendskab til udlændingens opholdssted.

4.1.A Melderegistrering inden for centret (KHG)

På KHG foregår melderegistreringen inden for indhegningen på udrejsecentret, og det kræver således ikke en udgangsregistrering fra udrejsecentret for at foretage melderegistreringen. Der er både opsat meldestandere til melderegistrering med biometriske kort og en meldestander til melderegistrering med stregkodekort. Hvis stregkodekortet anvendes, skal det ske ved aflevering af kortet til en medarbejder fra HJEMST, der forestår selve registreringen ved scanning af kortet. Det er de samme kort, som anvendes til henholdsvis passage ind og ud af udrejsecentrene og registrering af meldepligt.

4.1.B Melderegistrering uden for centret (SJM)

På SJM foregår melderegistreringen uden for udrejsecentrets indhegning, og det kræver således en udgangsregistrering fra udrejsecentret for at foretage melderegistreringen samt en indgangsregistrering, når beboeren skal ind på centret igen. Der er både opsat meldestandere til melderegistrering med biometriske kort samt en meldestander til melderegistrering med stregkodekort. Hvis stregkodekortet anvendes, skal det ske foran en af HJEMSTs medarbejdere for at sikre, at beboeren er den samme som personen, der er afbilledet på kortet. Det er de samme kort, som anvendes til henholdsvis passage ind og ud af udrejsecentrene og registrering af meldepligt.

3.2.2 Delproces 5. Øvrig hændelsesregistrering

Selvom der er elektroniske nøglebrikker og dørlåse på SJM, overføres registreringer fra dørlåsene på SJM ikke til AMS. På SJM benyttes et system, der er afkoblet fra AMS. I delproces 5 fokuseres der derfor på KHG og på den øvrige hændelsesregistrering på udrejsecentret. Årsagen er, at der er kobling mellem AMS og brikkerne til administration af adgange på KHG.

Procestrin 5.1 Registrér ind-/udgang fra beboerens værelse

Når en beboer skal bevæge sig ind og ud af sit værelse på KHG, anvendes det biometriske kort - eller alternativt en elektronisk nøglebrik, hvis beboeren ikke har et biometrisk kort. Hvis beboerens adgangsrettigheder skal ændres, skal kortet omkodes, hvorved data overføres til AMS.

Procestrin 5.2 Registrér ind-/udgang fra fællesarealer

Når en beboer skal bevæge sig gennem døre ved fællesarealer på KHG, er der også elektroniske dørlåse, som kan anvendes med enten det biometriske kort eller nøglebrikken for beboere uden et biometrisk kort.

3.2.2 Delproces 6. Udgangsregistrering

Procestrin 6.1 Registrér udgang fra center

Udgangsregistreringen følger samme mønster som indgangsregistreringen, og den beskrives derfor ikke i detaljer her (se den foregående delproces 3 for nærmere beskrivelse):

6.1.A Selvbetjent udgangsregistrering ved karrusel med biometrisk kort

Denne passage sker på samme måde som selvbetjent indgangsregistrering ved karrusel med biometrisk kort, Forskellen er blot, at beboeren bevæger sig ud af centret i stedet for ind i centret.

6.1.B Udgangsregistrering ved portvagt med biometrisk kort

Denne passage sker på måde som indgangsregistrering ved portvagt med biometrisk kort, Forskellen er blot, at beboeren bevæger sig ud af centret i stedet for ind i centret

6.1.C Udgangsregistrering ved portvagt med stregkodekort

Denne passage sker på samme måde som indgangsregistrering ved portvagt med stregkodekort, Forskellen er blot, at beboeren bevæger sig ud af centret i stedet for ind i centret

3.2.2 Delproces 7. Undersøgelse af overtrædelse af melde-, opholds- og underretningspligt

HJEMST kontrollerer løbende, om der er sket overtrædelse af de pligter, som beboerne er pålagt. Selve kontrollen er baseret på data fra AMS, som analyseres og visualiseres i it-plattformen ”QlikView”. HJEMST’s sagsbehandlere foretager herefter en gennemgang af visningerne i QlikView, som sammenholdes med øvrige oplysninger fra bl.a. sagsbehandlingssystemet ”Public360”, fx vedrørende lovligt fravær. På baggrund af en samlet vurdering af den konkrete sags omstændigheder foretages anmeldelse til politiet for eventuelle overtrædelser af pligter.

Procestrin 7.1 Kontrol af potentiel afvigelse fra opholds- eller underretningspligt i anmeldelseslisten

Anmeldelseslisten i QlikView (også kaldt Salto-log) indeholder en liste over potentielle overtrædelser af opholds- og underretningspligt, som præsenteres for medarbejderne i MOT i HJEMST. Hver række i anmeldelseslisten repræsenterer sammenhængen mellem en udgang og en indgang efter en række regler. Disse koblingsregler er ikke inden for genstandsfeltet af analysen, men disse inkluderer fx:

- **Fejlkobling:** Det fremhæves som en fejlkobling i denne undersøgelse, hvis en person går ud to gange i træk uden at gå ind, eller hvis en person går ind to gange i træk uden at gå ud. Andre typer af fejlkoblinger behandles ikke i denne undersøgelse.
- **Behandlet:** På hver række er der en indikation af, om sagen allerede er behandlet. Dette sker ved et opslag i sagsbehandlingssystemet ”Public 360” på baggrund af nogle givne parametre.

Procestrin 7.2 Dybdegående gennemgang af en potentiel afvigelse fra opholds- eller underretningspligt

Hvis en beboer er markeret med en potentiel overtrædelse på anmeldelseslisten, undersøger medarbejderen i MOT sagen nærmere, herunder ved opslag i sagsbehandlingssystemet Public 360 og i IBS med henblik på at kontrollere, om der fx er registreret fritagelser for beboeren på det pågældende tidspunkt, indlæggelser eller andre hændelser, der kan begrunde manglende anmeldelse, samt eventuelle opslag i Salto-log rådata eller hændelseslog med henblik på undersøgelse af fx fejlkoblinger. Vurderingen munder i sidste ende ud i, at der enten foretages en anmeldelse af sagen til Politiet (jf. procestrin 7.3), eller at sagen ikke anmeldes.

Procestrin 7.3 Anmeldelse af sag om brud på opholds- eller underretningspligt

Hvis medarbejderen vurderer, at der er grundlag for anmeldelse af en beboer for brud på opholds- eller underretningspligten, udarbejdes der en anmeldelse til politiet vedlagt relevant dokumentation for overtrædelsen for den pågældende beboer. Denne dokumentation fremsendes til politiet som bilag sammen med beskrivelse af grundlaget for anmeldelsen af beboeren. Primo oktober til primo december 2020 har Hjemrejsestyrelsen fremsendt udskrift af hændelsesloggen som del af ovennævnte dokumentation. Hændelsesloggen er et databaseudtræk af hændelser direkte fra AMS, der opsættes fra brugergrænsefladen (læs mere om hændelsesloggen i afsnit 3.5.1, hvor arkitekturen gennemgås). Der henvises også til anbefaling 1 om dataforvanskning i forbindelse med anvendelse af data fra offlineenheder, da hændelsesloggen også inkluderer data fra offlineenheder).

Procestrin 7.4 Kontrol af potentiel afvigelse fra meldepligt

Behandling af sager om overtrædelse af meldepligt sker på baggrund af Salto-Rådatalog, der via et særskilt værktøj kobler data op imod de konkrete ugedage, hvor beboeren skal afgive meldepligt. På baggrund heraf genereres en anmeldelsesliste over potentielle overtrædelser. På samme måde som for opholds- og underretningspligt undersøger sagsbehandleren sagsbehandlingssystemet Public 360 og IBS for oplysninger om lovligt forfald, hvorefter sagsbehandleren vurderer, om der er grundlag for anmeldelse. Visning af potentielle brud på meldepligten er ikke integreret i QlikView. Hjemrejsestyrelsen arbejder på en løsning, hvor anmeldelseslisten for potentielle overtrædelser af meldepligt integreres i QlikView på samme vis som for potentielle overtrædelser af opholds- og underretningspligt.

3.2.2 Støtteprocesser relateret til systemunderstøttelse af AMS

I dette underafsnit beskrives de støtteprocesser, der sikrer den nødvendige systemunderstøttelse for AMS (beskrevet i delproces 1-7). For en overordnet gennemgang af systemejrolleren se afsnit 3.6 om governance. Dette afsnittet beskriver disse processer overordnet og samlet på tværs af AMS-komplekset. Dog er disse processer ikke samlet under ét systemejerskab, hvilket beskrives nærmere i førnævnte afsnit 3.6. Generelt for støtteprocesserne kan det bemærkes, at de hver især understøttes på mange forskellige måder, som overordnet kan inddeles som følger:

- Systemunderstøttelse af hardwaremæssige (fysiske) dele af AMS på KHG og SJM (fx forskellige stregkodekort, biometriske kort og registreringsenheder på centrene)

- Systemunderstøttelse af hardwaremæssige (fysiske) dele af AMS på KHG og SJM, som er specifikt relateret til meldestanderne
- Systemunderstøttelse af netværk, server og server-operativsystem, som AMS-software afvikles på hos SIT
- Systemunderstøttelse af anskaffet tredjepartsapplikationssoftware, som indgår i AMS-komplekset (fx Salto ProAccess Space og Microsofts SQL)
- Systemunderstøttelse af egenudviklet applikationssoftware, som indgår i udtræk, transformation og indlæsning af data i hele dataflowet (fx egenudviklede jobs til at trække data ud fra hændelsesfiler og lægge disse data ind i databaser, og SQL-kode udviklet som stored procedures på databaser til at sammenkoble data fra forskellige kilder).

I de følgende underafsnit beskrives de forskellige støtteprocesser helt generelt, men hvor det er relevant, refereres der til ovennævnte inddelinger.

Støtteproces 8.1 Håndtér og priorité systemændringer (HJEMST)

US eller HJEMST kan melde nye ændringsønsker ind til UIM's Koncern IT (UIM-KIT). UIM-KIT har implementeret en ændringshåndterings- proces, der driver håndteringen og prioriteringen af disse ændringsønsker. Ønsker til ændringer screenes ifølge UIM-KIT i et "change advisory board" og lægges derefter til indstilling for ledelsen, hvorefter UIM-ledelsen prioriterer og godkender ændringsønskerne.

Støtteproces 8.2 Udvikl, test og lancér ændringer eller fejlrettelser

Prioriterede ændringsønsker implementeres på forskellige måder, alt efter hvilken del af det samlede AMS-kompleks der er tale om.

Såfremt en ændring relaterer sig til hardware på et udrejsecenter (fx opsætning af en ny karrusel til ind-/udgangsregistrering), håndteres dette via bilateral kommunikation mellem Kriminalforsorgens medarbejdere på det respektive udrejsecenter og dette udrejsecenters leverandører (fx ACTAS og Sanistål for SJM). Kriminalforsorgen skal samtidig sikre økonomisk dækning via den bevillingshavende myndighed, som er US. Denne proces er ikke formaliseret og beror på personlig kontakt mellem medarbejdere på centrene, leverandørerne og Udlændingestyrelsen (i forhold til finansiering).

For meldestandere foregår den løbende lancering af ændringer i en løbende og uformaliseret dialog mellem HJEMSTs medarbejdere og leverandøren på det pågældende udrejsecenter. Her er det blot HJEMSTs medarbejdere, der er involveret frem for Kriminalforsorgens medarbejdere. Ændringerne til meldestanderne (fx opsætning af nye standere) finansieres af HJEMST.

Hvis en ændring relaterer sig til netværk, server og operativsystem hos SIT (fx hvis der er behov for servere med mere kapacitet), laver UIM-KIT en ændringsanmodning til SIT, der gennemfører en standard ændringshåndteringsproces i SIT's It Service Management (ITSM)-system, ServiceNow. ITSM-systemet hos UIM-KIT er integreret med ITSM-systemet hos SIT således, at eventuelle tilbageløb i forbindelse med implementering kommunikerer tilbage til UIM-KIT på den "ticket", som repræsenterer ændringen. Nye ændringer testes ikke i et præproduktionsmiljø inden udrulning til AMS, og ændringer rulles således direkte ud i produktionsmiljøet. Historisk set er langt de fleste ændringer standardændringer, fx patching (en mindre opdatering) af servere hos SIT, der følger en helt fast proces.

Hvis en ændring relaterer sig til tredjepartsapplikationssoftware (her er det primært relevant at tale om Salto ProAccess Space, som er den tredjepartsløsning, der understøtter hele adgangskontrollen, indsamlingen af data fra registreringsenheder og opsætningen af brugere på centrene), udføres ændringer i opsætningen eller konfigureringen af systemet af Sanistål, som distribuerer Salto ProAccess Space i Danmark. Salto ProAccess Space er som udgangspunkt anskaffet som et standardsystem, men der er eksempler på lokale tilretninger, såsom udviklingen af en integration til IBS til indhentning af stamdata på beboeren fra CARL2 i forbindelse med beboeroprettelsen.

Endelig er der eksempler på, at man i systemunderstøttelsen har lavet forskellige egenudviklede ændringer til databaser, som indgår i udtræk, transformation og inddatering af data fra registreringsenhederne i løbet af dataflowet (læs mere om dette i afsnit 3.5 om arkitekturen). Disse ændringer implementeres i forbindelse med UIM Koncern IT's ændringshåndteringsproces. Nye ændringer testes ikke i et præproduktionsmiljø uden for AMS inden idriftsættelse. Ændringer rulles således direkte ud i produktionsmiljøet i AMS. Hvis der er sket ændringer i et udrejsecenters setup (fx hvis der er blevet tilføjet en ny registreringsenhed), skal der i forbindelse med disse ændringer laves en ny ændringsanmodning til UIM-KIT om at implementere, at alle registreringer fra denne registreringsenhed også inkluderes i de daglige udtræk fra Salto-databasen, hvis disse data skal med videre i datastrømmen, der til sidst ender i MOT-medarbejdernes overblik i QlikView (jf. delproces 7 i AMS-processen). Hvis der ikke laves en ændringsanmodning til UIM-KIT, kommer data fra registreringsenheden ikke med i AMS. (Se også afsnit 3.6 i forhold til observationer om fokus på driftssikkerhed, systemejerskab mv.)

Støtteproces 8.3 Oplær nye medarbejdere i systemet

Oplæring af nye medarbejdere omhandler i denne sammenhæng den oplæring, der sker ude på udrejsecentrene SJM og KHG. Oplæring af medarbejdere i anvendelsen af systemet sker primært i et samarbejde mellem udrejsecentret og distributøren af Salto ProAccess Space i Danmark, Sanistål. Herudover har der i nogle tilfældet været afholdt oplæring af medarbejdere i systemet af medarbejdere i den ansvarshavende styrelse (tidligere Udlændingestyrelsen og nu HJEMST). Læs mere om analysens observationer relateret til oplæring af medarbejdere i afsnit 3.3.

Støtteproces 8.4 Drift løsning, og monitorér overholdelse af SLA

Systemunderstøttelse af hardwaremæssige (fysiske) dele af AMS på KHG og SJM driftes og overvåges af Kriminalforsorgen, som har en operatørkontrakt med US. Overvågningen foregår manuelt, ved at de fleste af enhederne visuelt og via lyd tilkendegiver, hver gang der sker en succesfuld registrering. Kriminalforsorgens medarbejdere kan således selv konstatere det, hvis der opstår gentagne fejl, som ikke umiddelbart skyldes enkeltstående udfordringer med beboernes kort. Der er i dag ikke opsat nogen driftsalarmer med dashboard eller notifikationer til medarbejderne ude på centrene, hvis registreringsenheder registrerer problemer (fx manglende forbindelse til serveren). Medarbejderne er således afhængige af beboernes feedback, af at de selv fysisk kan se registreringsenhederne, eller af at de rutinemæssigt kontrollerer logoplysninger i AMS. For meldestandere foregår den løbende overvågning på samme vis. Her er det blot HJEMSTs medarbejdere, der manuelt overvåger standerne.

SIT drifter og overvåger netværk, servere og operativsystem på servere, mens UIM-KIT drifter og overvåger tredjepartsapplikationssoftware, der er installeret på servere hos SIT – nærmere bestemt Salto ProAccess Space og Windows MSSQL. UIM-KIT drifter og overvåger desuden egenudviklet SQL- og PowerShell-kode.

SIT og UIM-KIT har et fælles setup for overvågning, hvor der i Microsoft System Center Operations Manager (SCOM) er blevet opsat overvågning og alarmer i forhold til servernes kapacitet (RAM, CPU og opbevaringsplads). Overvågning af applikationssoftware håndteres alene af UIM-KIT i systemet Capmon.

Hvis der i de automatiske alarmer og overvågningsprocedurer identificeres en fejl, som er relevant for personer hos HJEMST, Udlændingestyrelsen og/eller Kriminalforsorgen, kommunikeres det ud via e-mail. Der er en dedikeret mailadresse hos HJEMST, hvor HJEMST orienteres om driftsforstyrrelser, når det vurderes relevant. Der er dog ikke nogen alarmer, der udløser automatiske notifikationer til andre end UIM-KIT og SIT.

Der foretages ikke formaliseret overvågning af systemets opetid holdt op imod en SLA-aftalt tilgængelighed for systemet mellem SIT og UIM-KIT. UIM-KIT har ingen aftalte SLA'er med HJEMST, US eller Kriminalforsorgen.

Støtteproces 8.5 Håndtér support og incidents

Ligesom med ændringshåndtering håndteres supportspørgsmål og fejlmeldinger i de to udrejsecentre i høj grad via bilateral kommunikation mellem Kriminalforsorgens medarbejdere på det respektive udrejsecenter og dette udrejsecenters leverandører (fx ACTAS og Sanistål for SJM). For meldestandere foregår dialogen mellem HJEMSTs medarbejdere og leverandørerne.

UIM-KIT har etableret en standardiseret incident-proces, der dækker over alle de områder, som UIM-KIT varetager, og som skal sikre en sammenhængende incident-håndteringsproces, fra en incident identificeres, til den behandles og løses samt til den efterfølgende håndtering af gentagne, kendte fejl. Processen er dokumenteret og er blevet delt med PwC i forbindelse med nærværende undersøgelse. Under interviewene er det oplyst, at denne proces er taget i anvendelse hos UIM-KIT og i samarbejdet med SIT, men de personer, der har indgået i denne undersøgelse fra Kriminalforsorgen og HJEMST oplyser, at de ikke har været oplyst om processen, og at de derfor endnu ikke følger processen i praksis i forbindelse med incident-håndtering.

Støtteproces 8.6 Vedligehold af systemer, standere og dørlåse

Vedligehold af hardware på KHG og SJM (fx registreringsenheder, elektroniske dørlåse, biometriske kort og stregkodekort) håndteres af Kriminalforsorgen i samarbejde med leverandørerne af de respektive komponenter.

SIT sørger for løbende vedligehold af netværk, servere og operativsystem på servere, mens UIM-KIT opdaterer tredjepartsapplikationssoftware, der er installeret på servere hos SIT – nærmere bestemt Salto ProAccess Space og Windows MySQL, som de respektive systemleverandører vedligeholder. UIM-KIT vedligeholder desuden egenudviklet SQL- og PowerShell-kode.

Støtteproces 8.7 Håndtér kontrakter og SLA

US håndterer kontrakter og allonger relateret til drift af de to udrejsecentre. Kriminalforsorgen har opgaven med at drifte udrejsecentrene KHG og SJM. Opgaven er defineret og styret via en operatørkontrakt, som er indgået mellem Kriminalforsorgen og Udlændingestyrelsen i december 2020. Operatørkontrakten opdateres typisk hvert år, og hvis der ikke foreligger en opdateret kontrakt ved kontraktens udløb, er der praksis for at oprette allonger til den eksisterende kontrakt i den mellemliggende periode, indtil en ny kontrakt er indgået.

Støtteproces 8.8 Vedligehold af systemdokumentation

Der er ikke en formaliseret proces for løbende opdatering af systemdokumentation for det samlede AMS-kompleks. Opgaven er i høj grad delt ud på de forskellige dele af systemkomplekset:

- Processen for løbende dokumentation af de hardwaremæssige (fysiske) dele af AMS på KHG og SJM (fx forskellige stregkodekort, biometriske kort og registreringsenheder på centrene) er ikke formaliseret, og der vedligeholdes således ikke et overblik over enhedernes fysiske placering på et kort over udrejsecentrene eller enhedernes tekniske specifikationer. Opgaven håndteres således i praksis af leverandørerne (Actas, Holstebro Låseteknik og Sanistål), der har kendskab til de tekniske specifikationer på alle enheder, der er opsat på centrene. Dette overblik vedligeholdes dog ikke et centralt sted med adgang for Kriminalforsorgens medarbejdere.
- SIT sørger løbende for dokumentation af netværk, servere og server-operativsystemer, der indgår i AMS, i tæt samarbejde med UIM-KIT. Da ændringsprocessen er så formaliseret for netværk, servere og server-operativsystemer, vil det være muligt at finde den nyeste dokumentation for dette i SIT's ITSM-værktøj.
- UIM-KIT står for at holde systemdokumentation opdateret for applikationssoftware, der indgår i AMS, og som installeres på SIT's servere. Denne opgave er ikke formaliseret og knyttet til et fast årshjul, men udføres i stedet efter behov. Der er ikke ét centralt sted, hvor denne type af systemdokumentation løbende opdateres.

3.3 Adfærd

Dette afsnit beskriver de adfærdsmæssige observationer ved brug af AMS, som er afdækket i undersøgelsen. De adfærdsmæssige observationer dækker her over udfordringer identificeret i relation til adfærden hos aktørerne i AMS-processen. Nogle af de observationer, der er gjort i relation til medarbejdernes adfærd, vil blive behandlet i afrapporteringen på kontrolanalysen i afsnit 3.4, i det omfang adfærden alene består i udførelse af kontroller.

Gennemgangen af adfærdsmæssige observationer ved brug af AMS tager udgangspunkt i den overordnede procesramme, som er præsenteret i afsnit 3.2, hvorudfra hver observation knyttes til én eller flere delprocesser (se figur 8). I relation hertil inddeles de fremkomne adfærdsmæssige observationer i følgende tre grupperinger, der vil strukturere de kommende afsnit: 3.3.1 Observationer tværgående for AMS-processen, 3.3.2 Observationer i forbindelse med delproces 2. Beboerregistrering og 3.3.3 Observationer i forbindelse med delproces 3. Indgangsregistrering og 6. udgangsregistrering.

Figur 8. Procesdiagram for AMS med angivelse af observationer



3.3.1 Observationer tværgående for AMS-processen

På tværs af AMS-processen er det observeret, at der er mangelfuld vejledning, oplæring og opfølgning til Kriminalforsorgens medarbejdere, og at der videre end dette forekommer forkert brug af datamodel i AMS.

10. Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentrene	
Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Det er observeret og tilkendegivet, at medarbejdere ikke er tilstrækkeligt oplærte og trænet i anvendelse af brugergrænsefladen i AMS, herunder mangler der i visse tilfælde systemforståelse. Et andet eksempel på disse manuelle fejl er, at det er forekommet, at personalet på udrejsecentrene ikke korrekt har fulgt de anvisninger, der er givet for at sikre en effektiv adgangskontrol og registrering.
Risiko-beskrivelse	Der er risiko for at manglende træning og forståelse af AMS kan medføre menneskelige fejl og uhensigtsmæssigheder i anvendelsen af systemet – fx stamdata, der ligger til grund for den efterfølgende datagenererende proces.
Kendte eksisterende kontroller	Begge udrejsecentre har lokalt været nødsaget til at opbygge processer, materiale og vejledninger til medarbejderne samt at oplære medarbejdere i disse lokalt på centrene. Kriminalforsorgen skal sikre, at systemet anvendes efter hensigten, herunder reagere relevant på fejlkilder, som kan påvirke datakvaliteten for registreringer i AMS samt vejlede beboerne om og bistå dem med anvendelsen af systemet. HJEMST deltager endvidere i faste driftsmøder, der holdes på udrejsecentrene, så HJEMST har en løbende dialog med udrejsecentrene om AMS.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at der implementeres et onboarding-koncept for procedurer og processer samt etableres en proces for løbende opfølgning på viden om samme. Det anbefales hertil, at der formaliseres procedure- og procesbeskrivelser, som dokumenterer best practice for opretholdelse af kontroltrykket samt relevante opfølgningsmekanismer for løbende ajourføring.

17. Forkert brug af datamodel (fx brug af statuskoder i beboers navnefelt)	
Prioritet	3
Udrejsecenter	KHG
Beskrivelse af problemstilling	Der er eksempler på, at medarbejdere bruger navnefeltet i datamodellen som et notefelt til at angive, at en beboer er flyttet fra centret. Fx er en beboers fornavn ændret til "23.08.2018 flyttet" og efternavnet ændret til "Slettet 23.08.2018". Dette vidner om, at brugerne mangler funktionalitet for at sikre, at det kan registreres, hvornår en beboer er flyttet fra et udrejsecenter, og hvornår en beboer er slettet. Der er også eksempler på, at en beboers efternavn er blevet suppleret med information såsom "(BRIK) FRIHEDSBERØVET".
Risiko-beskrivelse	Der er risiko for, at der ikke kan føres sager tilbage i tid for beboere, som ikke længere opholder sig på udrejsecentret, fordi det ikke er muligt at identificere beboeren længere, da navnet på beboeren ikke fremgår i databasen.
Kendte eksisterende kontroller	Det er uvist, om det er muligt at genfinde brugerens identitet ved at hente id'et fra CARL2.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at - det undersøges med leverandøren, om der kan tilføjes ekstra felter i datamodellen og mulighed for at redigere disse felter i brugergrænsefladen. Det bør i den sammenhæng afdækkes, hvad det specifikke brugerbehov er for yderligere felter. - det bliver pålagt, at alle nye beboere oprettes via stamdata fra CARL2 via IBS. - navnefelterne låses for redigering for almindelige brugere, således at kun privilegerede brugere kan redigere disse felter ved særlige undtagelser.

3.3.2 Observationer i forbindelse med delproces 2. Beboerregistrering

I relation til beboerregistrering er det observeret, at anti-passback-kontrol ikke er automatisk aktiveret for manuelt oprettede brugere i AMS, hvorved et biometrisk kort kan anvendes til to på hinanden følgende passager enten ind eller ud af udrejsecentret.

8. Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere	
Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Det er ved besigtigelse (på KHG) observeret, at det testkort, der blev oprettet i forbindelse med besigtigelsen, ikke havde fået slået anti-passback-funktionen til, hvilket resulterede i, at funktionen ikke slog i gennem på registreringsenheder til ind- og udgang (herunder karruseller). Den manglende anti-passback-kontrol skal normalt forhindre fejkoblinger, dvs. inden for denne undersøgelses genstandsfelt gentagne ind- eller udgangsregistreringer. Hvis beboere oprettes manuelt ved registrering, kan det ske, at funktionen ved en menneskelig fejl ikke slås til.
Risiko-beskrivelse	Der er risiko for gentagne fejkoblinger, dvs. ind- og udgangsregistreringer, hvormed data ikke afspejler beboerens reelle adfærd.
Kendte eksisterende kontroller	Det er i dag medarbejderens opgave at sikre, at anti-passback er slået til i forbindelse med oprettelse af brugeren. På SJM er der opsat en yderligere kontrol, idet rettighederne til manuelt at oprette brugere samt ændre i stamdata og dertilhørende rettigheder dér er begrænset til én udvalgt medarbejder med særligt fokus på og ansvar for aktivering af anti-passback.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at det afklares med leverandøren, om det er muligt at foretage en systemændring således, at manuelt oprettede brugere automatisk har aktiveret anti-passback. Det anbefales desuden at nedbringe antallet af manuelle brugeroprettelser (se anbefalinger til observation 17).

3.3.3 Observationer i forbindelse med delproces 3. Indgangsregistrering og 6. Udgangsregistrering

I relation til ind- og udgangsregistrering er det observeret, at dørene ved personslusen på SJM periodevist står åbne.

11. Periodevist åbne døre ved personsluse	
Prioritet	2
Udrejsecenter	SJM
Beskrivelse af problemstilling	Det er observeret, at dørene ved personslusen (ved portvagt) til ind- og udgang på SJM til tider står åbne, da den mekaniske åbne- og lukkemekanisme er langsom.
Risiko-beskrivelse	Der er risiko for at beboere uregistreret kan bevæge sig ind og ud af centret, hvorved data i AMS ikke vil afspejle beboernes reelle færden.
Kendte eksisterende kontroller	Portvagten har ansvaret for at kontrollere, at ingen personer går ind eller ud ad dørene ved personslusen uden at foretage en ind- eller udgangsregistrering.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales enten at opgradere de nuværende mekaniske døråbnere til nogle med en hurtigere åbne- og lukkemekanisme eller at udskifte de mekaniske døre med analoge døre uden åbne- og lukkemekanismer, men med medarbejderbetjent elektronisk lås.

3.3.4 Observationer i forbindelse med delproces 4. Melderegistrering

I relation til melderegistrering er det observeret, at nogle beboere konsekvent foretager melderegistrering på alle meldestandere.

25. Dobbeltregistreringer på meldestandere	
Prioritet	3
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Det er observeret, at nogle beboere foretager dobbeltregistreringer i forbindelse med melderegistrering for at sikre, at deres registrering er korrekt registreret i AMS. I forbindelse med PwC's dataanalyser (jf. afsnit 3.5.2), er det bekræftet, at der er et stort antal dobbelte registreringer ved meldestandere på begge centre, og at dette forekommer signifikant mere på KHG end på SJM (læs mere i kontrol 8 i afsnit 3.5.2).
Risiko-beskrivelse	Der er ikke nogen reel risiko forbundet med, at beboerne foretager to eller flere melderegistreringer på samme tid. Dog har HJEMST oplevet, at det i forbindelse med behandling af anmeldte sager har været kilde til forvirring blandt parterne i den retslige proces, at der har forekommet flere melderegistreringer fra den samme beboer inden for en kort tidsperiode, da dette potentielt kunne indikere, at der var dubletter, som fejlagtigt blev genereret i løbet af dataflowet.
Kendte eksisterende kontroller	Der er ingen kendte kontroller, der afholder beboerne for at anvende meldestanderne flere gange i træk. Der er en kontrol i AMS, der sikrer, at en hændelse ikke kan registreres mere end én gang i databasen (Salto DB), så det kan udelukkes, at der skulle være tale om dobbeltregistreringer, som er genereret i systemet ved en fejl.
Anbefalinger til yderligere tiltag	
Ingen yderligere anbefalinger	Der er ikke yderligere anbefalinger til denne observation, givet at det ikke er problematisk, hvis en beboer foretager mere end én melderegistrering i træk for at sikre, at registreringen er korrekt registreret i AMS.

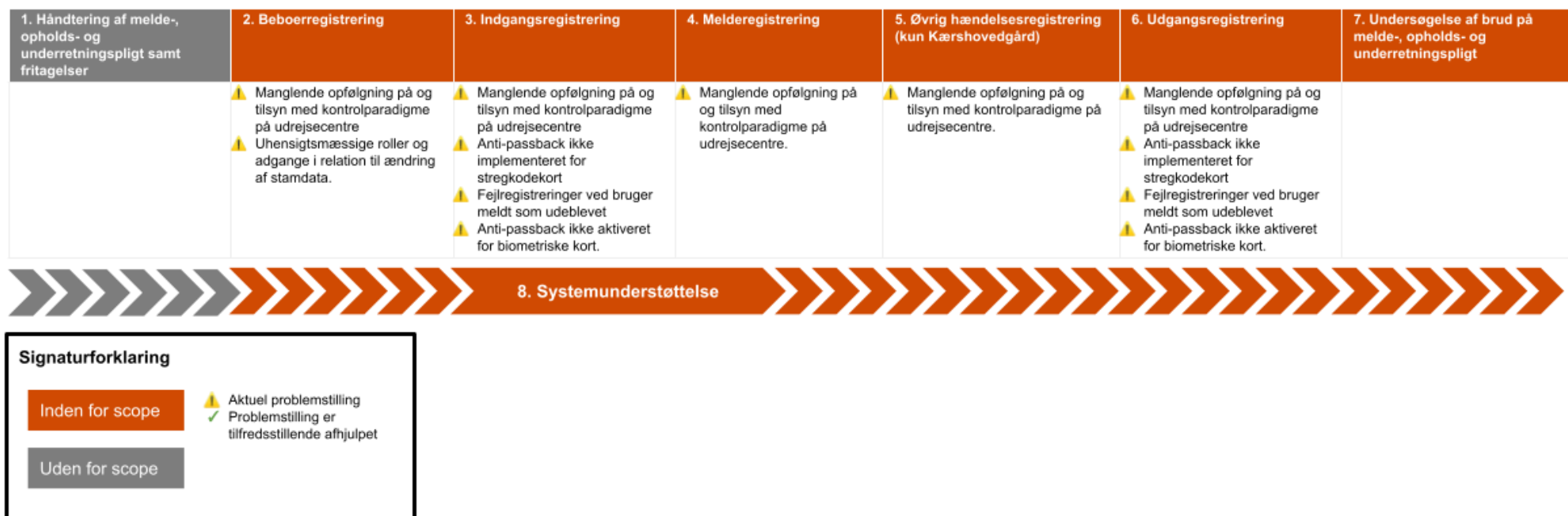
3.4 Validering og kontrol

Dette afsnit præsenterer observationer relateret til validering og kontrol, som undersøgelsen af AMS har ført til. Gennemgangen af observationer og udfordringer tager udgangspunkt i den overordnede procesramme, som er præsenteret i afsnit 3.2, hvorudfra hver observation knyttes til en eller flere delprocesser (se Figur 9). Der er for hver delproces identificeret primære risici for dataforvanskning, ligesom der følger beskrivelse og vurdering af de mest centrale eksisterende kontroller til afhjælpning af disse risici.

Observationer i dette afsnit dækker således over de mangler, der er identificeret, når der er taget højde for den samlede mængde af kontroller og validerende aktiviteter,

som indgår i AMS-processen for at sikre datavaliditet og -kvalitet, herunder særligt manuelle/personelle kontroller, automatiske kontroller og øvrige kontroller. Videre følger der for hvert procestrin en kort beskrivelse af de udførte kontroller. Kontrollerne i AMS er vurderet i forhold til kontrollernes "designeffektivitet", dvs. deres tilstrækkelighed og behov i forhold til risikoen for dataforvanskning og/eller datatab i og kontrollernes "funktionelle effektivitet", dvs. hvorvidt de etablerede kontroller faktisk udføres og fungerer. Kontrollernes funktionelle effektivitet er blevet testet via besigtigelserne, hvor det vurderes, om kontrollerne udføres som beskrevet, og efterfølgende om kontrollerne er dokumenteret på behørig vis.

Figur 9. Procesdiagram for AMS – validering/kontroller



3.4.1 Validerings- og kontrolmæssige observationer på tværs af AMS-processen

Det er i relation til kontrolanalysen observeret, at Udlændingestyrelsen fører tilsyn på udrejsecentre i henhold til operatørkontrakten med Kriminalforsorgen som led i et formelt kunde-/leverandørforhold. Disse tilsyn foretages primært i relation til bygninger, faglige tilsyn af udbetaling af ydelser (i forbindelse med IBS) mv. med henblik på overholdelse af operatørkontrakten. Undersøgelsen har ikke kunnet påvise procedure- og/eller procesbeskrivelser, dokumentation for udførelse af kontroller, rapporteringsskemaer, eventuel dokumentation for fejlbehandling og opfølgning (i tilfælde af at der er identificeret fejl) eller lignende, som understøtter løbende opfølgning på kontrolparadigmet på udrejsecentre.

12. Manglende opfølgning på og tilsyn med kontrolparadigme på udrejsecentre	
Prioritet	2
Udrejsecentre	KHG og SJM
Beskrivelse af problemstilling	Det er i relation til kontrolanalysen observeret, at der fra Udlændingestyrelsens side udføres tilsyn på udrejsecentre i henhold til operatørkontrakten med Kriminalforsorgen i et kunde-/leverandørforhold. Disse tilsyn foretages primært i relation til bygninger, faglige tilsyn af udbetaling af ydelser (i forbindelse med IBS) mv. med henblik på overholdelse af operatørkontrakten. Der udføres ikke kvalitetssikring af Kriminalforsorgens drift af udrejsecentre eller kontrol med adgangs- samt ind- og udgangsregistreringer i relation til dataforvanskning.
Risiko-beskrivelse	Der er risiko for, at manglende fysiske og adfærdsmæssige tilsyn medfører, at Kriminalforsorgens drift af udrejsecentre og kontrol med adgangs- samt ind- og udgangsregistreringer såvel som meldepligt ikke i tilstrækkeligt omfang tager højde for håndteringen af risici relateret til dataforvanskning og databaser.
Kendte eksisterende kontroller	Der er ikke indarbejdet kendte kontroller på tværs af AMS.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at der etableres et koncept for løbende Intern KvalitetsSikring (IKS) i forhold til at følge op på, at risici for dataforvanskning og databaser mitigeres på tværs af AMS. IKS'en bør tage udgangspunkt i udarbejdelse af standardiserede processer og procedurer og fx inkludere kvartalsvise opfølgninger/stikprøvekontroller.

3.4.2 Delproces 2. Beboerregistrering

Der er i relation til delprocessen omkring beboerregistrering identificeret følgende primære risici for dataforvanskning:

- Risiko for fejloprettelse og fejlindtastning (fx forkert navn eller forkert adgangs- og rettighedstildeling) ved oprettelse af beboer i AMS, herunder særligt ved manuel oprettelse
- Risiko for oprettelse af forkert identitet (registrering modsvarer ikke den pågældende person).

I relation hertil er en række automatiske og manuelle kontroller opsat til afhjælpning af ovennævnte risici (se også afsnit 3.5 i forhold til datakontroller).

Procestrin 2.1.A Registrér beboer ved at fremsøge fra IBS

Ved automatisk registrering og oprettelse af beboere ved fremsøgning af stamdata fra CARL2/IBS er der en indbygget automatiseret kontrol til afhjælpning af risici relateret til fejloprettelser og fejlindtastninger. Ved denne type oprettelse udfyldes de nødvendige oplysninger om beboeren automatisk, hvorefter det ikke er muligt at rette i disse autoritative data (de låses for redigering). Med dette sikres det ligeledes, at funktionaliteter, såsom anti-passback, hændelsesregistrering mv., er aktiveret for den givne beboer.

Medarbejderen, der er ansvarlig for oprettelsen, foretager også en manuel kontrol af, at den givne beboer er korrekt oprettet. Der er indarbejdet en automatisk kontrol af, at beboer-id er unikt og ved oprettelse ikke i forvejen forefindes i systemet.

Procestrin 2.1.B Opret beboer manuelt

Ved manuel registrering og oprettelse af beboere findes der ingen automatisk kontrol til afhjælpning af risici relateret til fejloprettelser og fejlindtastninger. Ved denne type oprettelse udfylder medarbejderen, efter en dertil udarbejdet vejledning, selv de nødvendige oplysninger om beboeren, ligesom medarbejderen selv tildeler de relevante funktioner og rettigheder, fx anti-passback og hændelsesregistrering. Der foretages her en manuel kontrol af, at de udfyldte oplysninger og tildelte adgange er korrekte. For anbefaling i relation hertil se afsnit 3.3.2, observation nr. 8, vedrørende observationen Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere. Det bemærkes, at der er indarbejdet en automatisk kontrol af, at beboer-id er unikt og ved oprettelse ikke i forvejen forefindes i systemet.

På SJM er der indarbejdet en yderligere kontrol af, hvilke medarbejdere der kan foretage manuelle oprettelser af beboere og efterfølgende foretage ændringer i de dertilhørende stamdata. På SJM er dette begrænset til én udvalgt medarbejder, hvormed det sikres, at alene medarbejdere med rette viden, erfaring og fokus kan oprette beboere manuelt samt delvist mitigere risici for fejloprettelser og fejlindtastninger. På KHG er det observeret, at der ikke er indarbejdet en begrænsning af medarbejdernes rettigheder til at ændre i stamdata, hvormed risikoen for fejloprettelser og fejlindtastninger ikke afhjælpes.

18. U hensigtsmæssige roller og adgange i relation til ændring af stamdata	
Prioritet	3
Udrejsecenter	KHG
Beskrivelse af problemstilling	Det er observeret, at alle medarbejdere fra Kriminalforsorgen på KHG frit kan tilgå og rette i stamdata for beboere (både ved manuel oprettelse og oprettelse med udgangspunkt i stamdata fra CARL2).
Risiko-beskrivelse	Der er en øget risiko for, at beboerprofiler opsættes forkert (hændelsesregistrering eller anti-passback aktiveres ikke), eller at der på anden måde rettes fejlagtigt i stamdata (navn, beboer-id mv.).
Kendte eksisterende kontroller	Der er på KHG ikke identificeret nogen kontroller. Det bemærkes, at disse rettigheder på SJM er begrænset til én medarbejder, der alene kan rette i stamdata.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at det på KHG begrænses, hvilke medarbejdere der kan tilgå og rette i stamdata.

I relation til risikoen for oprettelse af forkert identitet foreligger der ingen deciderede kontroller, idet det ikke er muligt for medarbejderne at kontrollere, at den påståede identitet på den givne fremmødte beboer stemmer overens med vedkommendes sande identitet. Fremmødte beboere oprettes alene ud fra stamdata og deres asyl-id (uden billedidentifikation). Der foretages ved oprettelsen en vurdering af, om beboeren er den, de giver sig ud for at være. I tvivlsspørgsmål kan udrejsecentrets medarbejdere kontakte booking-enheden hos US eller HJEMST for at bekræfte beboerens identitet. Det vurderes ikke muligt at opstille yderligere kontrolmekanismer for at afhjælpe risikoen for, at en beboer ikke er, hvem beboeren giver sig ud for at være. Der er således ikke i udarbejdet yderligere anbefalinger i reaktion til dette, og den tilbageværende

risiko vurderes at være et grundlæggende rammevilkår for kontrol af adgange samt melde- og opholdspligt i relation til AMS-processen.

Sluttelig bør det i relation til den samlede delproces omkring beboerregistrering bemærkes, at der i denne undersøgelse ikke er fundet tilstrækkelig dokumentation for udførelse af interne tilsyn og kontroller med kontrolparadigmet i denne delproces.

3.4.3 Delproces 3. Indgangsregistrering

Der er i relation til delprocessen omkring indgangsregistrering identificeret følgende primære risici for dataforvanskning:

- Risiko for, at mere end én person kan passere ind på udrejsecentret samtidig således, at kun den første person adgangsregistreres via sit biometriske kort (dobbeltgennemgang i adgangskarrusellen)
- Risiko for, at mere end én person kan gå ind således, at kun den første person adgangsregistreres via sit streghodekort (dobbeltgennemgang i personslusen)
- Risiko for, at beboere kan passere igennem indgangsslusen (personslusen) uden at blive registreret
- Risiko for, at den samme person kan gå ind eller ud to på hinanden følgende gange
- Risiko for, at det ved anvendelse af streghodekort kan være vanskeligt at identificere den rigtige identitet (data afspejler ikke den korrekte identitet).

I relation hertil er der opsat en række automatiske og manuelle kontroller til afhjælpning af ovennævnte risici. Kontrollerne gennemgås nedenfor for hver variant af indgangsregistrering.

Procestrin 3.1.A Selvbetjent indgangsregistrering ved karrusel med biometrisk kort

Ved selvbetjent indgangsregistrering ved karrusel er der indarbejdet henholdsvis en fysisk, en manuel og en automatisk kontrol.

Den fysiske kontrol består i, at der i karrusellen er begrænset fysisk plads, hvormed det i høj grad besværliggøres, men ikke umuliggøres, at passere to igennem denne på samme tid. Dette mitigerer i høj grad risikoen for dobbeltgennemgang.

Den manuelle kontrol består i, at der på KHG og SJM sidder portvagtspersonale tæt på karrusellen, hvormed disse døgnet rundt kan overvåge beboernes registreringer og gennemgang og sikre imod dobbeltgennemgang samt dobbelte ind- og udgangsregistreringer.

Den automatiske kontrol består i anti-passback-kontrollen, der giver en fejlmelding, såfremt en given beboer laver to på hinanden følgende ind- eller udgangsregistreringer. Hermed mitigeres risikoen for to på hinanden følgende ind- eller udgangsregistreringer. Såfremt der ikke reageres på baggrund af dette, eller der ikke er opmærksomhed på, at fejlmeldingen skyldes anti-passback-kontrol, vil beboeren i nogle tilfælde anvende stregkodekortet til ind- eller udgangsregistrering, hvormed risikoen for to på hinanden følgende ind- eller udgangsregistreringer ikke mitigeres. Det er dog observeret, at anti-passback for biometriske kort ikke er aktiveret på KHG, som det fremgår af observationen nedenfor.

14. Anti-passback ikke aktiveret for biometriske kort

Prioritet	2
Udrejsecenter	KHG
Beskrivelse af problemstilling	Det er under både besigtigelse og tillægsbesigtigelse på KHG dokumenteret, at anti-passback ikke er aktiveret for det biometriske kort ved anvendelse i ind- og udgangskarrusellerne.
Risiko-beskrivelse	Der er risiko for gentagne fejlkoblinger, dvs. inden for denne undersøgelses genstandsfelt gentagne ind- og udgangsregistreringer, hvormed data potentielt ikke afspejler beboerens reelle passager.
Kendte kontroller	Der er ikke indarbejdet kendte kontroller.

Anbefalinger til yderligere tiltag

Yderligere anbefalinger	Det anbefales, at anti-passback reimplementeres for biometriske kort i samarbejde med systemleverandøren, dvs. Holstebro Låseteknik.
--------------------------------	--

Procestrin 3.1.B Indgangsregistrering ved portvagt med biometrisk kort (kun på SJM)

Ved manuelt understøttet indgangsregistrering ved portvagten med biometrisk kort foretages der en manuel og automatisk kontrol.

Den manuelle kontrol består i, at personalet ved portvagten påser, at kun én person passerer igennem personslusen ad gangen. Videre sikrer overvågningen af personslusen, at risikoen for, at beboere kan passere igennem personslusen uden at

blive registreret, sammen med risikoen for, at mere end én beboer går igennem, og at kun den ene registreres, mitigeres i tilstrækkelig grad .

Den automatiske kontrol består ligeledes i anti-passback-kontrollen, der giver en fejlmelding, såfremt systemet registrerer to på hinanden følgende ind- eller udgangsregistreringer. Hermed mitigeres risikoen for to på hinanden følgende ind- eller udgangsregistreringer i AMS. Såfremt medarbejderen ikke er opmærksom på, at fejlmeldingen vedrører anti-passback, kan beboeren i nogle tilfælde anvende stregkodekortet til ind- eller udgangsregistrering, hvormed risikoen for to på hinanden følgende ind- eller udgangsregistreringer ikke mitigeres.

Det er PwC's vurdering, at for begge indgangsregistreringer med anvendelse af biometrisk kort sikrer de biometriske funktionaliteter, at risiko for, at den indregistrerede beboer ikke stemmer overens med den fremmødte person/beboer, mitigeres i tilstrækkelig grad.

Procestrin 3.1.C Indgangsregistrering ved portvagt med stregkodekort

Ved indgangsregistrering med stregkodekort er der alene indarbejdet manuelle kontroller.

Første manuelle kontrol består i, at portvagten døgnet rundt overvåger og påser, at hver beboer, der passerer igennem personslusen, foretager en korrekt indgangsregistrering med stregkodekortet, hvormed risici for, at beboere passerer uregistrerede igennem, mitigeres i tilstrækkelig grad.

Anden manuelle kontrol består i portvagtens kontrol af beboerens identitet ud fra billedet på stregkodekortet. Dette mitigerer i nogen grad risikoen for, at den beboer, der indgangsregistreres, ikke er overensstemmende med den beboer, der rent faktisk går ind på centret.

I relation til risikoen for, at der foretages dobbelte ind- og udgangsregistreringer, er det for stregkodekort observeret, at der ikke er implementeret de anti-passback-funktionaliteter, som er implementeret for biometriske kort.

9. Anti-passback ikke implementeret for stregkodekort

Prioritet	2
Udrejsecenter	KHG og SJM

Beskrivelse af problemstilling	Leverandøren Sanistål har oplyst, at anti-passback kun er aktiveret ved brug af biometriske kort. En beboer, som har bevæget sig ind på centret og efterfølgende er gået ud af centret uden at registrere denne udgang (fx ved at hoppe over hegnet) kan således frit benytte stregkode-scanneren i portvagten til at foretage endnu en indgangsregistrering uden at blive bremsat af anti-passback funktionen. PwC's gennemførte dataanalyser underbygger dette, da langt størstedelen af fejlkombinationer af ind- og udgangsregistreringer sker, hvor der anvendes et stregkodekort (jf. kontrol 9 i dataanalysen).
Risiko-beskrivelse	Der er risiko for gentagne fejlkoblinger, dvs. gentagne ind- og udgangsregistreringer, hvormed data potentielt ikke afspejler beboerens reelle passager.
Kendte eksisterende kontroller	Der er ikke indarbejdet kendte kontroller.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at der findes en løsning for, hvordan anti-passback håndhæves i praksis, hvis beboeren ikke anvender sit biometriske kort. En tilgang er at undersøge med leverandører, om anti-passback kan implementeres for stregkodekort uden at skulle foretage store og dyre ændringer i applikationskode i standardsystemet Salto ProAccess Space. Alternativt kan det undersøges med leverandører, om man i stedet for at anvende stregkodekort som backup for biometrisk registrering kan anvende RFID-kort med billede, da disse kort også ville kunne opbevare data på selve kortet ligesom de biometriske kort. Dette kan potentielt sikre en simplere systemisk integration af passback-funktionaliteter på ikke-biometriske kort. Herudover anbefales det, at der aktivt fokuseres på at reducere anvendelsen af stregkodekort på KHG ved at introducere håndscannere i portvagten til biometriske kort på KHG ligesom på SJM, samt ved at overgå til FUSE-kort på KHG ligesom på SJM, da erfaringerne indtil videre er, at disse er mere stabile i drift.

Det er hertil observeret, at såfremt en beboer er udeblevet eller af anden grund er meldt udeblevet fra udrejsecentret, vil vedkommende ikke længere være administrativt til stede på centret og i AMS for det givne center. Herefter vil beboeren hverken kunne anvende sit biometriske kort eller sit stregkodekort til ind- og udgangsregistrering på centret.

15. Fejlregistreringer ved bruger meldt som udeblevet	
Prioritet	3

Udrejsecenter	SJM
Beskrivelse af problemstilling	Hvis en beboer har været registreret som værende udenfor udrejsecentret i for lang tid, så registreres beboeren automatisk som udeblevet med statussen "forbyd bruger" i AMS. Herefter kan beboeren ikke længere foretage ind- og udregistrering med hverken stregkodekort eller biometrisk kort. Ved afvisning af en beboer med biometrisk kort registreres dette i hændelsesloggen med status "Åbning ikke tilladt: Nogle ugyldig". Ved afvisning af en beboer med stregkodekort registreres dette ikke i loggen.
Risiko-beskrivelse	Der er ikke store risici forbundet med denne observation, da beboeren korrekt afvises, som det er tiltænkt. Dog kan der være en lille risiko for, at medarbejdere på centrene ikke kan gennemskue, hvorfor en beboer er blevet afvist, hvis dette ikke logges korrekt i hændelsesloggen, når der er tale om stregkodekort.
Kendte eksisterende kontroller	Der er ikke indarbejdet kendte kontroller.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at det undersøges nærmere med leverandører, om det uden de store omkostninger kan tilføjes til hændelsesloggen, at afvisninger af beboere med koden "forbyd bruger" også logges fra stregkodekort.

Sluttelig bemærkes det for den samlede delproces omkring indgangsregistrering, at der ikke er fundet tilstrækkelig dokumentation for udførelse af interne tilsyn og kontroller med kontrolparadigmet i denne delproces.

3.4.4 Delproces 4. Meldepligtregistrering

Der er i relation til delprocessen omkring meldepligtregistrering identificeret følgende primære risici for dataforvanskning:

- Risiko for, at det ved anvendelse af stregkodekort kan være vanskeligt at identificere den rigtige identitet (data afspejler ikke den korrekte identitet).

I relation hertil er der automatisk og manuel kontrol til afhjælpning af ovennævnte risiko.

Procestrin 4.1.A Melderegistrering inden for centret (Kærshovedgård)

Ved afholdelse af meldepligt med anvendelse af biometrisk kort er der indbygget en automatisk kontrol. De biometriske funktionaliteter sikrer automatisk, at der er overensstemmelse mellem beboeren, der er registreret i AMS, og beboeren, der afholder sin meldepligt, hvormed risici i relation hertil mitigeres.

Procestrin 4.1.B Meldepligtregistrering med stregkodekort

Ved afholdelse af meldepligt med anvendelse af stregkodekort er der indbygget en manuel kontrol. Denne består i, at medarbejderen fra HJEMST påser meldepligtregistreringen og foretager en identifikation af beboeren og en kontrol af overensstemmelsen med billedet på stregkodekortet. Dette mitigerer i tilstrækkelig grad risikoen for, at meldepligtregistreringen foretages af en anden beboer end den, som stregkodekortet er tilknyttet.

3.4.5 Delproces 5. Øvrig hændelsesregistrering

Der er i relation til delprocessen omkring øvrig hændelsesregistrering identificeret følgende primære risici for dataforvanskning:

- Risiko for, at data ikke afspejler beboerens reelle færden (fx hvis der er sat en sko i døren, så der ikke registreres ind- og/eller udgang af værelse)
- Risiko for, at tidsstempler ikke afspejler de rigtige tidspunkter for registreringer.

Der er i relation hertil indarbejdet en manuel opdatering af offline dørenheder for at mitigere risikoen for, at tidsstempler ikke afspejler de rigtige tidspunkter for registreringer. Der er i relation hertil observeret fejl i tidsstempler, og den manuelle kontrol vurderes ikke at fungere tilstrækkeligt efter hensigten, hvorfor den ikke til fulde mitigerer risikoen i relation hertil.

For yderligere beskrivelse af observation og anbefaling om dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG se afsnit 3.5.3 (den første observation).

Der er under kontrolanalysen ikke fremkommet oplysninger om yderligere relevante kontroller, der kan mitigere risikoen for, at data og registreringer fra offline dørenheder ikke afspejler beboerens reelle færden inde på KHG. Der er således ikke systematiske kontroller til sikring imod, at beboere sætter sko i klemme i værelsesdøre, foretager registreringer for at åbne døre for andre beboere eller potentielt lader andre beboere anvende deres nøglebrik, hvilket vil føre til, at registreringer ikke stemmer overens med beboernes færden inde på centret.

3.4.6 Delproces 6. Udgangsregistrering

For kontrol- og valideringsmæssige observationer i relation til udgangsregistrering henvises til afsnit 3.4.3 om indgangsregistreringer, da disse har samme karakter, men alene adskiller sig ved at berøre henholdsvis ind- og udgangsregistreringer.

3.5 Arkitektur og dataanalyser

Afsnittet gennemgår de tekniske komponenter i AMS-komplekset og dataanalyser, der er foretaget som led i nærværende undersøgelse. Afslutningsvis præsenteres de identificerede observationer relateret til systemarkitekturen. Arkitekturafsnittet er på denne baggrund opdelt i tre underliggende afsnit:

- Afsnit 3.5.1 indeholder et overblik over og en beskrivelse af de væsentlige tekniske komponenter i AMS-komplekset.
- Afsnit 3.5.2 gennemgår dataanalyserne, som er foretaget af dataflowet i AMS-dataflowet.
- Afsnit 3.5.3 præsenterer undersøgelsens observationer relateret til arkitekturen for AMS-komplekset. Observationerne struktureres efter AMS-processen, som er blevet anvendt tidligere i undersøgelsen.

3.5.1 Gennemgang af arkitekturen

Figur 10 på næste side viser et overblik over de forskellige komponenter.

Pc

Kriminalforsorgens medarbejdere på SJM og KHG arbejder i AMS via en webapplikation (Salto- applikation), som de kan tilgå via browseren på deres pc.

Bordkoder

På både SJM og KHG er der bordkodere til at kode data ind på de biometriske kort. Der er to særskilte bordkodere hvert sted: Én bordkoder til at kode biometrisk data ind på kortet og én bordkoder til at kode beboerens stamdata fra AMS ind på kortet.

Biometriske kort

Langt de fleste beboere på både KHG og SJM udstyres med et biometrisk kort (se procesbeskrivelsen for udstedelsen af de biometriske kort i afsnit 3.2.2). Meget få beboere har ikke et biometrisk kort. Enkelte beboere har ikke et funktionsdygtigt fingeraftryk, mens det kan ske for et udrejsecenter, at man i en kortere periode er løbet tør for de biometriske kort. Der anvendes to typer af kort på de to centre. På KHG anvendes kort fra udbyderen Zwipe, mens SJM er overgået til at anvende kort fra udbyderen Fuse. Begge korttyper har en indbygget fingeraftryksscanner, et batteri, en aktiveringsfunktion (fx aktiveres Fuse-kortet ved at slå på siden af kortet) og mulighed for at lagre data på kortets RFID-chip. Da beboerens data (fx beboerens id og de registreringsenheder, beboeren skal kunne benytte sit kort på) lagres direkte på kortet, kan de biometriske kort også benyttes, når der ikke er forbindelse til serveren. Mens Zwipe-kortets batteri skal udskiftes efter batteriudløb, har man på SJM mulighed for

at genoplade Fuse-kortet, så det holder til 1.000 nye aktiveringer. Kortene kan autentificere, om det fingeraftryk, som er gemt på RFID-chippen, stemmer overens med det fingeraftryk, som beboeren med sin finger sætter på kortet, når beboeren ønsker at benytte en af de biometriske onlineenheder.

Stregkodekort

Alle beboere på SJM udstyres også med et særskilt stregkodekort. På KHG udstedes der særskilte stregkodekort, der påklister bagsiden af det biometriske kort til de beboere, som også har en brik (se også afsnit 3.2.2). Stregkodekortene opbevarer ikke data om beboeren. Der printes i stedet en stregkode på selve kortet, som stregkodescannerne kan scanne og identificere som tilhørende den pågældende beboer. Der printes yderligere et billede af beboeren på kortet for at sikre, at medarbejderen fra Kriminalforsorgen kan autentificere, at personen, der anvender stregkodekortet, er den samme person som den beboer, stregkoden tilhører.

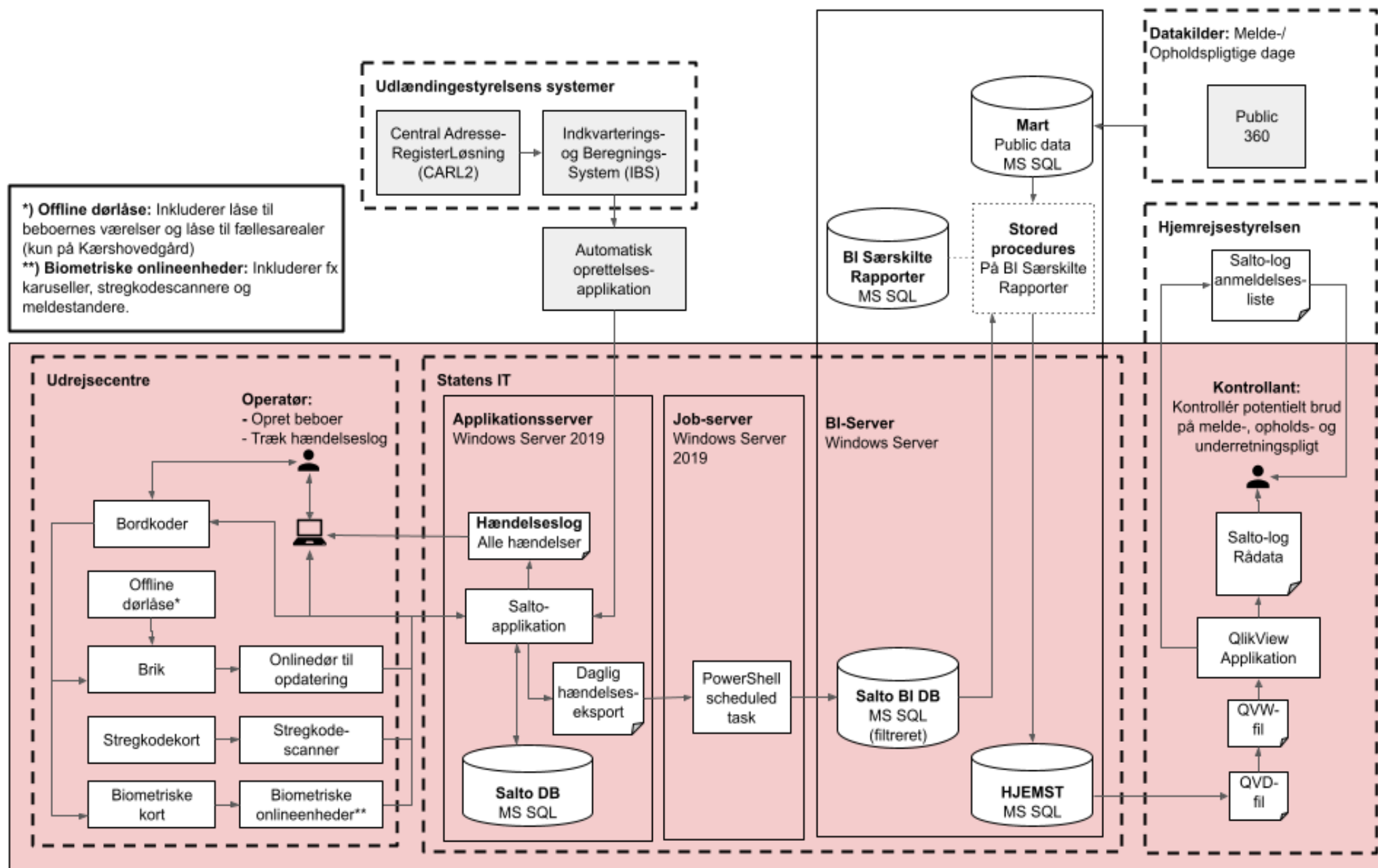
Brik

Der anvendes låsebrikker på begge centre, men det er kun på KHG, at disse anvendes som en del af AMS, og dette afsnit dækker derfor blot over anvendelsen af brikker på KHG. For beboere, der ikke har fået tildelt et biometrisk kort udstedes der på KHG en elektronisk brik, som anvendes til elektroniske dørlåse, der giver adgang til beboernes værelser og til fællesarealer. Brikkerne kan opbevare registreringer fra de offline registreringsenheder, som beboeren har anvendt. For beboere med biometriske kort, udstedes ikke en brik, da det biometriske kort også kan anvendes til de elektronisk dørlåse.

Offline dørlåse

På KHG er der elektroniske dørlåse ved beboernes værelser samt ved fællesarealer, som kan levere data til Salto DB i AMS. Disse enheder kaldes "offline" dørlåse, fordi de ikke har en forbindelse til SIT's servicenetværk, modsat stregkodescannere og de biometriske kortscannere. Data lagres i stedet på den elektroniske brik eller det biometriske kort, når en beboer benytter brikken eller det biometriske kort til at låse en offline dør op. På KHG er der en specifik online registreringsenhed/opdateringsenhed, hvor beboeren kan anvende sin brik for derved at overføre registreringer fra brikken til AMS (se også figur 10).

Figur 10. Systemoverblik



Biometriske onlineenheder

De biometriske onlineenheder indeholder en RFID-læser, der kan læse RFID-chippen på de biometriske kort og verificere, om kortholderens identitet er kendt. Ved at læse data på kortet er det desuden muligt at kontrollere, om beboeren har lov til at benytte den pågældende enhed. Der er desuden en kontrolboks på enhederne (også kaldet en Control Unit, CU), som opbevarer de seneste 3.000 eller 5.000 hændelser (afhængig af type). Kontrolboksen faciliterer datakommunikation med Salto-applikationen (læs mere om dette i faktaboks 1: "Integrationsmønstre mellem onlineenheder og Salto-applikationen").

Stregkodescanner

På både KHG og SJM kan portvagten scanne beboerens stregkodekort ved ind- og udgang via den bemandede port. Ligesom med de biometriske onlineenheder er stregkodescannerne koblet til en kontrolboks, som opbevarer de seneste 3.000 eller 5.000 hændelser (afhængig af type). Når stregkodescanneren anvendes, sker der et live-opslag fra enheden til Salto-databasen, som kontrollerer, om beboeren skal have adgang. Dette er nødvendigt, fordi der ikke kan skrives data ned på stregkodekortene. Det medfører dog, at der altid skal være forbindelse til serveren, hvis stregkodescanneren skal benyttes. Kontrolboksen faciliterer datakommunikation med Salto-applikationen (læs mere om integrationsmønstre for denne kommunikation i faktaboks 1).

Salto-applikationen (Salto-applikation + Salto DB)

Salto ProAccess Space er en softwareløsning, der er udviklet af leverandøren, Salto, og som i systemoverblikket på foregående side er opdelt i to dele:

- **Salto-applikation** er en webapplikation, der udstiller data og funktioner til brugerne via en brugergrænseflade, som er bygget til at kunne tilgås via brugerens browser. Salto-applikationen består også af en række backend-services, som giver mulighed for at skrive til og læse fra Salto DB fra både en brugergrænseflade og de online registreringsenheder på udrejsecentrene. Der er desuden oprettet en lille klient, kaldet "Automatisk Oprettelsesapplikation", som via en integration til IBS kan hente stamdata på beboeren fra CARL2. Denne del er dog uden for undersøgelsens primære genstandsfelt.
- **Salto DB** er en relationel database, der afvikles på Microsoft SQL. Salto DB indeholder bl.a. tabeller til data på hændelsesregistreringer, opsatte eksportjobs og stamdata om beboeren.

Faktaboks 1. Integrationsmønstre mellem onlineenheder og Salto-applikationen

Når online registreringsenheder (både de registreringsenheder, der anvendes til de biometriske scannere og de til stregkodescannere) kommunikerer med Salto-applikationen, som skal gemme beskederne i databasen, sker det med User Datagram Protocol (UDP)-beskeder. Der benyttes to forskellige integrationsmønstre for at sikre, at disse UDP-beskeder modtages korrekt i Salto DB hos SIT, også hvis der i en given periode ikke er forbindelse til serveren hos SIT. Det er vigtigt at bemærke, at enhedernes lagringsplads er en begrænsende faktor for, hvor lang tid en enhed kan være uden serverforbindelse uden at opleve datatab, idet de ældste registreringer slettes, når der kommer nye registreringer til. Læs mere herom i observation 22.

Integrationsmønstre for CU4200-registreringsenheder

CU4200-enhederne er nyere og har plads til at opbevare 5.000 hændelser. Alle enheder på SJM er af CU4200-typen, og på KHG er bl.a. meldestandere af CU4200-typen. For CU4200-enhederne er det registreringsenhederne, der initierer kommunikationen. Så snart en ny hændelse registreres, sender registreringsenheden hændelsen til Saltos backend-services, der ligger server-side hos SIT. Hvis der er forbindelse til serveren, får registreringsenheden en bekræftelse tilbage, på at hændelsen er modtaget, og herefter bliver næste hændelse sendt afsted. Hvis der derimod ikke er forbindelse, får registreringsenheden ikke nogen bekræftelse, og den vil herefter blive ved med at forsøge at sende den samme hændelse af sted, indtil den modtages i den anden ende. Ovenstående sikrer, at beskeder altid gensesendes, indtil beskeden er modtaget. Der er herudover en sikkerhed for, at den samme hændelse ikke registreres mere end én gang. Hver hændelsesregistrering har et unikt id, og det sikres ved skrivning på databasen, at Salto DB ikke kan indeholde to rækker med samme id (læs nærmere om denne kontrol af unikhed ved indlæsning til databasen i beskrivelsen af kontrol 7 i afsnit 3.5.2.2, Gennemgang af analyser).

Integrationsmønstre for CU5000-registreringsenheder

CU5000-enhederne er ældre og har plads til at opbevare 3.000 hændelser. Ind- og udgangskarrusellen på KHG er fx CU5000-enheder. For CU5000-enhederne er det Salto-applikationen, som med korte mellemrum sender forespørgsler til registreringsenhederne og spørger, om der er kommet nye hændelser siden sidst. Hvis der er nye hændelser, sender enhederne disse hændelser tilbage. Når hændelserne er gemt i databasen, sendes en bekræftelse tilbage til enheden om, at hændelserne er registreret. Den enkelte enhed kan således vedligeholde et indeks over, hvilke beskeder den endnu ikke har sendt til serveren, hvilket sikrer, at også beskeder, der i første omgang ikke blev modtaget i Salto DB, bliver gensesendt. På samme måde som for CU4200-registreringsenhederne sikres det ved indlæsning i databasen, at samme hændelse ikke kan registreres to gange i databasen (læs nærmere om denne kontrol af unikhed ved indlæsning til databasen i beskrivelsen af kontrol 7 i afsnit 3.5.2.2, Gennemgang af analyser).

Netværk

Alle online registreringsenheder på udrejsecentrene samt den pc, som medarbejdere fra Kriminalforsorgen benytter på hvert center, er koblet på en MPLS-netværksforbindelse, der leveres af SIT. Denne forbindelse faciliterer datakommunikationen mellem registreringsenheder/computere på udrejsecentrene og Salto-applikationen hos SIT. Den server, som i denne rapport kaldes "Applikationsserveren", hvorpå Salto ProAccess Space-softwaren (både applikationskoden og den underliggende database) afvikles, er placeret i SIT's "demilitarized zone" (DMZ).

Hændelseslog

I Salto-applikationens brugergrænseflade er det muligt at trække en hændelseslog, som viser alle registreringer fra databasen – både succesfulde registreringer, fejlmeddelelser og særskilte tekniske statuskoder.

Daglig hændesekseksport

I Salto-applikationens brugergrænseflade under ”Planlagte jobs” er det muligt at opsætte faste daglige eksporteringer af hændelser. Databaseadministratorer hos UIM-KIT har i samarbejde med medarbejdere med forretningsindsigt fra Udlændingestyrelsen (og efterfølgende HJEMST) opsat faste daglige hændesekseksporter, der genererer hændelsesfiler med registreringer fra en delmængde af registreringsenhederne og med en delmængde af de statuskoder, som genereres ved en registrering. Hvis en ny registreringsenhed ikke er registreret som værende inkluderet i den daglige hændesekseksport, vil registreringerne fra denne enhed ikke ende i QlikView, hvor sagsbehandlerne behandler sagerne i sidste ende. Der er opsat tre særskilte daglige eksporteringer:

- **KHG Log rullende 60 måneder tilbage - US:** Dette er en daglig eksport af hændelser med statuskoderne 17 (”Dør oplåst (nøgle)”) og 84 (”Åbning ikke tilladt: nøgle ugyldig”) fra 16 udvalgte onlineenheder på KHG for de seneste 60 måneder.
- **SJM Log rullende 60 måneder tilbage - US:** Dette er en daglig eksport af hændelser med statuskoderne 17 (”Dør oplåst (nøgle)”) og 84 (”Åbning ikke tilladt: nøgle ugyldig”) fra 15 udvalgte onlineenheder på SJM for de seneste 60 måneder.
- **HJEMST:** Dette er en daglig eksport af hændelser med samtlige 27 statuskoder fra 489 udvalgte enheder på KHG for de seneste 12 måneder. Modsat den anden eksport fra KHG indeholder denne eksport også hændelser fra udvalgte offlineenheder fra beboernes og fællesarealernes dørlåse.

De tre daglige hændesekseksporter danner tre CSV-filer på Salto-serveren, og det er kun data fra disse filer, der senere hen er synlige for sagsbehandlerne i QlikView. Eksempelvis er alle hændelser, der relaterer sig til ”anti-passback”, frasortet i den daglige hændesekseksport.

PowerShell scheduled tasks

UIM-KIT har udviklet en række ”scheduled tasks” i Microsoft PowerShell, som dagligt henter de tre CSV-filer på Salto-serveren, der er blevet genereret i den daglige hændesekseksport, flytter filen over på ”job-serveren”, og indlæser data fra hver fil på tre forskellige tabeller på Salto BI-databasen på ”BI-serveren”.

Salto BI DB

Data fra den daglige hændesekseksport indlæses via scheduled tasks i Salto BI DB, som er en relationel MS SQL-database. Databasen indeholder en delmængde af de registreringer, der er i Salto DB. Det er filtrene i den daglige hændesekseksport, der afgør, hvilke hændelsesregistreringer der ender i Salto BI DB. Data fra de tre CSV-filer indlæses på tre særskilte tabeller på Salto BI DB:

1. KHG (med data 60 måneder tilbage)
2. SJM (med data 60 måneder tilbage)
3. HJEMST (med data 12 måneder tilbage).

Hver dag tømmes data i hver af disse tabeller, og data fra den seneste version af hver af de respektive CSV-filer lægges ind på tabellen.

Stored procedures (uden for det primære genstandsfelt)

På databasen ”BI Særskilte Rapporter” er der opsat forskellige BI-rapporter, som anvendes i forskellige sammenhænge. I relation til undersøgelsens genstandsfelt er der udviklet en række stored procedures, som sammenkobler data fra Salto BI DB med data fra Public 360 (data indlæses fra en BI-mart med replikerede data). Disse stored procedures er udviklet i SQL-kode, og selvom de er uden for det primære genstandsfelt i denne undersøgelse, er det relevant at forstå på et overordnet niveau, at der sker en række ting i disse stored procedures, heriblandt:

- **Kobling af sagsbehandlingsdata og hændelsesregistreringer:** Sammenkobling af data mellem hændelsesregistreringer fra Salto BI DB og sager i Public 360. Denne sammenkobling sker på beboerens PersonID fra CARL2, som anvendes i begge systemer. Formålet med denne sammenkobling er at kunne vise for sagsbehandleren i QlikView, om der allerede er en sagsbehandling i gang af en potentiel anmeldelse af en beboer.
- **Kobling af ind-/ og udgangsregistreringer:** Sammenkobling af ind-/udgangsregistreringer for en konkret beboer med henblik på at kunne fremhæve en række relevante oplysninger til sagsbehandleren, såsom en potentiel udeblivelse (defineret som, når en beboer har befundet sig mere end 24 timer uden for centret) og en fejlkobling (forstået i denne undersøgelse som, hvis en person er passeret ind eller ud to gange i træk uden at have passeret den modsatte vej).

Efter indhentning og transformation af data i stored procedures leveres data videre til databasen ”HJEMST DB”. Denne indlæsning sker formentlig via et job, eventuelt på job-serveren, men dette har ligeledes været uden for det primære genstandsfelt i projektet.

HJEMST DB

Dataoutput fra stored procedures skrives dagligt ned på HJEMST DB. Fra HJEMST DB genereres der dagligt filer i QlikView-formaterne ”.QVD” og ”.QVW”, så data automatisk kan indlæses og opdateres i QlikView.

QlikView-applikation

Data fra QVD- og QVW-filerne fremvises i QlikView-applikationen i henholdsvis:

- **Salto-anmeldelseslisten**, som viser potentielle anmeldelser baseret på logik opsat i stored procedures. Det er uden for undersøgelsens genstandsfelt at analysere anmeldelseslisten. Læs mere om, hvordan medarbejderne i

HJEMST (MOT) anvender anmeldelseslisten i beskrivelsen af procestrin 7.1 i afsnit 3.2.2.

- **Salto-rådatalog**, som giver mulighed for at se en enkelt beboers registreringer, som er filtreret med filtre indarbejdet i den daglige hændelseseksport. Læs mere om anvendelsen af Salto-rådatalog i beskrivelsen af procestrin 7.2 i afsnit 3.2.2

Arkitekturens understøttelse af processen

Figur 11 nedenfor viser de enkelte komponenters relation til AMS-processen for at illustrere sammenhængen mellem teknologi og proces.

Figur	11.	Overblik	over	de	tekniske	komponenters	relation	til	processen
		1. Håndtering af melde-, opholds- og underretningspligt samt fritagelser	2. Beboerregistrering	3. Indgangsregistrering	4. Melderegistrering	5. Øvrig hændelsesregistrering (kun Kærshovedgård)	6. Udgangsregistrering	7. Undersøgelse af brud på melde-/ opholds- og underretningspligt	
		• Public 360 (EstherH) • IBS • Meldepligtdatabase.	• Salto ProAccess Space • Biometriske kort • Stregkodekort • Brikker til døråse • Bordkoder • Førstegangslæser • Automatisk oprettelsesapp. (integration til IBS / CARL2).	• Salto ProAccess Space • Biometriske kort • Stregkodekort • Biometriske scannere (indgangskarrusel og biometrisk håndscanner) • Stregkodescannere • Offline døråse.	• Salto ProAccess Space • Biometriske kort • Stregkodekort • Biometriske meldestandere • Stregkodescannere ved meldestander • Offline døråse.	• Salto ProAccess Space • Brikker til døråse • Offline døråse.	• Salto ProAccess Space • Biometriske kort • Stregkodekort • Biometriske scannere (udgangskarrusel og biometrisk håndscanner) • Stregkodescannere • Offline døråse.	• Anmeldelsesliste (i QlikView) • Rådatalog (i Qlikview) • To-be: Access-database til meldepligt • Public 360 • IBS • HJEMST DB • Salto BI DB.	

3.5.2 Gennemgang af dataanalyserne

Dette afsnit fokuserer på de dataanalyser, der er foretaget i forbindelse med nærværende undersøgelse. Afsnittet er inddelt i to underafsnit:

- 1. Første delafsnit giver et overblik over delanalyser foretaget i dataanalyserne og kontroller, der er gennemført i relation til hver delanalyse.
- 2. Andet delafsnit gennemgår hver af de gennemførte delanalyser og kontroller.

Der er i dataanalyserne ikke fundet nogen indikationer på hverken tab eller forvanskning af data i dataflowet. Dataanalysernes resultater bidrager til forskellige observationer i forskellige afsnit i rapporten:

- **9. Antipassback ikke implementeret for streghodekort:** Kontrol 9 tilbyder baggrund for fejlkoblinger ved brug af streghodekort

- **17. Forkert brug af datamodel:** Ved gennemgang af data i Salto DB blev det i kontrol 2 som en sideobservation bemærket, at datamodellen ikke altid anvendes efter hensigten i praksis.
- **24. Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data:** Kontrol 1-7 af dataanalyserne har ikke fundet nogen indikationer på datatab eller -forvanskning.
- **25. Dobbeltregistreringer på meldestandere:** Kontrol 7 undersøger, hvordan unikhed håndteres i Salto DB, hvilket indikerer at dobbeltregistreringer på meldestandere snarere er et udtryk for beboernes adfærd, mens kontrol 8 giver indsigt i omfanget af dobbeltregistreringer på meldestandere.

Tabel 2: Overblik over delanalyser og relaterede kontroller

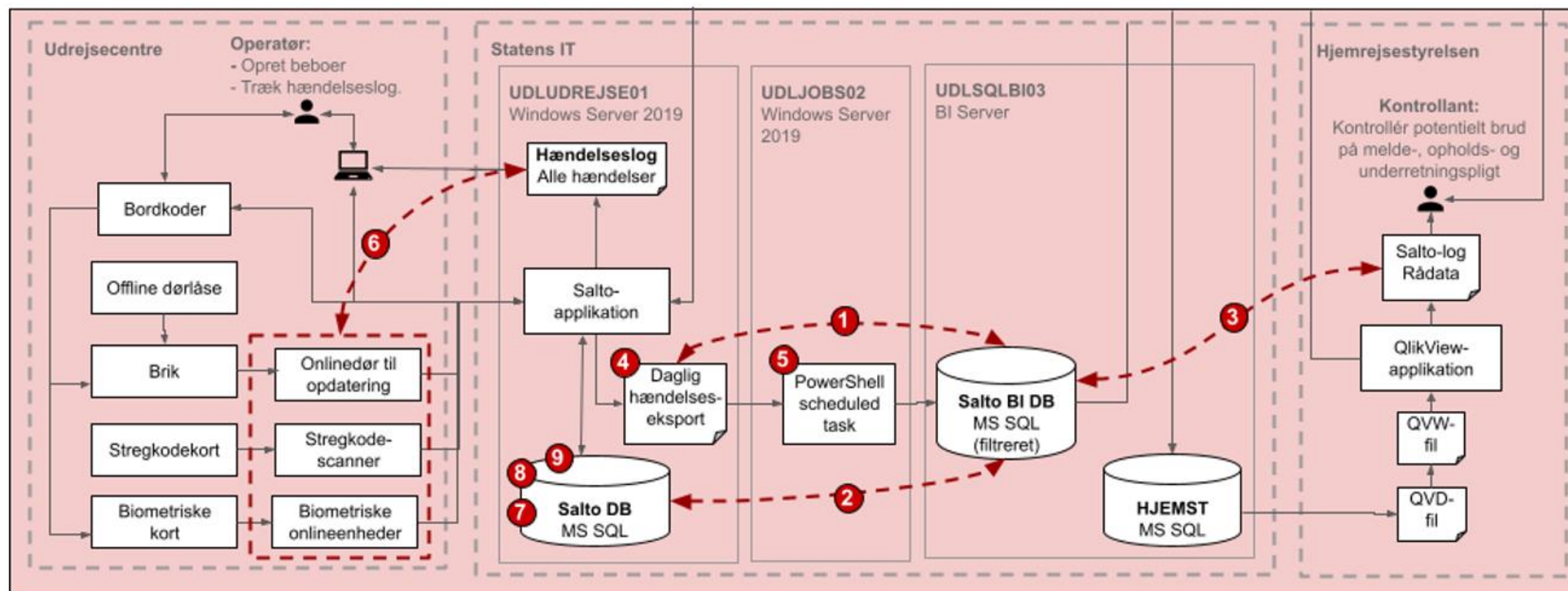
Delanalyser	Beskrivelse	Kontroller (af data)
Konsistens og validitet af registreringer	Formålet med analysen er at undersøge, om der er konsistens på tværs af dataflowet for at sikre, at der ikke sker dataforvanskning mellem datakilder. Hver konsistenskontrol sammenligner data i én del af dataflowet (fx en fil, database eller lignende) med data i en anden del af dataflowet for at se, om der er konsistens mellem disse. Et særligt fokusområde er at kontrollere formatet på tidsstemplerne for at validere, at der ikke sker en forvanskning af formatet i løbet af dataflowet.	● 1: Sammenligning af data fra Salto-applikationens daglige hændelseseksport med dataudtræk fra Salto BI DB på BI-serveren. ● 2: Sammenligning af data fra Salto DB på Salto-serveren med data fra Salto BI DB på BI-serveren. ● 3: Sammenligning af data fra Salto BI DB på BI-serveren med Salto-log Rådata i Qlikview.
Manuelt kode-review	Formålet med et manuelt kode-review er at kontrollere, om der i udvalgte tekniske komponenter, som bidrager til udtræk, transformation og indlæsning af data, sker noget, som potentielt kan forvanske data.	● 4: Review af filtrering på Saltos daglige hændelseseksport ● 5: Review af scheduled task (PowerShell) på job-serveren til overførsel af data fra Salto-serveren til BI-serveren.
Akkurathed af registrering	I denne delanalyse foretages der manuelle stikprøveregistreringer under besigtigelser på udrejsecentrene for at kontrollere, om en registrering på et givent tidspunkt udløser et korrekt datapunkt i hændelsesloggen. Analysen bidrager med et ekstra lag af kontrol ved at tjekke, om data også fødes rigtigt i AMS – mens de andre delanalyser kontrollerer dataflowet, efter data allerede er havnet i databasen.	● 6: Sammenligning af log fra manuel kontrol (besigtigelse) på udrejsecentrene med hændelseslog fra Salto-applikationen.
Unikhed af registrering	Denne delanalyse kontrollerer Salto DB's logik for at sikre, at én registrering ikke repræsenteres flere gange i databasen.	● 7: Kontrol af, hvordan unikhed af registreringer håndteres i Salto DB.
Dobbelt- registrering (adfærd)	Denne delanalyse undersøger omfanget af dobbeltregistreringer på meldestandere i Salto DB for at bekræfte hypotesen om beboeres mistillid til meldesystemet, som fører til flere registreringer af samme beboer. Dobbeltregistreringer er i denne sammenhæng defineret som to eller flere registreringer af samme beboer på en eller flere meldestandere inden for en afgrænset tidsperiode (her ti sekunder).	● 8: Undersøgelse af omfanget af dobbelte registreringer på meldestandere på Salto DB.
Fejlagtig kombination af registrering (adfærd)	Denne delanalyse undersøger omfanget af forkerte kombinationer af registreringer (fx to på hinanden følgende registreringer ved indgang uden en registrering af udgang imellem. Dette kaldes også en fejlkobling).	● 9: Undersøgelse af omfanget af "Fejlagtig kombination af registreringer" på Salto DB.

3.5.2.1 Introduktion til delanalyser og kontroller

Dataanalysen er opdelt i en række delanalyser, som hver udspringer af en eller flere hypoteser og relaterer sig til en eller flere komponenter af systemet. Tabel 2 på den

forrige side giver et overblik over delanalyserne og de relaterede kontroller, som er blevet gennemført for hver delanalyse. Figur 12 nedenfor giver et overblik over, hvordan hver kontrol relaterer sig til de tekniske komponenter i AMS-komplekset.

Figur 12. Overblik over, hvordan de gennemførte datakontroller relaterer sig til de tekniske komponenter i AMS-komplekset



3.5.2.2 Gennemgang af dataanalyser

Konsistens i og validitet af registrering

Dette afsnit gennemgår hver kontrol, som indgår i konsistensanalysen. Analysen sammenligner data på tværs af komponenterne gennem stikprøver med det formål at se, om der sker ændringer (forvanskning eller tab) i data på tværs af dataflowet i AMS (dvs. på tværs af flowet, som er optegnet i figur 12 ovenfor). En ændring kan eksempelvis være, hvis datoformatet ændrer sig fra et punkt til et andet, og et tab kan være, at en registrering mangler. Det er således formålet med konsistensanalysen at finde evidens for dataforvanskning gennem ændringer i data eller tab af data. I de tilfælde hvor der ikke er ændringer eller tab af data, konkluderes det, at der ingen evidens er fundet for, at dataforvanskning har fundet sted. Læg mærke til, at tabellerne i dette afsnit har en anden farve, da de røde tabeller repræsenterer kontroller udført i dataanalyserne, mens de orange tabeller i de andre afsnit repræsenterer undersøgelsens observationer.

Kontrol 1: Sammenligning af data fra Salto-applikationens daglige hændelseseksport med dataudtræk fra Salto BI DB på BI-serveren

Fremgangsmåde	Denne analyse er foretaget ved at sammenstille en stikprøve af data, som er genereret af Salto-applikationens eksportjob, med et databaseudtræk (stikprøve) fra Salto BI DB på BI-serveren. Som stikprøve er der anvendt et dataudtræk fra og med 1. januar 2021 til og med 30. januar 2021 med i alt 19.755 datapunkter. Kontrollen består i en sammenligning på tværs af de to datakilder af: • mængden af unikke registreringer • datatyper for alle kolonner • datoformat for ét felt, der indeholder både dato og tidsstempel.
Resultat af kontrollen	Det kan bekræftes ved sammenligning af data, at antallet af datapunkter (beboerregistreringer) er ens, og at datatyper og datoformat for tidsstempler alle er uændrede.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen.

Kontrol 2: Sammenligning af data fra Salto DB på Salto-serveren med data fra Salto BI DB på BI-serveren

Fremgangsmåde	Denne analyse er foretaget ved at sammenstille en stikprøve af de rådata, som er placeret på Salto DB, med et databaseudtræk (stikprøve) fra BI-serverens database, Salto BI DB. Som stikprøve anvendes følgende dataudtræk: 1. fra og med 1. januar 2021 til og med 30. januar 2021 2. fra og med 1. januar 2020 til og med 30. januar 2020 Kontrollen består i en sammenligning af følgende på tværs af de to datakilder: • Datoformat for ét felt, der indeholder både dato og tidsstempel • Ændring i enhedsnavnet for hver registrering • Ændring i statuskoden for hver registrering.
Resultat af kontrollen	• Ved denne sammenligning ses det i stikprøve 2, at ét beboernavn er blevet ændret. Helt konkret er karakteren ' udskifter med '. (Årsagen til denne uoverensstemmelse er fundet i forbindelse med kontrol 5). • Det kan bekræftes, at der ved denne sammenligning af datapunkter ikke er tegn på dataforvanskning på de resterende datafelter i stikprøven.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen.

Kontrol 3: Sammenligning af data fra Salto BI DB på BI-serveren med Salto-log Rådata i Qlikview

Fremgangsmåde	Denne analyse er foretaget ved at sammenstille en stikprøve fra Salto BI DB med en stikprøve fra Salto-log Rådata i Qlikview. 1. Som stikprøve anvendes følgende dataudtræk: fra og med 1. januar 2021 til og med 30. januar 2021. Kontrollen består i en sammenligning af følgende på tværs af de to datakilder: • Mængden af unikke registreringer • Datatyper for alle kolonner • Datoformat for ét felt, der indeholder både dato og tidsstempel. Der dannes en unik nøgle (composite key) ved at kombinere beboer-id, dato- og tidsstempel samt enhedsnavn for begge datakilder. Det undersøges dernæst, om disse to sæt af nøgler (én nøgle i Salto BI DB og én i rådataloggen i Qlikview) er helt ens, dvs. at alle datapunkter (nøgler) eksisterer i begge sæt.
	• For KHG eksisterer der 6.763 registreringer fra 103 unikke beboere fra onlineenheder (inklusive meldestandere) i stikprøven fra BI DB. Samtlige 6.763 registreringer fra samme unikke beboere er fundet i stikprøven fra Salto-log Rådata i Qlikview. • For SJM eksisterer der 1.252 registreringer fra 26 unikke beboere fra onlineenheder (inklusive meldestandere) i stikprøven fra BI DB. Samtlige 1.252 registreringer fra samme unikke beboere er fundet i stikprøven fra Salto-log Rådata i Qlikview. • Det kan bekræftes, at der ved denne sammenligning af datapunkter ikke er tegn på dataforvanskning på samtlige datafelter i stikprøven.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen.

Manuelt kode-review

Kontrol 2 og 3 er af typen review af udvalgte scripts/udvalgt kode (se tabel 2). Kodereviewet er foretaget kvalitativt af logik til eksport, import, filtrering og overførsel af data. Fokus i kode-reviewet har været på afdækning af risiko for dataforvanskning. Andre perspektiver på kodekvaliteten, såsom fx kodens kørselstid, ressourceforbrug og sikkerhedsmæssige sårbarheder, er ikke medtaget i kode- reviewet.

Kontrol 4: Review af filtrering på Saltos daglige hændesekseksport

Fremgangsmåde	Der er foretaget kontrol af tre daglige hændesekseksporteringer, som er opsat i Salto applikationens brugergrænseflade (læs mere om disse i underafsnittet om daglig hændesekseksport i afsnit 3.5.1, Gennemgang af arkitekturen. Kontrollen er foretaget ved først at gennemgå, hvordan udtrækkene er konfigureret i Salto-applikationens brugergrænseflade, og herefter foretage et kvalitativt review af, hvordan opsatte parametre i de enkelte hændesekseksportjobs gemmes og anvendes i Salto DB.
	Det er verificeret, at konfigurationen af hændesekseksportjobs fungerer efter hensigten. De opsatte eksportjobs gemmes i tabellen "tb_ScheduledJobs" på Salto DB, og det er valideret, at opbevaringen og anvendelsen af disse oplysninger sker korrekt.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen.

Kontrol 5: Review af scheduled task (PowerShell) på job-serveren til overførsel af data fra Salto-serveren til BI-serveren

Fremgangsmåde	Denne kontrol er foretaget ved at gennemføre et manuelt kode-review af følgende til scheduled tasks og tilhørende scripts: 1. Den schedulerede task "Daily Copy - Saltlogs", som afvikler scriptet "CopyDailySaltlogs.cmd", der kopierer daglige hændelseseksport-CSV-filer fra Salto-serveren til job-serveren 2. Den schedulerede task "ImportSaltoCSVFileIntoDatabase", der afvikler tre underliggende scripts: ○ Scriptet "Import_SJM_CSV_File_to_SQLTabel-US.ps1", der loader en daglig fil med hændelser med udvalgte statuskoder fra udvalgte enheder fra SJM ind i tabellen "SJM" på Salto BI DB ○ Scriptet "Import_KHG_CSV_File_to_SQLTabel-US.ps1", der loader en daglig fil med hændelser med udvalgte statuskoder fra udvalgte enheder fra KHG ind i tabellen "KHG" på Salto BI DB ○ Scriptet "Import_KHG_CSV_File_to_SQLTabel-Hjemst.ps1", der loader en daglig fil med hændelser med udvalgte statuskoder fra udvalgte enheder fra KHG ind i tabellen "HJEMST" på Salto BI DB.
Resultat af kontrollen	● Opmærksomhedspunkt: Ved gennemgang af "Import_SJM_CSV_File_to_SQLTabel-US.ps1" og "Import_KHG_CSV_File_to_SQLTabel-US.ps1" observeres en uhensigtsmæssig tilgang til indsætning af data i BI-serveren ved at foretage en udskiftning af karakteren ' med ' på beboernavnefeltet "UserName". Det antages, at dette foretages for at undgå fejl ved indsætning af data via et SQL INSERT-statement, da ' bruges som afgrænsning af tekststreng. ● Denne tilgang medfører ikke et direkte tab af registreringer, men data bliver reelt ændret, og det bliver derfor sværere at lave konsistenskontroller på tværs af dataflowet, givet at "UserName" ikke er konsistent på tværs af flowet ● Det observeres, at indlæsning af data i BI-serveren sker mere hensigtsmæssigt i "Import_KHG_CSV_File_to_SQLTabel-Hjemst.ps1", hvor bl.a. datatyper er bedre styret, og udskiftning af karakterer ikke finder sted.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen.

Akkurathed af registrering: Kontrol af, om en registrering på et givet tidspunkt udløser et korrekt datapunkt i hændelsesloggen. Denne delanalyse er udført ved sammenligning af log fra manuel kontrol på hjemrejsecentrene med dataudtræk fra Salto-applikationen.

Kontrol 6: Sammenligning af log fra manuel kontrol (besigtigelse) på udrejsecentrene med hændelseslog fra Salto-applikationen

Fremgangsmåde	Under besigtigelse på SJM og KHG blev der gennemført en kontrol af registreringer på udvalgte online- og offlineenheder for at validere, at registreringer får det korrekte tidsstempel i hændelsesloggen i Salto-applikationen. Kontrollen blev udført med både en brik til dørlåse (kun på KHG), biometriske testkort og stregkodekort. Både brikker og kort blev oprettet til PwC's medarbejder i forbindelse med besigtigelsen. For hver enhed blev der derefter gennemført en kontrol på følgende vis: ● Brikken/kortet blev anvendt på den pågældende enhed. ● Samtidig blev tidspunktet for registreringen noteret i en manuel log. ● Sluttelig blev der lavet en sammenligning mellem den af PwC udarbejdede manuelle registreringslog og hændelsesloggen fra Salto-applikationen. På KHG foregik dette ved ét samlet tjek, mens det på SJM foregik løbende efter hver registrering.
Resultat af kontrollen	Kontrollen viste på begge udrejsecentre, at alle tidsstempler i hændelsesloggen i Salto-applikationen var korrekte, når der blev sammenlignet med den manuelle registreringslog, som PwC havde udarbejdet.
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen. Note: På KHG fremgik offline-registreringerne ikke i loggen med den testbruger, der blev sat op til PwC's besigtigelse, evt. som følge af den konkrete brugeroprettelse. Derfor har det ikke været muligt at kontrollere, om der var tidsforskydning på hændelser fra offline-enheder på KHG.

Unikhed af registrering: Kan en enhed ved en fejl sende samme registrering flere gange?

Kontrol 7: Kontrol af, hvordan unikhed af registreringer håndteres i Salto DB	
Fremgangsmåde	Denne analyse er foretaget ved at undersøge en stikprøve af data fra Salto DB og undersøge unikheden af den enkelte registrering. Analysen forholder sig kun til data, som registreringsenhederne producerer til Salto DB, og kan derfor ikke udelukke fejl på selve enheden.
Resultat af kontrollen	Ved en kombination af felterne: • "EventDateTime" (dato- og tidsstempel for registrering) • "id_Object" (registreringsenheds id) • "id_Subject" (beboer id) • "EventCode" (registrering statuskode) kan samtlige registreringer i stikprøven identificeres unikt. Dvs. at ingen enheder i perioden for stikprøven har produceret en registrering til databasen med samme dato- og tidsstempel for samme beboer med samme statuskode. Det observeres, at Salto DB-tabellen "tb_LockAuditTrail" har en unik kolonne kaldet "InsertionCounter" (med "Unique"-constraint).
Overordnet konklusion	Ingen evidens for dataforvanskning fundet i kontrollen. Logikken i Salto DB vurderes at være tilstrækkelig til at sikre, at hændelser fra registreringsenhederne ikke kan være repræsenteret mere end én gang i databasen.

Dobbeltregistrering (adfærd): Forekommer samme registrering flere gange på kort tid fra samme person på en eller flere meldestander?

Kontrol 8: Undersøgelse af omfanget af dobbelte registreringer på meldestandere på Salto DB	
Fremgangsmåde	Denne delanalyse undersøger omfanget af dobbeltregistreringer på meldestandere i Salto DB for at bekræfte hypotesen om beboeres mistillid til meldesystemet, som fører til flere registreringer af samme beboer på en eller flere meldestandere. Dobbeltregistreringer er her defineret som to eller flere registreringer af samme beboer på en eller flere meldestandere inden for en afgrænset tidsperiode (her ti sekunder). Dette bliver undersøgt baseret på en stikprøve fra og med 1. januar 2021 til og med 30. januar 2021. På KHG er registreringer på følgende enheder betragtet: "khg_Meldestander 1", "khg_Meldestander 2", "khg_Meldestander 3" og "khg_Meldestander 4". På SJM er registreringer på følgende enheder betragtet: "SJM Meldepligt 2 TH", "SJM Meldepligt 1 TV" og "SJM Meldepligt 3".
Resultat af kontrollen	For KHG er der fundet i alt 4.327 dobbelte registreringer på meldestandere i perioden fra og med 1. januar 2021 til og med 30. januar 2021. For SJM er der fundet i alt 87 dobbelte registreringer på meldestandere i perioden fra og med 1. januar 2021 til og med 30. januar 2021.
Overordnet konklusion	Der er observeret et højt antal dobbelte registreringer ved meldestandere på begge centre, dog signifikant flere på Kærshovedgård end på Sjælsmark, (korrigeret for størrelsesforskel på centrene). Kontrol 7 har valideret, at disse dobbeltregistreringer ikke genereres ved en fejl i Salto DB, da logikken i Salto DB sikrer, at melderegistreringerne ikke gemmes mere end én gang i den respektive tabel. En forklaring på dobbeltregistreringerne kan i stedet være, at beboerne grundet mistillid til systemet eller manglende vejledning registrerer sig på alle 4 meldepligtsstandere ved hver aflæggelse af meldepligt.

Manglende registrering: Forkert kombination af registreringer (fx to på hinanden følgende registreringer ved indgang uden en udgangsregistrering).

Kontrol 9: Undersøgelse af omfanget af "Fejlagtig kombination af registreringer" på Salto DB

Fremgangsmåde	Denne delanalyse undersøger omfanget af forkerte kombinationer af registreringer (fx to på hinanden følgende registreringer ved indgang uden en registrering af udgang imellem. Dette kaldes også en fejlkobling). Analysen er baseret på en stikprøve fra og med 1. januar 2021 til og med 30. januar 2021. Analysen er foretaget ved at betragte beboerregistreringerne og validere, at en udgang er efterfulgt af en indgang og omvendt. På KHG er registreringer på følgende enheder betragtet som en udgang: "khg_Karrusel UD 2" og "khg_Modtagelse Streg UD", og følgende betragtet som en indgang: "khg_Karrusel IND 2" og "khg_Modtagelse Streg IND". På SJM er registreringer på følgende enheder betragtet som en udgang: "SJM Dør UD 2" og "SJM Stregkodescanner UD", og følgende betragtet som en indgang: "SJM Stregkodescanner IND" og "SJM Dør IND 2".
Resultat af kontrollen	For KHG er der fundet i alt 194 forkerte kombinationer af ind- og udregistreringer i perioden fra og med 1. januar 2021 til og med 30. januar 2021. Af disse er 147 (75 %) sket i forbindelse med registreringsenhederne "khg_Modtagelse Streg IND" eller "khg_Modtagelse Streg UD". For SJM er der fundet i alt 387 forkerte kombinationer af ind- og udregistreringer i perioden fra og med 1. januar 2021 til og med 30. januar 2021. Af disse er 248 (64 %) af dem sket i forbindelse med registreringsenhederne "SJM Stregkodescanner IND" eller "SJM Stregkodescanner UD".

Overordnet konklusion

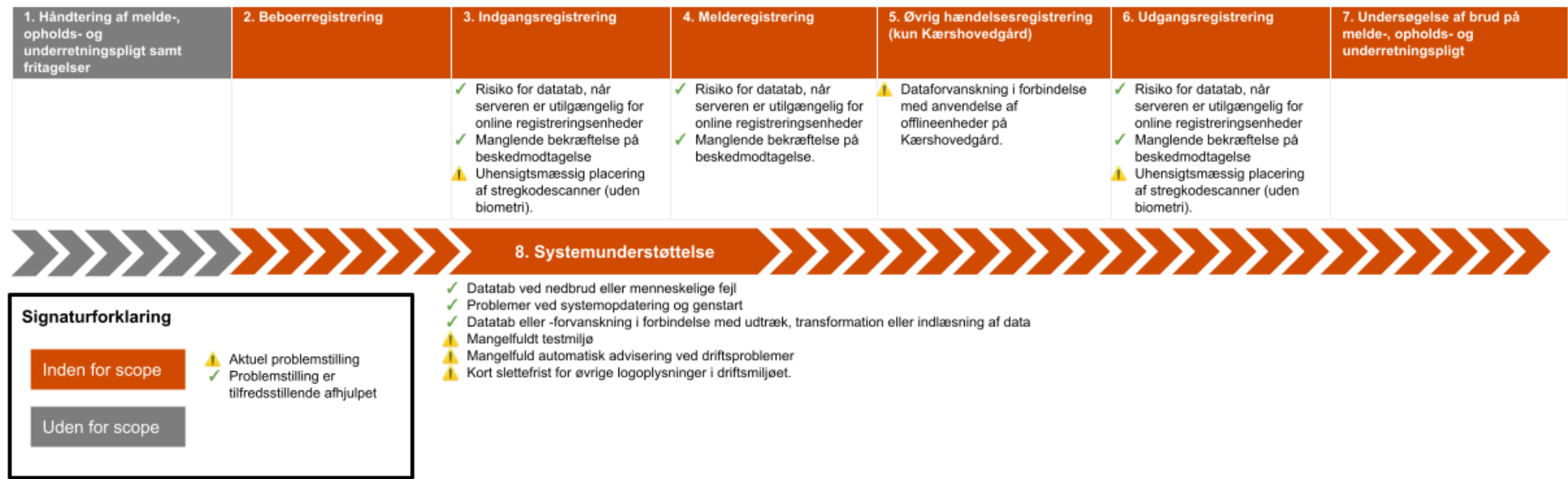
Der er observeret signifikant flere fejlkoblinger ved ind- og udgangsstregkodescannere end ved ind- og udgangssluser. Dette anses som en naturlig konsekvens af, at anti-passback ikke er slået til for stregkodekort. Se observation 9 "Anti-passback ikke implementeret for stregkodekort", hvor det anbefales, hvad der kan gøres for at reducere antallet af fejlkoblinger.

3.5.3 Gennemgang af observationer relateret til arkitekturen for AMS-komplekset

Dette afsnit præsenterer de it-arkitekturmæssige observationer, som undersøgelsen af AMS har ført til. Denne gennemgang af observationer og udfordringer tager udgangspunkt i den overordnede procesramme, som er præsenteret i afsnit 3.2, hvorudfra hver observation knyttes til en eller flere af delprocesserne i figur 13 nedenfor. Observationerne er i figur 13 kategoriseret efter, hvorvidt der fortsat er en aktuel problemstilling, eller om det i undersøgelsen er vurderet, at en identificeret

problemstilling er blevet tilfredsstillende afhjulpnet. I afsnittet gennemgås observationerne i figur 13 kronologisk på de følgende sider. Delproces 1 er uden for undersøgelsens primære genstandsfelt, og da der ikke er identificeret nogen observationer relateret til arkitektur i delproces 2, starter gennemgangen af arkitekturrelaterede observationer med delproces 3.

Figur 13. Overblik over aktuelle problemstillinger samt afhjulpne problemstillinger, der relaterer sig til arkitektur



Observationer relateret til delproces 3, 4 og 6: Indgangs-, melde- og udgangsregistrering

Ind- og udgangsregistrering sker på samme måde på både KHG og SJM, og observationerne på tværs af disse delprocesser er derfor identiske. I melderegistreringen er der også et stort overlap med observationer, da det er de samme registreringsenheder, der benyttes. Således præsenteres to observationer, der relaterer sig til både indgangs-, udgangs- og melderegistreringen, mens den sidste observation (observation 1), der præsenteres, udelukkende relaterer sig til den øvrige hændelsesregistrering på KHG.

22. Risiko for datatab, når serveren er utilgængelig for online registreringsenheder	
Prioritet	1
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Det kan forventes, at registreringsenhederne af forskellige årsager på visse tidspunkter kan miste forbindelsen til Salto-serveren hos SIT. Fx kan MPLS-forbindelsen, Salto-applikationen eller Salto DB være utilgængelig i kortere perioder ad gangen. I dette tilfælde vil enhedernes registreringer ikke bliver registreret i Salto DB. Systemet bør derfor være designet til, at der kan være utilgængelige perioder, hvor registreringsenhederne ikke kan få forbindelse til serveren.
Risiko-beskrivelse	Hvis systemet ikke i tilstrækkeligt omfang er designet til at kunne håndtere, at der i perioder ikke er forbindelse til serveren, er der en risiko for, at der sker datatab af de registreringer, der finder sted, mens serveren er utilgængelig.
Kendte eksisterende kontroller	Ifølge leverandøren Sanistål er der ved manglende netværks- eller serverforbindelse lokal lagring af data ved den kontrolboks, som sidder på registreringsenheder med onlineforbindelse. For de ældre enheder er der lagerplads til at kunne opbevare de seneste 3.000 registreringer, mens der på nyere enheder kan opbevares op til 5.000 registreringer. Når der igen er forbindelse, afleveres alle de registreringer, som ikke tidligere kunne blive afleveret. Registreringerne opbevares efter "first in, first out"-princippet således, at de ældste registreringer "smides ud", når nye registreringer kommer til.
Anbefalinger til yderligere tiltag	
Ingen yderligere anbefalinger	Det vurderes, at den eksisterende lagringsplads på enhederne er tilfredsstillende for at sikre, at der ikke sker datatab. Dette skyldes, at den enhed med langt flest gennemsnitlige registreringer (indgangskarrusellen ved KHG) gennemsnitligt har ca. 400 registreringer om dagen. Der skal således i gennemsnit gå over en uge uden adgang til serveren, før de første af de 3.000 registreringer ikke længere kan opbevares på standen. Interviewene på begge udrejsecentre har peget på, at der meget sjældent opleves systemnedbrud, og at disse typisk ikke varer ved i lang tid. Det vurderes ikke, at det er nødvendigt, at systemet opgraderes til at kunne opbevare flere registreringer således, at systemets maksimale tålelige nedetid udvides til endnu længere end en uge.

23.Manglende bekræftelse på beskedmodtagelse	
Prioritet	1
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Når de online registreringsenheder kommunikerer med Salto-applikationen, kan det forventes, at enhederne på visse tidspunkter kan miste forbindelse til serveren hos SIT (jf. beskrivelse i observation 22). Sanistål har bekræftet, at beskeder fra online registreringsenheder sendes via User Datagram Protocol (UDP), som ikke i sig selv understøtter, at der i en kommunikation mellem to enheder er sikkerhed for, at alle afsendte beskeder når sikkert frem til modtageren – modsat Transmission Control Protocol (TCP), som understøtter netop dette.
Risiko-beskrivelse	Såfremt der ikke på anden vis er implementeret denne sikkerhed for, at UDP-beskederne modtages og gemmes i Salto DB, vil der være risiko for, at ikke alle registreringer gemmes i Salto DB.
Kendte eksisterende kontroller	Det er blevet bekræftet af producenten Salto, at der i applikationskoden i Salto-applikationen er indbygget et kontrollag, der sikrer, at UDP-beskeder altid modtages, og at samme besked ikke gemmes flere gange. Denne implementering er lavet med to forskellige integrationsmønstre – ét mønster for enheder af typen CU4200 og et andet mønster for enheder af typen CU5000. For en nærmere uddybning af disse to integrationsmønstre, se faktaboks 1 i afsnit 3.5.1, som gennemgår arkitekturen.
Anbefalinger til yderligere tiltag	
Ingen yderligere anbefalinger	Det vurderes, at den iboende risiko for, at beskeder ikke modtages, er fuldt mitigeret af det kontrollag, som producenten har implementeret uden for UDP-beskederne. Det bemærkes, at det ikke har været muligt at få adgang til Saltos kodebase, da det er et proprietært stykke software, som producenten ikke ønsker at udlevere. Der er dog ingen indikationer fra dataanalysen på, at producentens beskrivelse ikke er en præcis angivelse af den faktiske implementering.

3. Uhensigtsmæssig placering af stregkodescanner (u. biometri)	
Prioritet	2
Udrejsecenter	KHG
Beskrivelse af problemstilling	Ud- og indgangsscannerne i portvagten på KHG (stregkodescanner uden biometri) er placeret tæt på hinanden, hvilket indebærer en risiko for, at en medarbejder kommer til at foretage en registrering af en passage i den forkerte retning, fx registrering af en indgang, som skulle have været en udgang.
Risiko-beskrivelse	Hvis medarbejderen ved en fejl laver en forkert registrering (fx en udgang fremfor en indgang), vil nedbringe validiteten af datagrundlaget i hændelsesloggen i forhold til beboerens færden.
Kendte eksisterende kontroller	Der er etableret anti-passback på både KHG og SJM, således at der ikke kan foretages to på hinanden følgende passager i samme retning, fx to udgange. Anti-passback er dog pt. kun aktiveret ved brug af biometriske adgangskort. Det udestår at undersøge, om anti-passback kan etableres på stregkodescannere, ligesom der skal etableres en procedure for håndtering af sådanne spærringer, når de opstår.
Anbefalinger til yderligere tiltag	
Anbefaling 1.1	Det anbefales, at stregkodescannerne ved ind- og udgangsregistrering i portvagten placeres med større afstand imellem for at reducere risikoen for, at der sker en forkert registrering. Herudover anbefales det, at der aktivt fokuseres på at reducere anvendelsen af stregkodekort på KHG ved at introducere håndscannere i portvagten til biometriske kort på KHG ligesom på SJM, samt ved at overgå til FUSE-kort på KHG ligesom på SJM, da erfaringerne indtil videre er, at disse er mere stabile i drift.

Observationer relateret til delproces 5: Øvrig hændelsesregistrering (kun KHG)

Observation 1, Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG, er en sammenfatning af udfordringer, der er kogt ned til én observation, som vedrører delproces 5.

1. Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG	
Prioritet	1
Udrejsecenter	KHG
Beskrivelse af problemstilling (årsager til dataforvanskning)	• Tidsforskydning: Systemdistributøren og installationsleverandøren har oplyst, at klokkeslættet i tidsstyringsenhederne i offlineregistreringsenhederne (fx låse til værelsesdøre) erfaringsmæssigt tidsforskydes mellem gensynkroniseringer, og at offlineenhederne skal gensynkroniseres regelmæssigt, hvis data (tidsstempellerne) i enhederne skal være valide i forhold til beboernes reelle færden. Leverandørerne kender ikke den præcise tidsforskydning, men formoder, at denne udgør ca. +/- to minutter pr. måned (hvis der ikke gensynkroniseres løbende). Ifølge leverandøren bør offlineenheder opdateres ugentligt, ligesom der bør være opmærksomhed på, at de ved batteriskift skal opdateres for at sikre imod, at enhederne tilbagesendes til fabriksindstillingen (inklusive tidsstempel). • Beboeradfærd: PwC har på baggrund af interviews og besigtigelse noteret, at beboerne på flere forskellige måder forsøger at omgå registrering af ind- og udgange af døre på værelser, fællesarealer og lignende, fx ved at placere sko i dørene, holde døre for øvrige beboere mv. • Registreringer fra besigtigelser er foretaget korrekt, men fremgår ikke efterfølgende af hændelsesloggen.
Risiko-beskrivelse	Ovenstående problemer udgør tilsammen en væsentlig risiko for forvanskning af data i fra offlineenheder. Hermed vil inddragelse af data fra offlineenheder i AMS nedbringe validiteten i det samlede datagrundlag og dataflow.
Kendte kontroller	Der er ikke identificeret relevante kontroller i undersøgelsen.
Anbefalinger til yderligere tiltag	
Anbefaling 1.1	Det anbefales, at data fra offlineenheder afkobles fra AMS, da tidsforskydning i registrering her fra offlineenheder og beboeradfærden tilsammen udgør en væsentlig risiko for forvanskning af data. Hermed udgør inddragelse af data fra offlineenheder i AMS en væsentlig risiko for at nedbringe validiteten af data i AMS.

Observationer relateret til delproces 8: Systemunderstøttelse

I dette afsnit gennemgås alle observationer under delproces 8 på tværs af aktiviteter.

20. Datatab ved nedbrud eller menneskelige fejl

Prioritet	1
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Der er identificeret ét tilfælde, hvor en sagsgennemgang viste, at en medarbejder ved en fejl havde slettet en datadisk på Salto-serveren på et tidspunkt den 10. juni 2020, og man kunne konstatere, at der manglede data i tidsrummet fra den 9. juni 2020 kl. 22:16:39 til den 10. juni 2020 kl. 10:18:16. Det var muligt at genskabe dele af de tabte data for perioden 9. juni 2020 kl. 22:16:39 til 10. juni 2020 kl. 00.00.00. (for ind- og udgange). Data fra den resterende periode (00.00.01 til 10.18.16) var det imidlertid ikke muligt at genskabe.
Risiko-beskrivelse	Hvis der opleves datatab (fx i tilfælde af menneskelige fejl som ved denne hændelse), vil data kunne gendannes automatisk fra seneste backup eller ved en smule mere indsats fra transaktionslogs, hvis disse produceres hyppigere end databasebackups. Der er således en risiko for, at registreringer foretaget efter seneste tidspunkt for backup/transaktionslog kan være umulige at gendanne.
Kendte eksisterende kontroller	UIM-KIT, som er ansvarlig for drift af Salto DB, oplyste under interviewet med SIT, at man har implementeret fuld backup af Salto DB hver aften, og at man genererer inkrementelle transitionslogs hver time. Hvis en utilsigtet hændelse kun rammer databasen (som i tilfældet med den slettede datadisk), vil data altså kunne gendannes med en times interval. Dvs. at der maksimalt kan ske et datatab på en time. Hvis den utilsigtede hændelse derimod rammer hele serveren (fx ved en brand), vil transaktionslogfilerne også være utilgængelige, og data skal således gendannes fra seneste fulde databasebackup. Det fremgår af den reviderede redegørelse om datanedbruddet (bilag 2), at der er opsat ekstra overvågning af serveren, som Salto ProAccess Space kører på, på baggrund af nedbruddet i perioden 2.-3. juli 2020, så denne type fejl fremover vil kunne blive fanget langt hurtigere.

Anbefalinger til yderligere tiltag

Ingen yderligere anbefalinger	• Det vurderes, at implementeringen af daglige fulde backups samt inkrementelle backups i form af transaktionslogfiler hver time er tilstrækkelige indsatser for at reducere konsekvenserne, hvis et datatab foranlediget af en utilsigtet hændelse skulle indtræffe igen. • Det vurderes desuden som tilfredsstillende, at der er implementeret yderligere serverovervågning for at sikre, at lignende hændelser i fremtiden hurtigere vil kunne identificeres, og at der således hurtigere kan reageres på disse.
--------------------------------------	--

21. Problemer ved systemopdatering og genstart

Prioritet	1
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Der er registreret nedbrud på Salto-systemet den 2.-3. juli 2020 og den 17. juli 2020, som angiveligt skyldtes, at systemservice på den server hos SIT, som Salto-systemet er placeret på, ikke genstartede automatisk efter opdateringer af serveren, selvom det er konfigureret til at gøre dette.
Risiko-beskrivelse	Hvis Salto-systemet ikke startes korrekt op, har det flere konsekvenser i den tidsperiode, hvor det er utilgængeligt: • Beboerregistrering, ind-/udgangsregistrering og melderegistrering kan ikke afvikles med den normale systemunderstøttelse, og der skal derfor indføres manuel kontrol/registrering i alle disse trin. • Registreringer fra Salto-systemet fra det tidsrum, hvor Salto-systemet er utilgængeligt, kan ikke anvendes til anmeldelse af eventuelle overtrædelser.
Kendte eksisterende kontroller	Det er blevet oplyst, at AMS før den 17. juli 2020 ikke var konfigureret til at genstarte repeteret, men at dette blev iværksat efter den 17. juli 2020. En repeteret genstart har til hensigt at sikre, at AMS starter op korrekt i fremtiden. Det er i interviewet med UIM-KIT blevet valideret, at den nye genstartsprocedure er blevet implementeret og testet således, at problemet ikke vil opstå i fremtiden.

Anbefalinger til yderligere tiltag

Ingen yderligere anbefalinger	Der anbefales ikke yderligere tiltag, idet det vurderes, at den implementerede genstartsprocedure effektivt sikrer, at der ikke igen opstår problemer ved genstart efter en systemopdatering.
--------------------------------------	---

19. Mangelfuldt testmiljø	
Prioritet	3
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Der er ikke et testmiljø, hvor det kan sikres, at ændringer i systemlandskabet implementeres og testes, inden de rulles ud i produktionsmiljøet.
Risiko-beskrivelse	Hvis der ikke er et testmiljø til at sikre, at nye systemopdateringer, patches til servere, ændringer til eksisterende integrationer, helt nye integrationer og andre ændringer i det samlede systemkompleks testes igennem, inden de rammer produktionsmiljøet, er der en risiko for, at eventuelle uhensigtsmæssigheder, fejl og uventede hændelser indtræffer i selve produktionsmiljøet, hvor det vil være kritisk og eventuelt kan føre til dataforvanskning.
Kendte eksisterende kontroller	Ved oprettelse af en beboers kort er der førstegangslæsere på begge udrejsecentre, som anvendes til at teste, at kortet er blevet oprettet korrekt – uden at registreringen medfører en registrering i produktionsdatabasen, der kan skabe støj. Der er ikke identificeret yderligere foranstaltninger til at teste systemændringer, inden de rammer produktionsmiljøet.
Anbefalinger til yderligere tiltag	
Anbefaling 8.1	Det anbefales, at der designes en samlet teststrategi for systemkomplekset. Strategien skal designes nærmere, men kunne fx indeholde: • Et testmiljø, fx bestående af: ○ En testserver identisk med Salto-serveren ○ En Salto-testdatabase med fiktive registreringer og fiktive beboere ○ Testidentitetskort tilhørende fiktive beboere ○ Testregistreringsenheder (enten dedikerede testenheder, hvis UDP-beskeder peger på Salto-testdatabasen frem for den normale, eller mulighed for, at normale enheder kan kodes til at sende til testdatabasen, hvis der anvendes testidentitetskort) • Integrationstestprocedurer, hvor testidentitetskort benyttes på testregistreringsenheder for at teste, at tidsregistreringerne ender i Salto-testdatabasen • Testperiode på testserver, inden nye patches rulles ud i produktion • Beredsskabstests, hvor der testes for forskellige mulige problematiske scenarier, som det samlede system bør kunne håndtere (fx at VPN-forbindelsen er nede) • Faste testprocedurer ved tilbagevendende begivenheder (fx faste procedurer for, hvordan opsætning af en ny registreringsenhed testes – også med fokus på at teste, om data korrekt ender helt ude i enden af dataflowet i QlikView).

13. Mangelfuld automatisk advisering ved driftsproblemer	
Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	HJEMST og Kriminalforsorgens medarbejdere får ikke automatisk besked om driftsforstyrrelser på AMS fra SIT eller UIM-KIT.
Risiko-beskrivelse	Manglende advisering om systemnedbrud kan have forskellige konsekvenser: • Hvis Kriminalforsorgens medarbejdere ikke via et dashboard kan få indsigt i eller automatisk adviseres, når der opstår driftsproblemer, skaber det unødige udfordringer på udrejsecentrene, som kunne være håndteret hurtigere. • Hvis HJEMST's medarbejdere ikke er bevidste om en relevant driftsforstyrrelse, når en potentiel anmeldelse behandles, kan det i yderste konsekvens føre til, at der fejlagtigt laves en anmeldelse for en pligtovertrædelse.
Kendte eksisterende kontroller	SIT og UIM-KIT har et fælles setup for overvågning, hvor der i Microsoft System Center Operations Manager (SCOM) er blevet opsat overvågning og alarmer for servernes kapacitet (RAM, CPU og opbevaringsplads). Overvågning af applikationssoftware håndteres alene af UIM-KIT i systemet Capmon. Hvis der i de automatiske alarmer og overvågninger identificeres en fejl, som er relevant for personer hos HJEMST, Udlændingestyrelsen og/eller Kriminalforsorgen, kommunikerer det ud via e-mail efter en manuel proces. Der er en dedikeret mailadresse hos HJEMST, hvor dette kommunikerer ud. Der er dog ikke nogen alarmer, der udløser nogen automatiske notifikationer til andre end UIM-KIT og SIT.
Anbefalinger til yderligere tiltag	
Anbefaling 23.1	Det anbefales, at der etableres et løbende driftsoverblik (fx dashboard) over AMS og etableres en proces for fremsendelse af automatisk advisering til både Kriminalforsorgens medarbejdere på udrejsecentrene (til e-mailadresser på begge centre) samt til HJEMST's og US' e-mailadresser til formålet (anmeldelser@hjemst.dk) og (indkvarteringsvilkaar@us.dk).

16. Kort slettefrist for øvrige logoplysninger i driftsmiljøet	
Prioritet	3
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Nogle typer af logs (applikations-, system- og SQL-logs) slettes efter relativt kort tid (fx ca. ni måneder for applikationsloggen), hvilket kan være en udfordring i forbindelse med gennemgang af retslige sager, hvor historiske hændelser i logoplysningerne ellers kan bidrage til opklaringen af sagen. I en hændelsesredegørelse fremgår det således, at Koncern IT/SIT ikke samlet set har kunnet levere de efterspurgte logoplysninger til at kaste lys over nogle specifikke sager (jf. "Redegørelse for hændelse i Salto-systemet", side 4).
Risiko-beskrivelse	Hvis der opstår tvivlsspørgsmål i en sag, der ligger mere end ni måneder tilbage, vil der i de fleste tilfælde være de fornødne oplysninger til stede for at undersøge mulige fejl, givet at de vigtigste logoplysninger gemmes i mere end ni måneder. Men visse typer af hændelser vil ikke længere fremgå efter ni måneder. Fx vil det kun være SQL-loggen (som blot gemmes i ni måneder), der har oplysninger om tilfælde, hvor en medarbejder med administratoradgang ved en fejl har slettet én eller flere rækker direkte i databasen. I langt de fleste tilfælde vil det sandsynligvis ikke være nødvendigt at anvende disse øvrige logoplysninger.
Kendte eksisterende kontroller	Andre logs (fx Salto-servicelog og driftsovervågning) kunne godt leveres i forbindelse med den pågældende hændelsesredegørelse. Det er dog uklart, 1) hvor lang tid de forskellige logs gemmes, og 2) om der er foretaget en konkret vurdering af, hvilke logs der er nødvendige for at kunne løfte bevisbyrden i en given sag.
Anbefalinger til yderligere tiltag	
Anbefaling 3.1	Det anbefales, at der foretages en vurdering af, hvor langt tilbage i tiden, man i HJEMST ønsker at kunne foretage anmeldelser af pligtovertrædelser, og at levetiden for de forskellige typer af logs herefter justeres efter dette.

24. Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data	
Prioritet	1
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	En af grundene til, at indeværende undersøgelse er blevet igangsat har været, at der grundet tidligere hændelser er blevet sået tvivl om, hvorvidt der på et tidspunkt i dataflowet kan forekomme enten et tab eller forvanskning af data. I dataanalyserne i afsnit 3.5.2 har kontrol 1-7 til formål at kaste lys på, om der kan påvises nogen form for datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data på et tidspunkt i dataflowet.
Risiko-beskrivelse	Hvis der sker datatab eller forvanskning i dataflowet til og med Salto DB, vil det underliggende datagrundlag for anmeldelser af beboere være fejlbehæftet. Hvis der efterfølgende i dataflowet sker datatab eller forvanskning, kan det betyde, at det datagrundlag, som anvendes af HJEMST's medarbejdere til vurdering af potentielle anmeldelser, kan være fejlbehæftet.
Kendte eksisterende kontroller	Salto DB har en kontrol, der sikrer, at alle nye hændelser, der indsættes i databasen er unikke.
Anbefalinger til yderligere tiltag	
Ingen yderligere anbefalinger	Der er ikke blevet påvist nogen form for hverken dataforvanskning eller datatab i de udvalgte tekniske komponenter i dataflowet, som har indgået i kontrol 1-7 i indeværende dataanalyser, og der er således ingen yderligere anbefalinger (læs mere under selve beskrivelsen af kontrol 1-7 i afsnit 3.5.2). Det kan dog overvejes, om den kode, der er blevet udviklet for at kunne gennemføre kontrol 1-7 i dataanalyserne skal genbruges og implementeres som løbende kontroller i dataflowet med automatiske alarmer og notifikationer.

3.6 Governance, risk og compliance

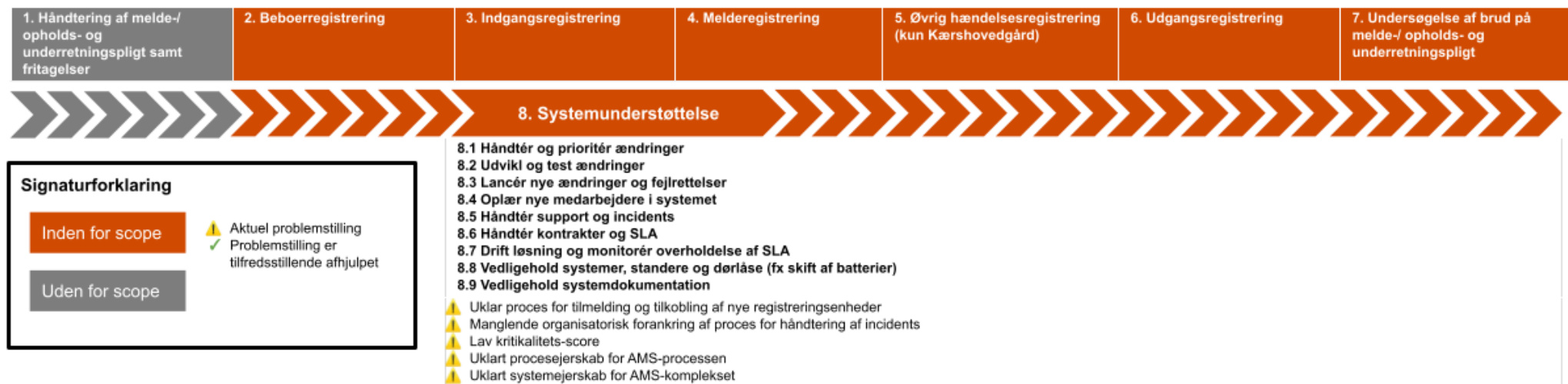
Dette afsnit præsenterer og uddyber observationer relateret til området i PAVA-modellen (Proces, Adfærd, Validering og Arkitektur) om governance, risici og compliance (regelefterlevelse), som er identificeret i forbindelse med undersøgelsen af AMS. Det vil sige, at observationerne er rammesættende for de andre områder i PAVA-modellen, hvorved flere af observationerne går på tværs af de andre områder i PAVA-modellen og har mere generel karakter end flere af de ovenfor beskrevne observationer. Det vil også sige, at alle observationer i dette afsnit er gældende for både KHG og SJM. Eksempelvis er det uklart, hvilken organisation/instans/person(er) som har det overordnede procesejerskab for AMS på tværs af processen (fra step 1 til 7 i procesdiagrammet) og hermed ansvaret for bibeholdelse af kontroltrykket i forhold til de tildelte til beboerne på udrejsecentrene. Denne observation har betydning for hvert af de andre PAVA-områder. Gennemgangen af observationer og udfordringer tager udgangspunkt i den overordnede procesramme, som er præsenteret i afsnit 3.2,

hvorudfra hver observation knyttes til en eller flere af delprocesserne herunder (se Figur 14).

Som det fremgår af procesdiagrammet, er alle observationer relateret til governance, risk og compliance placeret under procestrin 8. Årsagen er, at dette trin er tværgående for AMS og hermed også observationerne, som alle er tværgående i karakter. Derfor struktureres dette afsnit i det efterfølgende efter observationer startende med højest kritikalitet og nedefter, herunder:

- Uklar proces for tilmelding og tilkobling af nye registreringsenheder
- Manglende organisatorisk forankring af proces for håndtering af incidents
- Lav kritikalitetsscore
- Uklart procesejerskab for AMS-processen
- Uklart systemejerskab for AMS-komplekset.

Figur 14. Procesdiagram for AMS – governance



3.6.1 Uklar proces for tilmelding og tilkobling af nye registreringsenheder

Der er identificeret én observation, som har prioritet 1, da den afledte problemstilling i sig selv indebærer en risiko for datatab. Det drejer sig om de tilfælde på begge udrejsecentre, hvor der skal tilmeldes og tilkobles nye registreringsenheder ved ind- og/eller udgang samt i forbindelse med melderegistrering. Det bemærkes, at der er tale om en observation, som ikke er baseret på en besigtigelse, men udelukkende interview, hvorfor det ikke er muligt at konkludere, om der historisk set har været datatab på denne baggrund.

2. Uklar proces for tilmelding og tilkobling af nye registreringsenheder	
Prioritet	1
Udrejsecentre	KHG og SJM
Beskrivelse af problemstilling	Det er i forbindelse med interview med Koncern IT i UIM-KIT observeret, at registreringerne af beboernes passager og meldepligt ikke automatisk indgår i data. Forudsætningen er, at en registreringsenhed skal inkluderes i dataflowet (ikke filtreres fra), så de daglige udtræk indeholder hændelser fra den pågældende registreringsenhed. Hvis registreringsenheden ikke er inkluderet i det videre dataflow, så kommer disse data ikke med, og en beboers færden vil ikke fremgå af rådataloggen i QlikView. Det betyder først og fremmest, at hvis der opsættes nye enheder på udrejsecentrene, så er det essentielt at huske at orientere UIM-KIT, så det sikres, at disse enheders registreringer også kommer med i filtreringen.
Risiko-beskrivelse	Det har i undersøgelsen ikke været muligt at identificere en formaliseret proces for sikring af, at nye registreringsenheder (fx nye registreringsenheder ved ind-/udgangskarrusseler og meldestandere) inkluderes i dataflowet (særligt hændelsesjobs i Salto DB). Det er samtidig uklart, hvorvidt det er HJEMST (vilkårene på udrejsecentrene), Udlændingestyrelsen (kontrakt- og bevillingsejer), (Kriminalforsorgen) eller leverandørerne, der har dette ansvar. Det er også uklart, om en advisering skal gå til UIM-KIT eller SIT (ansvarlig for drift af servicenetværk og database). Der er således risiko for, at information om nye registreringsenheder ikke gives videre til UIM-KIT eller SIT, så udtræk af data fra AMS ikke længere afspejler beboerens færden for de pågældende registreringsenheder.
Kendte eksisterende kontroller	Der er ikke identificeret relevante kontroller i undersøgelsen.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at der etableres og implementeres en formaliseret proces for tilmelding af nye registreringsenheder til de ansvarlige for drift og opsætning af udtræk (filtrering/jobs) i forhold til at sikre, at registreringsenhedens hændelser medtages i hændelsesjobs i Salto DB.

3.6.2 Uklar proces for håndtering af incidents

Der er identificeret to observationer, som har prioritet 2, dvs., at de kan have væsentlig betydning i forhold til eventuel dataforvanskning og/eller datatab. Det drejer sig om de tilfælde, hvor en hændelse (incident) har negativ påvirkning på driften af AMS, fx i form af et servicenedbrud, fejl i en genstartsprocedure, problemer med servicenetværket mv. Formålet med håndtering af incidents er således at identificere problemstillingen og genskabe sikker drift af AMS på niveau med de aftalte servicestandarder (SLA'er) så hurtigt og effektivt som muligt.

4. Manglende organisatorisk forankring af proces for håndtering af incidents

Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Der er dokumenteret en incident den 10. juni 2020, hvor en medarbejder ved en fejl fjernede og slettede data fra Salto-serveren. I den forbindelse blev UIM ved en fejl ikke orienteret om hændelsen samt udbedring af fejlen. Denne enkeltstående observation er gennem interviews med UIM KIT, HJEMST samt udrejsecentrene umiddelbart udtryk for en generel problematik omkring processen for håndtering af incidents.
Risiko-beskrivelse	Der er risiko for, at uklarhed omkring rolle-/ansvarsfordelingen i processen for håndtering af incidents kan medføre, at der ikke reageres rettidigt ved systemnedbrud, samt at der ikke iværksættes procesmæssige "workarounds" for at sikre, at AMS-processen kan fortsætte med en alternativ proces, mens eventuelle systemnedbrud pågår. Samtidig kan det have som konsekvens, at der bruges fejlbehæftede data i retsmæssig sammenhæng, hvis HJEMST og/eller UIM ikke er bevidste om, at der har været problemer med systemet i den periode, hvor en incident har fundet sted.
Kendte eksisterende kontroller	Incident-proces: Der er blevet etableret en "to-be" incident-proces, som redegør klart for ansvarsfordelingen mellem 1st line incident-håndtering (dispatch), 2nd line incident-håndtering (drift og support), 3rd line incident-håndtering (systemforvaltning), SIT samt andre tredjeparter og systemleverandører. Samtidig fremgår det af denne to-be incident-proces, at der skal vedligeholdes en Known Error Database (KEDB) med henblik på at sikre, at kendte fejl registreres, beskrives og håndteres. Det er uklart, hvad status er på implementeringen af denne to-be-proces.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at den udarbejdede proces for håndtering af incidents implementeres og forankres blandt alle interessenter i AMS-processen, således at der skabes større klarhed omkring, hvordan og til hvem der skal tages kontakt i forbindelse med nye incidents samt supportspørgsmål.

3.6.3 Lav kritikalitetsscore

Den anden observation med prioritet 2 er også relateret til incident-processen og omhandler prioritering af incidents relateret til AMS, herunder reguleringen af samme i kundeaftalen mellem leverandøren SIT og UIM.

5. Lav kritikalitetsscore	
Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	I kundeaftalen mellem UIM og SIT er ansvarsfordelingen mellem organisationerne beskrevet såvel som procedurer for prioritering af incidents relateret til kundeaftalen, særligt infrastruktur, herunder servere, netværk på udrejsecentrene mv. Det fremgår af kundeaftalen (bilag 6, urgency impact), at kritikaliteten af AMS er vurderet til niveau "D", som er det laveste niveau i SIT's kundeaftaler. Niveau D definerer nedbrud i driften (AMS) med følgende konsekvenser: Mindre ulemper og begrænsede tab eller omkostninger. Denne kategorisering er påfaldende lav set i forhold til, hvor kritisk data fra Salto-systemet er til brug som grundlag i anmeldelsessager.
Risiko-beskrivelse	Kritikalitetsvurderingen af AMS til niveau "D" kan medføre, at medarbejdere i SIT nedprioriterer incidents, der er relateret til AMS, og at der dermed ikke følges op i tide på disse incidents med risiko for datatab.
Kendte eksisterende kontroller	Ifølge Bilag 3 er der i SIT blevet gjort følgende i SIT for at forbedre incident-håndteringsprocessen: - Der er blevet indskærpet over for involverede medarbejdere, at fejl skal meldes direkte til systemejere. - Der er blevet kommunikeret klart ud i SIT, at eksisterende retningslinjer skal læses og følges. - Disse retningslinjer inkluderer fx, at UIM's vagttelefon skal kontaktes ved genstart af server, hvor Salto-systemet er installeret (hvilket ikke skete i forbindelse med en tidligere hændelse).
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at AMS' kritikalitet revurderes og opjusteres fra den nuværende klassifikation "D" til enten niveau "A" eller "B", idet det kun er i disse kategorier, at systemnedbrud vurderes at kunne føre til væsentlige brud på målopnåelse for myndigheden, hvilket vurderes at være tilfældet for AMS. Formålet med opjusteringen af systemets kritikalitet er at sikre en hurtigere genopretningstid til

normal drift, når der indtræffer incidents, givet at niveau A og B systemer prioriteres højere i incidenthåndteringen.

3.6.4 Uklart procesejerskab for AMS-processen

Der er endvidere to observationer kategoriseret som prioritet 2, som relaterer sig til selve organiseringen og governance omkring AMS. Det drejer sig i et it-perspektiv om procesejerskabet og systemejerskabet i AMS. Observationerne skal ses i lyset af en kompleks og uklar fordeling af opgaver og ansvarsområder på tværs af interne som eksterne aktører i relation til AMS. Nedenfor er aktørernes rolle i forhold til AMS beskrevet:

- *UIM* varetager opgaver inden for drift og systemforvaltning (særligt datasikkerhed og systemovervågning) af databaserne og netværk med SIT som leverandør på visse driftsopgaver.
- *HJEMST* varetager pr. 1. august 2020 en række opgaver vedrørende vilkårene for de personer, som befinder sig i hjemrejsefasen, herunder motivationsfremmende foranstaltninger. *HJEMST* træffer bl.a. afgørelse om opholds-, underretnings- og meldepligt, kontrollerer overholdelse og foretager politianmeldelse ved overtrædelse.
- *US* har pr. 1. august 2020 overdraget ansvaret til *HJEMST* for området og kontrollen med overholdelsen af opholds-, underretnings- og meldepligten (meldepligt overdraget fra politiet) – ligesom centrale medarbejdere og kompetencer som følge heraf er overdraget til *HJEMST*. Udlændingestyrelsen har fortsat ansvaret for den overordnede driftsopgave af centrene i henhold til operatørkontrakten med Kriminalforsorgen, herunder visse fysiske og adfærdsmæssige tilsyn på centrene og kontrakt- og leverandørstyring vedrørende det fysiske setup i forhold til Kriminalforsorgen og systemleverandører (Sanistål, Actas og Holstebro Låseteknik).
- *SIT* leverer it-understøttelse til AMS-processen, herunder servere, databaser, netværk mv. Det indebærer, at der er en overordnet kundeaftale, som regulerer ansvarsfordelingen med UIM, herunder også aftale om standarddriftsplatform.
- *Udrejsecenter KHG* og *Udrejsecenter SJM* er åbne centre med døgnbemanding, videoovervågning og adgangskontrol. Beboerne er ikke frihedsberøvede og kan derfor frit komme og gå på centret. Beboerne vil dog som udgangspunkt være underlagt såkaldt melde- og opholdspligt. Det betyder, at de har pligt til at bo og overnatte på centret.

- *Kriminalforsorgen* driver, med udgangspunkt i en operatørkontrakt med US, de to udrejsecentre for afviste asylansøgere, mennesker, der er udvist ved dom, samt mennesker på tålt ophold.
- *Sanistål* (leverandør til begge udrejsecentre) er leverandør af biometriske kort og grossist på licenser til AMS, som er installeret på en server hos SIT samt på en pc på Udrejsecenter SJM og en pc på Udrejsecenter KHG.
- *Actas* (lokal leverandør) har ansvaret for installation, drift og vedligehold af diverse systemkomponenter og enheder på Udrejsecenter SJM.
- *Holstebro Låseteknik* (lokal leverandør) har ansvaret for installation, drift og vedligehold af diverse systemkomponenter og enheder på Udrejsecenter KHG.

Hertil kommer yderligere aktører i relation til AMS, nemlig politiet og Anklagemyndigheden, som dog begge er udenfor denne undersøgelses genstandsfelt. politiet modtager anmeldelser fra US/HJEMST omkring overtrædelse af en kontrolforpligtelse eller kontrolforpligtelser; Anklagemyndigheden er ansvarlig for at føre anmeldelsessager. På baggrund af oplysningerne, der via registreringer i AMS opbevares i databaser hos SIT, undersøger HJEMST, om der er sket en overtrædelse af en eller flere kontrolforpligtelser. Hvis HJEMST konstaterer, at der er sket en overtrædelse af en eller flere pligter, fremsendes en anmodning om indledning af en straffesag efter udlændingelovens § 60 til Anklagemyndigheden i den lokale politikreds.

6. Uklart procesejerskab for AMS-processen	
Prioritet	2
Udrejsecentre	KHG og SJM
Beskrivelse af problemstilling	Det er uklart, hvilken organisation eller aktør, som har det samlede procesejerskab for AMS på tværs af dataflowet. Eksempelvis har Udlændingestyrelsen fortsat det kontraktuelle og bevillingsmæssige ansvar samt ansvar for tilsyn i medfør af operatørkontrakten med Kriminalforsorgen. Heroverfor er HJEMST ansvarlig for kontrol med overholdelsen af de af HJEMST pålagte pligter på centrene samt håndtering af beboernes pligter i det daglige. Dette forhold skaber uklarhed, fx i forbindelse med leverandørkontakt som beskrevet ved incidents ovenfor.
Risiko-beskrivelse	Der er risiko for, at den samlede AMS-proces ikke lever op til de forretningsmæssige og forvaltningsmæssige mål om at opretholde kontroltrykket i forhold til beboernes pligter. Det kan have en effekt på tilstedeværelse samt kvalitet og validitet af data, hvorved data ikke afspejler beboernes reelle færden.
Kendte eksisterende kontroller	Der er ikke identificeret relevante kontroller i undersøgelsen.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at der implementeres et egentligt procesejerskab i overensstemmelse med gældende best practice, særligt med henblik på entydig ansvarsplacering af koordineringen af den samlede AMS-proces. Procesejerskabet bør placeres tæt på relevante opgaver inden for myndighedsområdet, herunder fx motivationsfremmelse og kontrol af pligter samt hos medarbejdere med indgående forretnings- og målkendskab for AMS-processen.

3.6.5 Uklart systemejerskab for AMS-komplekset

Den anden observation, der er relateret til organisering og governance samt kategoriseret som prioritet 2, omhandler ejerskabet omkring den systemtekniske løsning, dvs. AMS. Også denne observation skal ses i lyset af en kompleks og uklar fordeling af opgaver og ansvarsområder på tværs af interne som eksterne aktører i relation til AMS. Det er uklart, hvilke(n) organisation(er) der har det samlede centrale systemansvar for AMS på tværs af alle komponenter, der indgår i det samlede systemkompleks. Der er ikke i dag udpeget en egentlig systemejer for AMS. I løbet af undersøgelsen er det observeret, at UIM varetager opgaver inden for drift og systemforvaltning (særligt datasikkerhed og systemovervågning) af databaserne og netværk med SIT som leverandør på visse driftsopgaver. Det er også observeret, at distributøren af systemkomponenter fra producenten Salto samtidig er central vidensperson i forhold til produkternes forretningslogik, fx i forhold til beskedmodtagelse.

Bilag 7.4 udgør et overblik over systemkomponenter i relation til AMS, herunder hvilke aktører der for hver komponent er hhv. kunde, medarbejder samt leverandøransvarlig for fx installation, vedligehold, drift og monitorering mv.

7. Uklart systemejerskab for AMS-komplekset	
Prioritet	2
Udrejsecenter	KHG og SJM
Beskrivelse af problemstilling	Den manglende placering af systemejerskabet har været tydelig på forskellige områder i løbet af undersøgelsen, eksempelvis i form af en ufuldstændig, samlet systemdokumentation, og viden om systemet har været fragmenteret og fordelt på mange forskellige personer fra forskellige organisationer (særligt US, HJEMST, leverandøren Sanistål, Koncern IT, SIT, udrejsecentrene samt de lokale leverandører Actas og Holstebro Låseteknik). Der er endvidere også observeret manglende formalisering og usystematisk kontrakt- og leverandørstyring, herunder særligt anvendelse af SLA'er, opfølgning på opetider mv.
Risiko-beskrivelse	Hvis der ikke vedligeholdes en tilstrækkelig dokumentation og viden om, hvad der sker i hele systemkomplekset, så risikeres det, at der over tid er uklarhed om, hvorvidt data fortsat er tilstrækkelig sikret mod forvanskning, i takt med at systemet opdateres og tilrettes, og at der sker udskiftning af medarbejdere på vigtige poster. Der er således en indirekte risiko for dataforvanskning og databab forbundet med et manglende systemejerskab.
Kendte eksisterende kontroller	Der er ikke identificeret relevante kontroller i undersøgelsen.
Anbefalinger til yderligere tiltag	
Yderligere anbefalinger	Det anbefales, at det samlede systemejerskab for AMS forankres ét sted, herunder særligt under hensyntagen til at forankre den tekniske viden om systemet ét sted i Udlændinge- og Integrationsministeriets koncern. Systemejerskabet bør således inkludere følgende elementer (nuværende primære vidensorganisation i parentes): Viden om systemarkitekturen på udrejsecentrene (hvor leverandørerne Sanistål, Actas og Holstebro Låseteknik ligger inde med mest viden). Viden om systemarkitekturen på den såkaldte Salto-server, hvor systemet driftes (hvor UIM-KIT og SIT ligger inde med mest viden). Viden om efterfølgende filtrering, sammenlægning og forretningslogik til datakontroller til brug i QlikView på den såkaldte BI-server (hvor HJEMSTs dataanalytikere ligger inde med mest viden). Hvis det ikke er muligt at ansvarsplacere systemejerskabet hos én organisatorisk enhed, så kan systemejerskabet evt. opdeles i et teknisk og forretningsmæssigt ejerskab. I den konstellation vil det tekniske systemejerskab stå for basal drift og stabilitet af AMS, udvikling af løsninger samt sammenhæng til øvrige systemer; det forretningsmæssige systemejerskab er fx ansvarlig for at indhente og prioritere ændringsønsker på tværs af AMS.

4. Bilag

4.1 Begrebsdefinitioner

For at skabe en fælles begrebsmæssig forståelse og grundlag for undersøgelsen og dens konklusion defineres en række nøglebegreber i den følgende tabel.

Overblik over centrale begreber og uddybende beskrivelser i AMS

Begreb	Beskrivelse
Adgangskontrol- og Meldepligtsystemet (AMS)	Det elektroniske adgangskontrolsystem, som anvendes i Udrejsecenter KHG og SJM til ind- og udgang af centrene samt aflæggelse af meldepligt. På KHG anvendes systemet også som låsesystem til værelsesdøre og andre døre til fx fællesarealer mv.
Opholdspligt	Opholdspligten betyder, at en udlænding skal bo på udrejsecentret og i udgangspunktet overnatte på centret hver nat.
Meldepligt	Meldepligten betyder, at en udlænding skal møde hos HJEMST på nærmere angivne tidspunkter mhp. løbende at sikre, at myndighederne har kendskab til udlændingens opholdssted.
Underretningspligt	Underretningspligten betyder, at en udlænding skal underrette sit udrejsecenter, hvis udlændingen opholder sig uden for udrejsecentret i tidsrummet mellem kl. 23.00 og kl. 6.00.
Stregkodescanner (u. biometri)	Medarbejderbetjent enhed til scanning af stregkodekort til registrering af ind- og udgang på Udrejsecenter SJM og KHG. Ind- og udgangsscannere er monteret ved siden af hinanden på væggen i stuen hos Kriminalforsorgens medarbejdere (portvagten). Såfremt der er foretaget en korrekt registrering, og der er forbindelse til serveren, vil enheden skifte fra rødt til grønt lys.
Biometrisk håndscanner	Medarbejderbetjent enhed til scanning af biometriske kort til registrering af ind- og udgang på Udrejsecenter SJM. Placeret på bord (men delvist mobil).
Karrusel (m. biometri)	Beboer-selvbetjent enhed til scanning af biometriske kort til registrering af ind- og udgang af Udrejsecenter SJM og KHG. Sluseopbygget med først én scanningsenhed, karrusel, sluse, anden scanningsenhed og dør til endelig ind-/udgang. Der er på hvert udrejsecenter én karrusel til indgang og én karrusel til udgang.
Meldepligtscanner med biometri	Beboer-selvbetjent enhed til scanning af biometriske kort til registrering af meldepligt på Udrejsecenter SJM og Udrejsecenter KHG.
Meldepligt-stregkodescanner (u. biometri)	Medarbejderrbetjent enhed til scanning af stregkodekort til registrering af meldepligt på Udrejsecenter SJM og KHG. Scanneren er fastmonteret på væggen i HJEMST's meldepligtlokaler.
Biometrisk kort	Kort med fingeraftryksbiometri til anvendelse for beboere til at registrere deres ind- og udgange og til at foretage deres meldepligtregistrering på Udrejsecenter SJM og KHG. KHG har leverandøren Zwipe, og SJM har leverandørerne Fuse og Zwipe (udfases).
Stregkodekort (u. biometri)	Stregkodekort med foto, stregkode, navn og id til anvendelse for beboere til at registrere ind- og udgange og til at foretage meldepligtregistrering på Udrejsecenter SJM og KHG. Kort gives til alle beboere og er eneste kort, såfremt det ikke er muligt at oprette et biometrisk kort, fx fordi en beboers fingeraftryk ikke kan indlæses. Såfremt der også haves et biometrisk kort, sammenklæbes disse to kort (KHG) eller kobles sammen kortholder (SJM), hvormed dette i praksis bæres af beboeren som ét kort.
Brik (u. biometri)	Offline nøglebrik til ind- og udgang af værelser og fællesarealer på Udrejsecenter SJM og Udrejsecenter KHG. På SJM bliver registreringer fra disse enheder registreret separat fra øvrige registreringer. På KHG bliver registreringer fra disse enheder registreret sammen med øvrige hændelsesregistreringer via AMS.
Offline dørlåse	Låseenheder ved døre, som opsættes ved fx beboerdøre og døre til fællesarealer. På SJM er offline dørlåse ikke integrerede i AMS. På KHG er offline dørlåse integrerede i AMS.
PC	Medarbejderbetjent stand-alone-pc på begge udrejsecentre med adgang til Salto-system via WebApp (browser). Anvendes bl.a. til oprettelse af beboere. Denne lagrer ikke data lokalt, men formidler data direkte til Salto-system via serverforbindelse.
Førstegangsscanner	Enhed placeret ved PC i døgnbemandet portvagt. Anvendes ved oprettelse af biometrisk kort til kontrol af, at kort fungerer og demonstrere dette over for beboer.
Brugeroprettelsesenhed/ Bordkoder	Enhed placeret ved PC i døgnbemandet portvagt. Anvendes ved oprettelse af biometrisk kort til pålægning/opdatering af Salto-rettigheder, herunder brugerprofiler, adgange mv.
Serviceport	Større ind- og udgang for varetransport, biler mv.
Personsluse ved portvagt	Den fysiske ind- og udgang for beboere og medarbejdere. Slusen har to mekaniske døre og er placeret ved den døgnbemandede portvagt.
Døgnbemandet portvagt	Kontor døgnbemandet med Kriminalforsorgens personale. Fysisk placeret nær beboersluse til ind- og udgang.

4.2 Liste over afholdte møder, interviews og workshops

Interview / Workshops	Dato	Navne	Repræsentant for
Opstartsworkshop	4/2	Janus Andersen	HJEMST
		Andreas Alsøe	UIM
		Kenneth Rasmussen	UIM
		Anne Dorte Weismann	UIM
		Aleksander Bjerrum	PwC
		Nikolaj Thiesen	PwC
		Frederik Skjærning	PwC
UIM's koncern IT	11/2	Nikolaj Thiesen	PwC
		Frederik Skjærning	PwC
		Kjeld Neumann	UIM - Koncern IT
		Martin Hjort Jørgensen	UIM - Koncern IT
		Andreas Alsøe	UIM - Koncern IT
		Søren Michael Pedersen	UIM - Koncern IT
		Andreas Prisholm	UIM - Koncern IT
		Thomas Krohn	UIM - Koncern IT
Leverandør-interview, Actas (Sjælsmark)	2/3	Nikolaj Thiesen	PwC
		Frederik Skjærning	PwC
		Janus Andersen	HJEMST
		Michael Petersen	Actas
Leverandør-	4/3	Aleksander Bjerrum	PwC

interview, Holstebro Låseteknik (Kærshovedgård)		Frederik Skjærning	PwC
		Janus Andersen	HJEMST
		Henrik Mølgaard	Holstebro Låseteknik
		Bent	Holstebro Låseteknik
Leverandør-interview, Sanistål	5/3	Nikolaj Thiesen	PwC
		Aleksander Bjerrum	PwC
		Janus Andersen	HJEMST
		Kasper Løth Kure-Olsen	Sanistål
Interview med SIT	22/2	Nikolaj Thiesen	PwC
		Aleksander Bjerrum	PwC
		Birgitte Basse Gade	SIT
		Jesper Jensen	SIT
		Søren Rueskov Walther	SIT
		Kenneth Leif Rasmussen	UIM
QlikView	5/3	Nikolaj Thiesen	PwC
		Oliver Brandt	PwC
		Janus Andersen	HJEMST
		Kjeld Wallentin	UIM
		Camilla Sparre Rügge	US
		Elsebet Seest	HJEMST
		Anders Mostrup Gudmansen	Danmarks Domstole

		Jeanett Jezewski	HJEMST
Hjemrejsestyrelsen	25/2	Nikolaj Thiesen	PwC
		Frederik Skjerning	PwC
		Jeanett Jezewski	HJEMST
		Janus Andersen	HJEMST
Udlændingestyrelsen (ift. System- og serviceaftale)	24/2	Aleksander Bjerrum	PwC
		Frederik Skjerning	PwC
		Ditte Kruse Dankert	US
		Thomas C. H. Mortensen	US
		Mikael Bo Pedersen	US
		Jasmina Jankovic	US
Udrejsecenter, Sjælsmark	5/3	Nikolaj Thiesen	PwC
		Frederik Skjerning	PwC
		Henriette Nguyen	Udrejsecenter Sjælsmark
		Janus Andersen	HJEMST
Udrejsecenter, Kærshovedgård	1/3	Mathias Holdt	PwC
		Frederik Skjerning	PwC
		Peter Wiinberg Karbo	Udrejsecenter Kærshovedgård
		Erik Eriksen	Udrejsecenter Kærshovedgård
		Susanne Lübcker	Udrejsecenter Kærshovedgård
		Janus Andersen	HJEMST
Besigtigelse:	10/3	Frederik Skjerning	PwC

Sjælsmark		Nikolaj Thiesen	PwC
		Janus Andersen	HJEMST
		Henriette Nguyen	Udrejsecenter Sjælsmark
Besigtigelse: Kærshovedgård	4/3	Mathias Holdt	PwC
		Niels Johan Geil	Udrejsecenter Kærshovedgård
		Janus Andersen	HJEMST
		Peter Wiinberg Karbo	Udrejsecenter Kærshovedgård
Styregruppe	Mødehyppighed: hver 2. uge (ulige uger)	Haythan Almumar	Udrejsecenter Kærshovedgård
		Jakob Lundsager	UIM
		Louise Vinther Torrendrup	HJEMST
		Grith Sandst Poulsen	US
Projektgruppe	Mødehyppighed: hver 2. uge (lige uger)	Esben Toft	PwC
		Aleksander Bjerrum	PwC
		Nikolaj Thiesen	PwC
		Frederik Skjerning	PwC
		Andreas Alsøe	UIM - Koncern IT
		Anne Dorte Weismann	UIM - Koncern IT
		Janus Andersen	HJEMST
		Dorte Lohmann Kjærdsgaard	HJEMST
		Ditte Kruse Dankert	US
		Jasmina Jankovic	US

4.3 Materialeliste

Materialeliste: Liste over tilsendt materiale

- Orientering af UUI 29.09.20
- Orientering til FT om suspendering af anmeldelse for overtrædelse af kontrolforpligtelser
- Orientering til UUI 02.12.20
- Orientering til UUI 14.12.20
- Bilag 1 Redegørelse om episode i perioden 9.11. marts 2020
- Bilag 4 - Anmeldelse til Datatilsynet-1
- Bilag 4 Faktaark om Saltosystemet
- Bilag 7 - Begrebsliste vedrørende Salto
- Følgrebrev_HJEMSTs udtalelse til Datatilsynet
- Opdateret faktaark (opdateret 6. november 2020)
- Spørgsmål til skønsmand-udkast_Bortredigeret
- Supplerende udtalelse til faktaark om Saltosystemet af 20. november 2020
- Udtalelse vedr. anmodning om syn og skøn_Bortredigeret
- Bilag 1 Faktaark om Saltosystemet-1
- Bilag 2 Revideret redegørelse om datanedbrud ved registrering af opholds- og meldepligt i perioderne 9.-10. juni og 2.-3. juli 2020
- Bilag 3 Hændelsesrapport Salto Server Låsesystem
- Bilag 5 - Incidents proces-1
- Bilag 6 - UrgencyImpact
- Redegørelse for hændelse i Salto-systemet

- Udtalelse til Datatilsynet
- Bilag 2 - Varedeklaration for informationssikkerhed
- Bilag 3 - Snitflader mellem kunden og SIT
- Bilag 4a - SIT's Standarddriftsplatform
- Driftsindberetning for Salto Server låsesystem Final (2019-06-01)
- US - Årsrapport tilsyn 2018
- US - Årsrapport tilsyn 2019_bilag
- US - Årsrapport tilsyn 2019
- US - Bilag 1. Tilsynskoncept maj 2017
- US - Bilag til årsrapport tilsyn 2018
- US - KRF kontrakt 18.12.2020 - klar til underskrift (003)
- Øvrigt: tilsendt materiale i relation til uddannelse, oplæring og vejledning af operatører i anvendelse af Salto-system
- Salto-netværk - overblik over systemkomponenter

4.4 Overblik over systemkomponenter

Navn på systemkomponent	Kunde	Medarbejder	Leverandør Installation	Leverandør Vedligehold	Leverandør Drift og monitor.	Distributør af software / hardware	Producent af software / hardware
PC	US	KRIMFO	Holstebro Låseteknik (KHG) + ACTAS (SJM)		KRIMFO / HJEMST	Holstebro Låseteknik (KHG) + ACTAS (SJM)	
IO bridge enhed - Kærshovedgård	US	KRIMFO	Holstebro Låseteknik (KHG)	Så ringer centret til Holstebro Låseteknik	KRIMFO / HJEMST	Sanistål	Salto
IO bridge enhed - Sjælsmark	US	KRIMFO	ACTAS	Så ringer centret til Actas	KRIMFO / HJEMST	Sanistål	Salto
PPD (Portable Programming Devices) - Kærshovedgård	US	KRIMFO	Holstebro Låseteknik (KHG)	Så ringer centret til Holstebro Låseteknik	KRIMFO / HJEMST	Sanistål	Salto
Brugeroprettelsesenhed / Bordkoder (KHG)	US	KRIMFO	Holstebro Låseteknik		KRIMFO / HJEMST	Sanistål	Salto
Brugeroprettelsesenhed / Bordkoder (SJM)	US	KRIMFO	ACTAS		KRIMFO / HJEMST	Sanistål	Salto
Biometrisk kort (m. biometri)	US	KRIMFO	Sanistål		KRIMFO / HJEMST	Sanistål	Tredjepart - Zwipe (nuværende) - Fuse (fremtidig)
Brik (u. biometri) (KHG)	US	KRIMFO	Holstebro Låseteknik		KRIMFO / HJEMST	Holstebro Låseteknik	Ukendt producent
Stregkodekort (u. biometri) - Kærshovedgård	US	KRIMFO	Holstebro Låseteknik		KRIMFO / HJEMST	Holstebro Låseteknik	ID Companies
Stregkodekort (u. biometri) - Sjælsmark	US	KRIMFO	ACTAS		KRIMFO / HJEMST	ACTAS	ID Companies
Online registreringsenheder (KHG)	US	KRIMFO	Holstebro Låseteknik	Holstebro Låseteknik	KRIMFO / HJEMST	Sanistål	Salto
Online registreringsenheder (SJM)	US	KRIMFO	ACTAS	ACTAS	KRIMFO / HJEMST	Sanistål	Salto
Stregkodescanner (KHG)	US	KRIMFO	Holstebro Låseteknik	Holstebro Låseteknik	KRIMFO / HJEMST	Sanistål	IBC (svensk grossist)
Stregkodescanner (SJM)	US	KRIMFO	ACTAS	ACTAS	KRIMFO / HJEMST	Sanistål	IBC (svensk grossist)
Biometrisk håndscanner (SJM)							
Offline dørlåse (KHG)	US	KRIMFO	Holstebro Låseteknik	Holstebro Låseteknik	KRIMFO / HJEMST	Sanistål	Salto
VPN Servicenet	UIM-KIT		SIT	SIT	SIT	SIT	
MPLS-netværk	UIM-KIT		SIT	SIT	SIT	SIT	
Hændelseslog (Alle hændelser)							
Salto ProAccess Space applikation	US	UIM-KIT	Holstebro Låseteknik	UIM-KIT	UIM-KIT	Sanistål (kontrakt med Holstebro Låseteknik)	Salto

Salto database (ufiltreret)			UIM-KIT	UIM-KIT	UIM-KIT	SIT	Microsoft
Daglige jobs			UIM-KIT	UIM-KIT	UIM-KIT		
CARL2							
IBS							
Powershell scheduled tasks			UIM-KIT	UIM-KIT	UIM-KIT		UIM-KIT, udviklet tasks
Salto BI database (filtreret)			UIM-KIT	UIM-KIT	UIM-KIT	SIT	Microsoft
HJEMST							
Applikationsserver	UIM-KIT		SIT	SIT	SIT	SIT	Microsoft
Job-server	UIM-KIT		SIT	SIT	SIT	SIT	Microsoft
BI-server	UIM-KIT		SIT	SIT	SIT	SIT	Microsoft
Stored procedures							
QVD-fil							
QVW-fil							
QlikView							
Saltolog Rådata							
Saltolog anmeldelsesliste							
EsterH							
Public 360							

4.5 Observationsskema (simplificeret)

#	Titel	Udrejsec enter	Priorit et (1-3)*	Beskrivelse af problemstillingen	Risiko- beskrivelse	#	Anbefaling til yderligere tiltag	Delpro ces	PAVA (delområ de)	Ressour cer (1-3)**	Effekt (1-3)**
1	Dataforvanskning i forbindelse med anvendelse af offline-enheder på Kærshovedgård	KHG	1	Der er en række årsager til, at de offline enheder på Kærshovedgård kan afstedkomme dataforvanskning i AMS, herunder særligt tidsforskydning og beboeradfærd: <i>Tidsforskydning:</i> Systemdistributøren og installationsleverandøren har oplyst, at klokkeslættet i tidsstyringsenhederne i offline-registreringsenhederne (fx låse til værelsesdøre) erfaringsmæssigt tidsforskydes mellem gensynkroniseringer, og at offline-enhederne skal gensynkroniseres regelmæssigt, hvis data (tidsstemplerne) i enhederne skal være valide ift. beboernes reelle færden. Leverandørerne kender ikke den præcise tidsforskydning, men formoder, at denne udgør omkring +/- 2 minutter pr. måned, (hvis der ikke gensynkroniseres løbende). Dette kan skyldes manglende lokalt vedligehold. Ifølge leverandør bør offline enheder opdateres ugentligt, ligesom der bør være opmærksomhed omkring at der ved batteriskift skal opdateres for at sikre imod at enheden tilbagesættes til fabriksindstilling (inkl. tidsstempel). <i>Beboeradfærd:</i> PwC har på baggrund af interviews og besigtigelse noteret, at beboerne på flere forskellige måder forsøger at omgå registrering af ind- og udgange af døre på værelser, fællesarealer og lignende, fx ved at placere sko i dørene, holde døre for øvrige beboere mv. <i>Manglende registreringer:</i> registreringer fra besigtigelser er foretaget korrekt, men fremgår ikke efterfølgende i hændelsesloggen.	Ovenstående problemer udgør tilsammen en væsentlig risiko for forvanskning af data i de offline enheder. Hermed udgør inddragelse af data fra de offline enheder i AMS som helhed en væsentlig risiko for at nedbringe validiteten i det samlede datagrundlag og dataflow.	1.1	Det anbefales, at data fra offline enheder afkobles fra AMS, da tidsforskydning i de offline enheder og beboeradfærden tilsammen udgør en væsentlig risiko for forvanskning af data i de offline enheder. Hermed udgør inddragelse af data fra de offline enheder i AMS som helhed en væsentlig risiko for at nedbringe validiteten i det samlede datagrundlag og dataflow.	5	Arkitektur	2	3
2	Uklar proces for tilmelding og tilkobling af nye registreringsenheder	KHG og SJM	1	Det er i forbindelse med interview med Koncern IT i Udlændinge- og Integrationsministeriets Departement (UIM-KIT) observeret, at registreringerne af beboernes passager og meldepligt ikke automatisk indgår i data. Forudsætningen er, at en registreringsenhed skal inkluderes i dataflowet (ikke filtreres fra), så de daglige udtræk indeholder hændelser fra den pågældende registreringsenhed. Hvis registreringsenheden ikke er inkluderet i det videre dataflow, så kommer disse data ikke med, og en beboers færden vil ikke fremgå af data SALTO-loggen. Det betyder først og fremmest, at hvis der opsættes nye enheder på Udrejsecentrene, så er det essentielt at huske at orientere UIM-KIT, så det sikres, at disse enheders registreringer også kommer med i filtreringen.	Det har i undersøgelsen ikke været muligt at identificere en formaliseret proces for sikring af, at nye registreringsenheder (dvs. registreringsenheder ved sluser, ind- og udgangsstandere og meldestandere) inkluderes i dataflowet (særligt hændelsesjobs i Salt BI DB-databasen). Det er samtidig uklart, hvorvidt det er Hjemrejsestyrelsen (vilkårene på udrejsecentrene, Udlændingestyrelsen (kontrakt- og bevillingsejer), (Kriminalforsorgen) eller leverandørerne. Det er også uklart, om en advisering skal gå til UIM KIT eller Statens IT (ansvarlig for drift af servicenetværk og database). Der er således risiko for, at information om nye registreringsenheder ikke gives videre til UIM-KIT eller Statens IT, så udtræk af data fra AMS ikke længere afspejler beboerens færden for de pågældende registreringsenheder.	2.1	Det anbefales, at der etableres og implementeres en formaliseret proces for tilmelding af nye registreringsenheder til de ansvarlige for drift og opsætning af udtræk (filtrering/jobs) i forhold til overførsel af hændelser fra registreringsenheder til SALTO BI-databasen.	8	Governance	1	2
3	Uhensigtsmæssig placering af strekkodescanner (u. biometri)	KHG	2	Ud- og indgangsscannerne i portvagten på Kærshovedgård (strekkodescanner uden biometri) er placeret tæt på hinanden, hvilket indebærer en risiko for, at en medarbejder kommer til at foretage en registrering af en passage i den forkerte retning, fx registrering af en indgang, som skulle have været en udgang.	Hvis medarbejder ved en fejl laver en forkert registrering (fx en udgang fremfor en indgang), vil nedbringe validiteten af datagrundlaget i hændelsesloggen i forhold til beboerens færden.	3.1	Det anbefales, at strekkodescannerne ved ind- og udgangsregistrering i portvagten placeres med større afstand i mellem for at reducere risikoen for, at der sker en forkert registrering. Herudover anbefales det, at der aktivt fokuseres på at reducere anvendelsen af strekkodekort på KHG ved at introducere håndscannere i portvagten til biometriske kort på KHG ligesom på SJM, samt ved at overgå til FUSE-kort på KHG ligesom på SJM, da erfaringerne indtil videre er, at disse er mere stabile i drift.	3 og 6	Arkitektur	1	3

4	Manglende organisatorisk forankring af proces for håndtering af incidents	KHG og SJM	2	Der er dokumenteret en hændelse (incident) den 10. Juni 2020, hvor en medarbejder ved en fejl fjernede og slettede data fra Salto Serveren. I den forbindelse blev UIM ved en fejl ikke orienteret om hændelsen samt udbedring af fejlen. Denne enkeltstående observation er gennem interviews med UIM KIT, Hjemrejsestyrelsen samt udrejsecentrene umiddelbart udtryk for en generel problematik omkring processen for håndtering af incidents.	Der er risiko for, at uklarhed omkring rolle-/ansvarsfordeling i processen for håndtering af incidents kan medføre, at der ikke reageres rettidigt ved systemnedbrud samt at der ikke iværksættes procesmæssige "workarounds" for at sikre, at AMS-processen kan fortsætte med en alternativ proces, mens eventuelle systemnedbrud pågår. Samtidig kan det have som konsekvens, at der bruges fejlbehæftede data i retsmæssig sammenhæng, hvis HJEMST og/eller UIM ikke er bevidst om, at der har været problemer med systemet i den periode, hvor en hændelse/incident har fundet sted.	4.1	Der er beskrevet en proces for håndtering af incidents, som redegør klart for ansvarsfordelingen mellem 1st line incidenthåndtering (dispatch), 2nd line incidenthåndtering (drift og support), 3rd line incidenthåndtering (systemforvaltning), Statens IT samt andre tredjeparter og systemleverandører. Samtidig fremgår det af denne to-be incidentproces, at der skal vedligeholdes en "KEDB" (Known Error Database) med henblik på at sikre, at kendte fejl registreres, beskrives og håndteres. Det anbefales, at den udarbejdede proces for håndtering af incidents implementeres og forankres blandt alle interessenter i AMS-processen, således at der skabes større klarhed omkring, hvordan og hvem der skal tages kontakt ifm. nye incidents/hændelser samt supportspørgsmål.	8	Governance	2	2
5	Lav kritikalitetsscore	KHG og SJM	2	I kundaftalen mellem UIM og SIT er ansvarsfordelingen mellem organisationerne beskrevet såvel som procedurer for prioritering af incidents relateret til kundaftalen, (særligt infrastruktur, herunder servere, netværk på udrejsecentrene mv.). Det fremgår af kundaftalen (bilag 6, urgency impact), at kritikaliteten af AMS er vurderet til niveau "D", som er det laveste niveau i SIT's kundaftaler. Niveau D definerer nedbrud i driften (AMS) med følgende konsekvenser: Mindre ulemper og begrænsede tab eller omkostninger. Denne kategorisering er påfaldende lav henset til, hvor kritisk data fra Salto-systemet er til brug i retsmæssig sammenhæng.	Kritikalitetsvurderingen af AMS som D kan medføre, at medarbejdere i SIT nedprioriterer incidents, relateret til AMS, og at der dermed ikke følges op i tide på disse incidents med risiko for databtab.	5.1	Det anbefales, at AMS' kritikalitet revurderes og justeres fra den nuværende klassifikation "D" til enten niveau "A" eller "B", idet det kun er i disse kategorier, at systemnedbrud vurderes at kunne føre til væsentlige brud på målopnåelse for myndigheden, hvilket vurderes at være tilfældet for AMS. Formålet med opjusteringen af systemets kritikalitet er at sikre en hurtigere genopretningstid til normal drift, når der indtræffer incidents, givet at niveau A og B systemer prioriteres højere i incidenthåndteringen.	8	Governance	[den øgede udgift er ikke afdækket i undersøgelsen]	3
6	Uklart procesejerskab for AMS-processen	KHG og SJM	2	Det er uklart, hvilken organisation eller aktør, som har det samlede procesejerskab for AMS på tværs af dataflowet. Eksempelvis har Udlændingestyrelsen fortsat det kontraktuelle og bevillingsmæssige ansvar samt ansvar for tilsyn i medfør af operatørkontrakten med Kriminalforsorgen. Heroverfor er Hjemrejsestyrelsen ansvarlig for udmøntning af vilkårene på centrene samt håndtering af beboernes pligter i det daglige. Dette forhold skaber uklarhed, fx i forbindelse med leverandørkontakt som beskrevet ved incidents ovenfor.	Der er risiko for, at den samlede AMS proces ikke lever op til de forretningsmæssige og forvaltningsmæssige mål om at opretholde kontroltrykket i forhold til beboernes pligter. Det kan kan have en effekt på tilstedeværelse samt kvalitet og validitet af data, hvorved data ikke afspejler beboernes reelle færden.	6.1	Det anbefales, at der implementeres et egentligt procesejerskab i overensstemmelse med gældende best practice, særligt med henblik på entydig ansvarsplacering af koordineringen af den samlede AMS-proces. Procesejerskabet bør placeres tæt på relevante opgaver inden for myndighedsområdet, herunder fx motivationsfremmelse og kontrol af pligter samt hos medarbejdere med indgående forretnings- og målkendskab for AMS-processen.	8	Governance	2	2
7	Uklart systemejerskab for AMS-komplekset	KHG og SJM	2	Den manglende placering af systemejerskabet har været tydelig på forskellige områder i løbet af undersøgelsen, eksempelvis i form af en ufuldstændig, samlet systemdokumentation, samt at viden om systemet har været fragmenteret og fordelt på mange forskellige personer fra forskellige organisationer (særligt Udlændingestyrelsen, Hjemrejsestyrelsen, leverandøren Sanistål, Koncern IT, Statens IT, Udrejsecentrene samt de lokale leverandører Actas og Holstebro låseteknik). Der er videre også observeret manglende formalisering og usystematisk kontrakt- og leverandørstyring, herunder særligt anvendelse af SLA'er, opfølgning på oppejder osv.	Hvis der ikke vedligeholdes en tilstrækkelig dokumentation og viden om, hvad der sker i hele systemkomplekset, så risikeres det, at der over tid er uklarhed omkring, hvorvidt data fortsat er tilstrækkelig sikret mod forvanskning i takt med, at systemet opdateres, tilrettes og at der sker udskiftning af medarbejdere på vigtige poster. Der er således en indirekte risiko for dataforvanskning og databtab forbundet med et manglende systemejerskab.	7.1	Det anbefales, at det samlede systemejerskab for AMS forankres ét sted, herunder særligt under hensyntagen til at forankre den tekniske viden om systemet ét sted i Udlændinge- og Integrationsministeriets koncern. Systemejerskabet bør således inkludere følgende elementer (nuværende primære vidensorganisation i parentes): Viden om systemarkitekturen på udrejsecentrene (hvor leverandørerne Sanistål, Actas og Holstebro låseteknik ligger inde med mest viden). Viden om systemarkitekturen på den såkaldte "Salto-server", hvor systemet driftes (hvor UIM-KIT og SIT ligger inde med mest viden). Viden om efterfølgende filtrering, sammenlægning og forretningslogik til datakontroller til brug i QlikView på den såkaldte "BI-server" (hvor Hjemrejsestyrelsens dataanalytikere ligger inde med mest viden). Hvis det ikke er muligt at ansvarsplacere systemejerskabet hos én organisatorisk enhed, så kan systemejerskabet evt. opdeles i et teknisk og forretningsmæssigt ejerskab. I den konstellation vil det tekniske systemejerskab stå for basal drift og stabilitet af AMS, udvikling af løsninger samt sammenhæng til øvrige systemer; det forretningsmæssige systemejerskab er fx ansvarlig for at indhente og prioritere ændringsønsker på tværs af AMS.	8	Governance	2	2

8	Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere	KHG og SJM	2	Det er ved besigtigelse (på Udrejsecenter Kærshovedgård) observeret, at det testkort, der blev oprettet ifm. besigtigelsen ikke havde fået slået anti-passback funktion til, hvilket resulterede i, at funktionen ikke slog i gennem på registreringsenheder til ind- og udgang (herunder karusseller). Den manglende antipassback-kontrol skal normalt forhindre fejlkoblinger, dvs. gentagne ind- eller udgangsregistreringer. Hvis beboere oprettes manuelt ved registrering, kan det ske, at funktionen ved en menneskelig fejl ikke slås til.	Der er risiko for gentagne fejlkoblinger, dvs. ind- og udgangsregistreringer, hvormed data ikke afspejler beboerens reelle adfærd.	8.1	Det anbefales, at det afklares med leverandøren, om det er muligt at foretage en systemændring således, at manuelt oprettede brugere automatisk har aktiveret anti-passback.	2	Adfærd	2	3
9	Anti-passback ikke implementeret for streghodekort	KHG og SJM	2	Leverandøren Sanistål har oplyst, at anti-passback kun er aktiveret ved brug af biometriske kort. En beboer, som har bevæget sig ind på centret og efterfølgende er gået ud af centret uden at registrere denne udgang (fx ved at hoppe over hegnet) kan således frit benytte streghode-scanneren i portvagt til at foretage endnu en indgangsregistrering uden at blive bremset af anti-passback funktionen. PwC's gennemførte dataanalyser underbygger dette, da langt størstedelen af fejlkombinationer af ind- og udgangsregistreringer sker, hvor der anvendes et streghodekort (jf. kontrol 9 i dataanalysen).	Der er risiko for gentagne fejlkoblinger, dvs. gentagne ind- og udgangsregistreringer, hvormed data potentielt ikke afspejler beboerens reelle passage.	9.1	Det anbefales, at der findes en løsning for, hvordan anti-passback håndhæves i praksis, hvis beboeren ikke anvender sit biometriske kort. En tilgang er at undersøge med leverandører, om anti-passback kan implementeres for streghodekort uden at skulle foretage store og dyre ændringer i applikationskode i standardsystemet Salto ProAccess Space. Alternativt kan det undersøges med leverandører, om man i stedet for at anvende streghodekort som backup for biometrisk registrering kan anvende RFID-kort med billede, da disse kort også ville kunne opbevare data på selve kortet ligesom de biometriske kort. Dette kan potentielt sikre en simplere systemisk integration af passback-funktionaliteter på ikke-biometriske kort. Herudover anbefales det, at der aktivt fokuseres på at reducere anvendelsen af streghodekort på KHG ved at introducere håndscannere i portvagt til biometriske kort på KHG ligesom på SJM, samt ved at overgå til FUSE-kort på KHG ligesom på SJM, da erfaringerne indtil videre er, at disse er mere stabile i drift.	3 og 6	Validering/ Kontrol	2	3
10	Mangelfulde vejledninger, oplæring og opfølgning til medarbejdere på udrejsecentre	KHG og SJM	2	Det er uklart, hvilken organisation eller aktør, som har det samlede procesejerskab for AMS på tværs af dataflowet. Eksempelvis har Udlændingestyrelsen fortsat det kontraktuelle og bevillingsmæssige ansvar samt ansvar for tilsyn i medfør af operatørkontrakten med Kriminalforsorgen. Heroverfor er HJEMST ansvarlig for kontrol med overholdelsen af de af HJEMST pålagte pligter på centrene samt håndtering af beboernes pligter i det daglige. Dette forhold skaber uklarhed, fx i forbindelse med leverandørkontakt som beskrevet ved incidents ovenfor.	Der er risiko for at manglende træning og forståelse for AMS kan medføre menneskelige fejl og u hensigtsmæssigheder i anvendelse af systemet, herunder fx stamdata der ligger til grund for den efterfølgende datagenererende proces	10.1	Det anbefales, at implementeres et on-boarding koncept i procedurer og processer samt proces for løbende opfølgning på viden om samme. Det anbefales videre, at der formaliseres procedure- og procesbeskrivelser, som dokumenterer bedste praksis for opretholdelse af kontroltrykket samt relevante opfølgningsmekanismer for løbende ajourføring.	2-6	Adfærd	2	2
11	Døre ved persons-luse står periodevist åbne	SJM	2	Det er observeret, at dørene ved persons-lusen (ved portvagt) til ind- og udgang på SJM til tider står åbne, da den mekaniske åbne- og lukkemekanisme er langsom.	Der er risiko for at beboere uregistreret kan bevæge sig ind og ud af centret, hvorved data i AMS ikke vil afspejle beboerens reelle færden.	11.1	Det anbefales enten at opgradere de nuværende mekaniske døråbnere til nogle med en hurtigere åbne- og lukkemekanisme eller at udskifte de mekaniske døre med analoge døre uden åbne- og lukkemekanismer, men med medarbejderbetjent elektronisk lås.	3 og 6	Adfærd	2	1
12	Manglende opfølgning og tilsyn af kontrolparadigme på udrejsecentre	KHG og SJM	2	Det er i relation til kontrolanalysen observeret, at der fra Udlændingestyrelsens side udføres tilsyn på udrejsecentre i henhold til operatørkontrakten med Kriminalforsorgen i et kunde-/leverandørforhold. Disse tilsyn foretages primært i relation til bygninger, faglige tilsyn af udbetaling af ydelser (i forbindelse med IBS) mv. med henblik på overholdelse af operatørkontrakten. Der udføres ikke kvalitetssikring af Kriminalforsorgens drift af udrejsecentre eller kontrol med adgangs- samt ind- og udgangsregistreringer i relation til dataforvanskning.	Det er i relation til kontrolanalysen observeret, at der fra Udlændingestyrelsens side udføres tilsyn på udrejsecentre i henhold til operatørkontrakten med Kriminalforsorgen i et kunde-/leverandørforhold. Disse tilsyn foretages primært i relation til bygninger, faglige tilsyn af udbetaling af ydelser (i forbindelse med IBS) mv. med henblik på overholdelse af operatørkontrakten. Der udføres ikke kvalitetssikring af Kriminalforsorgens drift af udrejsecentre eller kontrol med adgangs- samt ind- og udgangsregistreringer i relation til dataforvanskning.	12.1	Det anbefales, at der etableres et koncept for løbende Intern KvalitetsSikring (IKS) i forhold til at følge op på, at risici for dataforvanskning og datatab mitigeres på tværs af AMS. IKS'en bør tage udgangspunkt i udarbejdelse af standardiserede processer og procedurer og fx inkludere kvartalsvise opfølgninger/stikprøvekontroller.	2-6	Validering/ Kontrol	2	2

13	Mangelfuld automatisk advisering ved driftsproblemer	KHG og SJM	2	Hjemrejsestyrelsen og Kriminalforsorgens medarbejdere får ikke automatisk besked om driftsforstyrrelser på Saltosystemet fra Statens IT (SIT) eller UIM Koncern-it (KIT)	Manglende advisering om systemnedbrud kan have forskellige konsekvenser: - Hvis Kriminalforsorgens medarbejdere ikke via et dashboard kan få indsigt i eller automatisk adviseres, når der opstår driftsproblemer, så skaber det unødige udfordringer på Udrejsecentrene. - Hvis Hjemrejsestyrelsens medarbejdere ikke er bevidst om en relevant driftsforstyrrelse, når en potentiel anmeldelse behandles, så kan det i yderste konsekvens føre til, at der fejlagtigt laves en anmeldelse for en pligtovertrædelse	13.1	Det anbefales, at der etableres et løbende driftsoverblik (fx dashboard) over AMS samt etableres en proces for fremsendelse af automatisk advisering til både Kriminalforsorgens medarbejdere på udrejsecentrene (til email adresser på begge centre) samt til Hjemrejsestyrelsens e-mailadresse til formålet (anmeldelser@hjemst.dk.).	8	Arkitektur	1	2
14	Antipassback ikke aktiveret for biometriske kort	KHG	2	Det er under både besigtigelse og tillægsbesigtigelse på udrejsecenter Kærshovedgård dokumenteret, at anti-passback ikke er aktiveret for det biometriske kort ved anvendelse i ind-/udgangskarrusellerne.	Der er risiko for gentagne fejlkoblinger, dvs. gentagne ind- og udgangsregistreringer, hvormed data potentielt ikke afspejler beboerens reelle passager.	14.1	Det anbefales at anti-passback i samarbejde med systemleverandører, dvs. Holstebro Låseteknik, reimplementeres for biometriske kort.	3 og 6	Validering/ Kontrol	1	2
15	Fejlregistreringer ved bruger meldt som udeblevet	SJM	3	Hvis en beboer har været registreret som værende udenfor udrejsecentret i for lang tid, så registreres beboeren automatisk som udeblevet med statussen "forbyd bruger" i AMS. Herefter kan beboeren ikke længere foretage ind- og udregistrering med hverken stregkodekort eller biometrisk kort. Ved afvisning af en beboer med biometrisk kort registreres dette i hændelsesloggen med status "Åbning ikke tilladt: Nøgle ugyldig". Ved afvisning af en beboer med stregkodekort registreres dette ikke i loggen.	Der er ikke store risici forbundet med denne observation, da beboeren korrekt afvises, som det er tiltænkt. Dog kan der være en lille risiko for, at medarbejdere på centrene ikke kan gennemskue, hvorfor en beboer er blevet afvist, hvis dette ikke logges korrekt i hændelsesloggen, når der er tale om stregkodekort.	15.1	Det anbefales, at det undersøges nærmere med leverandører, om det uden de store omkostninger kan tilføjes til hændelsesloggen, at afvisninger af beboere med koden "forbyd bruger" også logges fra stregkodekort.	3 og 6	Validering/ Kontrol	2	1
16	Kort slettefrist for øvrige logoplysninger i driftsmiljøet	KHG og SJM	3	Nogle typer af logs (applikations-, system- og SQL-log) slettes efter relativt kort tid (fx ca. 9 mdr. for applikationsloggen), hvilket kan være en udfordring i forbindelse gennemgang af retslige sager, hvor historiske hændelser i logoplysningerne ellers kan bidrage til opklaringen af sager. I en hændelsesredegørelse fremgår det således, at Koncern IT / Statens IT ikke samlet set har kunne levere de efterspurgt logoplysninger til at kaste lys på nogle specifikke sager ("Redegørelse for hændelse i SALTO-systemet", side 4)	Hvis der opstår tvivlsspørgsmål i en sag, der ligger mere end 9 måneder tilbage, så vil der i de fleste tilfælde være de fornødne oplysninger til stede for at undersøge mulige fejl, givet at de vigtigste logoplysninger gemmes i længere end 9 måneder. Men visse typer af hændelser vil ikke længere fremgå efter 9 måneder. Fx vil det kun være SQL-loggen (som blot gemmes i 9 måneder), der har oplysninger om, hvis en medarbejder med administratoradgang ved en fejl har slettet en eller flere rækker direkte i databasen. I langt de fleste tilfælde vil det sandsynligvis ikke være nødvendigt at anvende disse øvrige logoplysninger.	16.1	Det anbefales, at der foretages en vurdering af, hvor langt tilbage i tiden, man i Hjemrejsestyrelsen ønsker at kunne foretage anmeldelser af pligtovertrædelser, og at levetiden for de forskellige typer af logs herefter justeres efter dette.	3, 4 og 6	Arkitektur	2	3
17	Forkert brug af datamodel (fx brug af statuskoder i beboers navnefelt)	KHG	3	Der er eksempler på, at Kriminalforsorgens medarbejdere bruger navnefeltet i datamodellen som et notefelt til at angive, at en beboer er flyttet fra centret. Fx er en beboers fornavn ændret til "23.08.2018 flyttet" og efternavnet ændret til "Slettet 23.08.2018". Dette vidner om, at brugerne mangler funktionalitet for at sikre, at det kan registreres hvornår en beboer er flyttet fra et Udrejsecenter samt hvornår en beboer er slettet. Der er også eksempler, hvor en beboers efternavn er blevet suppleret med information såsom "(BRIK) FRIHEDSBERØVET"	Der er risiko for, at der ikke kan føres sager tilbage i tid for beboere, som ikke længere opholder sig på Udrejsecentret, fordi det ikke er muligt at identificere beboeren længere, da navnet på beboeren ikke fremgår i databasen.	17.1	Det anbefales, at - det undersøges med leverandøren, om der kan tilføjes ekstra felter i datamodellen og mulighed for at redigere disse felter i brugergrænsefladen. Det bør i den sammenhæng afdækkes, hvad det specifikke brugerbehov er for yderligere felter. - det bliver pålagt, at alle nye beboere oprettes via stamdata fra CARL2 via IBS. - navnefelterne læses for redigering for almindelige brugere, således at kun privilegerede brugere kan redigere disse felter ved særlige undtagelser.	2	Adfærd	2	3
18	Uhensigtsmæssige roller og adgange i relation til ændring af stamdata	KHG	3	Det er observeret, at alle medarbejdere fra Kriminalforsorgen på KHG frit kan tilgå og rette i stamdata for beboere (både ved manuel oprettelse og oprettelse med udgangspunkt i stamdata fra CARL2).	Der er øget risiko for at beboerprofiler opsættes forkert (hændelsesregistrering eller antipassback aktiveres ikke), eller der på anden måde rettes fejlagtigt i stamdata (navn, beboerid osv.).	18.1	Det anbefales, at det på KHG begrænses, hvilke medarbejdere der kan tilgå og rette i stamdata.	2	Validering/ Kontrol	1	2
19	Mangelfuldt test-miljø	KHG og SJM	3	Der er et fravær af test-miljø, hvor det kan sikres, at ændringer i systemlandskabet implementeres og testes, inden de rulles ud i produktionsmiljøet.	Hvis der ikke er et test-miljø til at sikre, at nye systemopdateringer, patches til servere, ændringer til eksisterende integrationer, helt nye integrationer og	19.1	Det anbefales, at der designes en samlet teststrategi for AMS-systemkomplekset. Strategien skal designes nærmere men kunne fx indeholde:	8	Arkitektur	3	2

					andre ændringer i det samlede systemkompleks testes i gennem inden de rammer produktionsmiljøet, så er der en risiko for, at eventuelle uhensigtsmæssigheder, fejl og uventede hændelser indtræffer i selve produktionsmiljøet, hvor det vil være kritisk og evt. kunne føre til dataforvanskning.		- Et test-miljø - fx bestående af: -- En test-server identisk til Salto-serveren -- Salto testdatabase med fiktive registreringer og fiktive beboere -- Test-identitetskort tilhørende fiktive beboere -- Test-registreringsenheder (enten dedikerede test-enheder, hvis UDP-beskeder peger på Salto testdatabasen fremfor den normale / eller mulighed for, at normale enheder kan kodes til at sende til testdatabasen, hvis der anvendes test-identitetskort) - Integrationstest-procedurer, hvor test-identitetskort benyttes på test-registreringsenheder for at teste, at tidsregistreringerne ender i salto testdatabasen - Testperiode på test-server, inden nye patches rulles ud i produktion - Beredsskabstests, hvor der testes for forskellige mulige problematiske scenarier, som det samlede system bør kunne håndtere (fx at VPN-forbindelsen er nede) - Faste testprocedurer ved tilbagevendende begivenheder (fx faste procedurer for, hvordan opsætning af en ny registreringsenhed testes - også med fokus på at teste, om data korrekt ender helt ude i enden af dataflowet i QlikView)."				
20	Datatab ved nedbrud eller menneskelige fejl	KHG og SJM	1	Der er identificeret et tilfælde, hvor en sagsgennemgang viste, at en medarbejder ved en fejl havde slettet en data-disk på SALTO serveren på et tidspunkt den 10. juni 2020, og man kunne konstatere, at der manglede data i tidsrummet den 9. juni 2020 kl. 22:16:39 til den 10. juni 2020 kl. 10:18:16. Det var muligt at genskabe dele af de tabte data for perioden 9. juni 2020 kl. 22:16:39 til 9. juni 2020 kl. 24:00:00. (for ind- og udgange). Data fra den resterende periode (24:00 til 10:18) var det imidlertid ikke muligt at genskabe.	Hvis der opleves datatab (fx i tilfælde af menneskelige fejl som ved denne hændelse) vil data kunne genskabes automatisk fra seneste backup eller ved en smule mere indsats fra transaktionslogs, hvis disse produceres hyppigere end databasebackups. Der er således en risiko for, at registreringer foretaget efter seneste tidspunkt for backup/transaktionslog kan være umulige at gendanne.	20.1	1. Det vurderes, at implementeringen af daglige fulde backups samt inkrementielle backups i form af transaktionslogfiler hver time er tilstrækkelige indsatser for at reducere konsekvenserne, hvis et datatab foranlediget af en utilsigtet hændelse skulle indtræffe igen. 2. Det vurderes desuden som tilfredsstillende, at der er implementeret yderligere serverovervågning for at sikre, at lignende hændelser i fremtiden hurtigere vil kunne identificeres og at der således hurtigere kan reageres på disse.	8	Arkitektur	NA	NA
21	Problemer ved systemopdatering og genstart	KHG og SJM	1	Der er registreret nedbrud på Salto-systemet den 2.-3. juli 2020 og den 17. juli 2020, som angiveligt skyldtes, at systemservice på den server hos Statens IT, som Salto-systemet er placeret på, ikke genstartede automatisk efter opdateringer af serveren, selvom den er konfigureret til at gøre det.	Hvis Salto-systemet ikke startes korrekt op, så har det flere konsekvenser i den tidsperiode, hvor det er utilgængeligt: - Dels kan beboerregistrering, ind-/udgangsregistrering og melderegistrering ikke afvikles med den normale systemunderstøttelse, og der skal derfor indføres manuel kontrol/registrering i alle disse trin. - Dels kan registreringer fra Salto-systemet fra det tidsrum, hvor Salto-systemet er utilgængeligt, ikke anvendes til anmeldelse af eventuelle overtrædelser.	21.1	Det vurderes, at den implementerede genstartsprocedure effektivt sikrer, at der ikke igen opstår problemer ved genstart efter en systemopdatering.	8	Arkitektur	NA	NA
22	Risiko for datatab, når serveren er utilgængelig for online registreringsenheder	KHG og SJM	1	Det kan forventes, at registreringsenhederne af forskellige årsager på visse tidspunkter kan miste forbindelsen til serveren "Applikationsserver" hos Statens IT. Fx kan MPLS-forbindelsen, Salto-applikationen eller databasen på serveren være utilgængelig i kortere perioder ad gangen. I dette tilfælde, vil enhedernes registreringer ikke bliver registreret i databasen. Systemet bør derfor være designet til, at der kan være utilgængelige perioder, hvor registreringsenhederne ikke kan få forbindelse til serveren.	Hvis systemet ikke i tilstrækkeligt omfang er designet til at kunne håndtere, at der i perioder ikke er forbindelse til serveren, så er der en risiko for, at der sker datatab af registreringer, der finder sted, mens serveren er utilgængelig.	22.1	Det vurderes, at eksisterende lagringsplads på enhederne er tilfredsstillende for at sikre, at der ikke sker datatab. Dette skyldes: - At den enhed med langt flest gennemsnitlige registreringer (indgangsskarsel ved Kærshovedgård) gennemsnitligt har ca. 400 registreringer om dagen. - Der skal således i gennemsnit gå over en uge uden adgang til serveren, før de første af de 3000 registreringer ikke længere kan opbevares på standeren. - Interviewene på begge udrejsecentre har peget på, at der meget sjældent opleves systemnedbrud, og at disse typisk ikke varer ved i lang tid.	2-6	Arkitektur	NA	NA

							- Det vurderes ikke, at det er nødvendigt, at systemet opgraderes til at kunne opbevare flere registreringer, således at systemets maksimale tålelige nedetid udvides til endnu længere end en uge."				
23	Manglende bekræftelse på beskedmodtagelse	KHG og SJM	1	Når de online registreringsenheder kommunikerer med Salto applikationen, så kan det forventes, at enhederne på visse tidspunkter kan miste forbindelse til serveren hos SIT (jf. beskrivelse ved observation 22). Sanistål har bekræftet, at beskeder fra online registreringsenheder sendes via protokollen UDP (Unified Datagram Protocol), som ikke i sig selv understøtter, at der i en kommunikation mellem to enheder er sikkerhed for, at alle afsendte beskeder når succesfuldt frem til modtageren - modsat TCP (Transmission Control Protocol), som understøtter netop dette.	Såfremt der ikke på anden vis er implementeret denne sikkerhed for, at UDP-beskederne succesfuldt modtages og gemmes i databasen, så vil der være stor risiko for, at ikke alle registreringer gemmes i databasen.	23.1	Det vurderes, at den iboende risiko for, at nogen beskeder ikke modtages, er fuldt mitigeret af det kontrollag, som producenten har implementeret uden for UDP-beskederne. Det bemærkes, at det ikke har været muligt at få adgang til Saltos kodebase, da det er et proprietært stykke software, som producenten ikke ønskede at udlevere. Der er dog ingen indikationer fra dataanalyserne på, at producentens beskrivelse ikke er en præcis angivelse af den faktiske implementering.	3-6	Arkitektur	NA	NA
24	Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data	KHG og SJM	1	En af grundene til, at indeværende undersøgelse er blevet igangsat har været, at der grundet tidligere hændelser er blevet sået tvivl om, hvorvidt der på et tidspunkt i dataflowet kan forekomme enten et tab eller forvanskning af data. I dataanalysenr nei afsnit 3.5.2 har kontrol 1-7 til formål at kaste lys på, om der kan påvises nogen form for datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data på et tidspunkt i dataflowet.	Hvis der sker datatab eller forvanskning i dataflowet til og med Salto DB, vil det underliggende datagrundlag for anmeldelser af beboere være fejlbehæftet. Hvis der efterfølgende i dataflowet sker datatab eller forvanskning, kan det betyde, at det datagrundlag, som anvendes af HJEMST's medarbejdere til vurdering af potentielle anmeldelser, kan være fejlbehæftet.		Salto DB har en kontrol, der sikrer, at alle nye hændelser, der indsættes i databasen er unikke.	8	Arkitektur	NA	NA
25	Dobbeltregistreringer på meldestandere	KHG og SJM	1	Det er observeret, at nogle beboere foretager dobbeltregistreringer i forbindelse med melderegistrering for at sikre, at deres registrering er korrekt registreret i AMS. I forbindelse med PwC's dataanalyser (jf. afsnit 3.5.2), er det bekræftet, at der er et stort antal dobbelte registreringer ved meldestandere på begge centre, og at dette forekommer signifikant mere på KHG end på SJM (læs mere i kontrol 8 i afsnit 3.5.2).	Der er ikke nogen reel risiko forbundet med, at beboerne foretager to eller flere melderegistreringer på samme tid. Dog har HJEMST oplevet, at det i forbindelse med behandling af anmeldte sager har været kilde til forvirring blandt parterne i den retslige proces, at der har forekommet flere melderegistreringer fra den samme beboer inden for en kort tidsperiode, da dette potentielt kunne indikere, at der var dubletter, som fejlagtigt blev genereret i løbet af dataflowet.		Der er ingen kendte kontroller, der afholder beboerne for at anvende meldestanderne flere gange i træk. Der er en kontrol i AMS, der sikrer, at en hændelse ikke kan registreres mere end én gang i databasen (Salto DB), så det kan udelukkes, at der skulle være tale om dobbeltregistreringer, som er genereret i systemet ved en fejl.	4	Adfærd	NA	NA

4.6 Vurdering af gennemførte ændringer

UIM har i forbindelse med opfølgning på rapportens konklusioner implementeret en løsning for håndtering af observation 1 om “dataforvanskning i forbindelse med anvendelse af offlineenheder på Kærshovedgård” samt udarbejdet en løsningsmodel for observation 2 om “Uklar proces for tilmelding og tilkobling af nye

registreringsenheder”. PwC har efterfølgende gennemført en gennemgang og vurdering af tiltagene for begge observationer. Dette bilag inkluderer en gennemgang og vurdering af effekten af tiltagene på den oprindelige observation samt den afledte risiko for dataforvanskning og datatab.

Tabel 3: Overblik over to observationer udvalgt til opfølgende analyse

#	Titel	Udrejsecenter	Tilstand*	Prioritet (1-3)**	PAVA (delområde)
1	Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG	KHG	3. Valideret	1	Arkitektur
2	Uklar proces for tilmelding og tilkobling af nye registreringsenheder	KHG og SJM	3. Valideret	1	Governance

Observation 1

Observationen omhandler dataforvanskning i forbindelse med anvendelse af offlineenheder på Kærshovedgård. Observationen indeholder tre problemstillinger omkring tidsforskydning i/af offline registreringsenheder, beboeradfærd med henblik på at undgå registreringer såvel som manglende registreringer i hændelsesloggen i AMS. Problemstillingerne medfører en væsentlig risiko for dataforvanskning, hvorfor PwC har anbefalet at afkoble offline data fra AMS.

UIM’s løsning indebærer en ændring i opsætningen af den daglige hændelseseksporth fra Salto-applikationen til den filtrerede Salto BI DB, jf. figur 10 for systemoverblik. Der er etableret tre hændelseseksporther:

- Online standere fra Kærshovedgård
- Online standere på Sjælsmark
- Alle enheder (online og offline) fra Kærshovedgård.

UIM har fjernet hændelseseksporther for alle enheder (online og offline) på Kærshovedgård med det formål, at offline data ikke indgår i den filtrerede SALTO BI DB server og hermed Hjemrejsestyrelsens kontroller af potentielle brud på melde-, opholds- og underretningspligt. PwC har gennemført en række kontrolanalyser med henblik på at vurdere, om løsningen nedbringer risikoen for dataforvanskning og datatab.

Opfølgende kontrol af tilstedeværelse af offline data fra Kærshovedgård i AMS efter endt hændelseseksporth	
Fremgangs-måde	• Denne kontrolanalyse undersøger tilstedeværelsen af data fra Kærshovedgårds offline-enheder i AMS efter endt hændelseseksporth. • Følgende kontrolleres: 1. At data fra offline-enheder ikke længere eksisterer i databasen SALTO på UDLSQLBIO3 (specifikt i tabellen “dbo.Hjemrejsestyrelsen”). 2. At data fra offline-enheder ikke eksisterer i tabellen “dbo.KHG” på databasen SALTO, dvs, at det resterende eksporth job i Salto applikationen ikke også medtager data fra offline-enhederne på Kærshovedgård. 3. At det daglige eksporthjob fra Salto applikationen er nedlukket, dvs. at jobbet “Hjemrejsestyrelsen” i Salto applikationen er sat på pause. 4. At de midlertidige datafiler med formatet “KHG-saltolog-Hjemst_(\$DAY)_(\$MONTH)_(\$YEAR).csv” er fjernet fra Salto-serveren i mappen D:\FileHub\Export.
Resultat af kontrollen	• Det kan bekræftes at der ikke længere eksisterer data fra offline-enheder i SALTO databasen (Salto BI DB) på UDLSQLBIO3 i tabellen dbo.Hjemrejsestyrelsen (delkontrol 1). Det er observeret d. 06-05-2021, at tabellen dbo.Hjemrejsestyrelsen er tom. • Det kan bekræftes at der ikke eksisterer data fra offline-enheder i SALTO databasen (Salto BI DB) på UDLSQLBIO3 i tabellen dbo.KHG (delkontrol 2)

	• Det kan bekræftes at det daglige eksportjob "Hjemrejsestyrelsen" fra Salto applikationen er deaktiveret og sidst kørt den 2021-05-05 00:00:00 (delkontrol 3). • Det kan bekræftes at midlertidige datafiler er fjernet fra mappen D:\FileHub\Export på Applikationsserveren (UDLUDREJSE01) (delkontrol 4).
Overordnet konklusion	Der er i forbindelse med kontrolanalyserne ikke fundet data fra Kærshovedgårds offline-enheder i Salto BI DB, hvorved det kan konkluderes, at disse data på kontrol tidspunktet ikke eksporteres til Salto BI DB. Det bemærkes, at offline data med denne løsning stadig vil være tilgængelig i Salto Applikationen og dermed i AMS.

Observation 2

Det er i forbindelse med undersøgelsen observeret, at der ikke er formaliseret en proces for opsætning og tilkobling af nye online registreringsenheder på udrejsecentrene. Det indebærer en risiko for, at nye registreringsenheder ikke tilkobles AMS, hvilket kan medføre, at beboernes registreringer fra passager ind og ud af centrene samt i forbindelse med meldepligt ikke indgår i AMS. Årsagen hertil er, at der i forbindelse med de daglige dataeksporter afvikles en række planlagte jobs, der udlæser data og hvori der sker en specifik filtrering på data i forhold til de pågældende registreringsenheder. Opsætning af nye registreringsenheder kræver derfor en manuel omkonfigurering af de pågældende jobs, hvis omkonfigureringen ikke foretages, så vil registreringer fra nye online registreringsenheder ikke fremgå af AMS.

UIM har udarbejdet en proces for opsætning, tilkobling samt test af nye enheder. Processen beskriver de enkelte aktiviteter og placerer samtidigt ansvaret for udførsel af disse hos henholdsvis HJEMST, Statens IT og UIM's koncern IT. Der er overordnet set defineret følgende med henblik på at minimere risikoen for mangelfulde datasæt i AMS som følge af manglende tilkobling af nye registreringsenheder:

- Indførsel af krav om formel ændringsanmodning (fra HJEMST til UIM Koncern IT)
- Ansvarsplacering af håndtering af ændringsanmodning (UIM Koncern IT)

- Verifikationstest af ændringen (HJEMST)
- Dokumentation for udførte handlinger i forbindelse med håndtering af ændringsanmodningen (HJEMST og UIM Koncern IT).

UIM har således defineret konkrete aktiviteter og placeret ansvar for gennemførsel af aktiviteterne i forbindelse med opsætning og tilkobling af nye online registreringsenheder på udrejsecentrene. PwC har gennemført en vurdering processen med henblik på at vurdere, om den nedbringer risikoen for databab.

Opfølgende vurdering af instruks for proces for tilmelding og opkobling af nye registreringsenheder	
Fremgangsmåde	• Denne vurdering undersøger aktiviteter og dækningsgrad af processen, med henblik på at vurdere effektiviteten af disse og dermed, om risikoen for databab minimeres. • Følgende kontrolleres særligt: 1. At de beskrevne aktiviteter er fyldestgørende i forhold til minimering af risikoen for databab 2. At ansvar for gennemførsel af aktiviteter er defineret for alle de beskrevne aktiviteter 3. At de gennemførte aktiviteter afprøves og verificeres og at der er mulighed for "fallback" (tilbagevenden til foregående sagstrin) ved fejl 4. At alle relevante aktiviteter dokumenteres.
Resultat af kontrollen	• Det kan bekræftes at processen for tilmelding og tilkobling af nye registreringsenheder er fyldestgørende i forhold til de definerede aktiviteter i ændringsanmodningen • Det kan bekræftes at der er defineret ansvar for gennemførsel for alle de relevante aktiviteter • Det kan bekræftes, at verifikation påkræves før endelig idriftsættelse • Det kan bekræftes at dokumentation påkræves, både i form af ændringsanmodninger samt for gennemførsel af verifikationstest.
Overordnet konklusion	Det er forbindelse med gennemgangen vurderet, at UIM's instruks for opsætning og tilkobling af nye online-registreringsenheder på udrejsecentrene er fyldestgørende i forhold til mitigerende af risikoen for databab.

4.7 Vurdering af gennemførte ændringer (2023)

Indledning:

PwC foretog i foråret 2021 en undersøgelse af Udlændinge- og Integrationsministeriets (herfra UIM) Adgangs- og Meldepligtssystem (AMS) på landets to daværende udrejsecentre Kærshovedgård og Sjælsmark.

Her blev 25 observationer identificeret, som i varierende grad kunne medføre risiko for dataforvanskning eller tab af data i AMS.

Heraf blev 2 observationer vurderet til at udgøre en *direkte* risiko for at kunne medføre dataforvanskning eller tab af data i AMS. Yderligere blev 17 observationer vurderet til at udgøre en *indirekte* risiko for datatab/-forvanskning. Endelig blev der for de 6 resterende observationer enten ikke observeret en problematik eller den afledte risiko var allerede afhjulpet. Det blev samlet anbefalet, at observationerne skulle indgå i arbejdet med at videreudvikle og forbedre AMS med det formål eksempelvis at opnå større organisatorisk modenhed, øge brugervenlighed, etablere testmiljø mv.

De 2 observationer, som blev vurderet at udgøre en *direkte* risiko for dataforvanskning eller tab, blev i forbindelse med undersøgelsen afhjulpet i 2021 og tilbage var således kun observationer, som *indirekte* kunne udgøre en risiko. UIM har sidenhen iværksat en række tiltag mhp. at afhjælpe disse *indirekte* risici samt at videreudvikle AMS generelt.

I efteråret 2022 har PwC gennemgået de tiltag, som UIM har gennemført, med det formål at dokumentere tiltagene og disses effekt, samt at vurdere om de resterende *indirekte* risici for dataforvanskning og/eller datatab er nedbragt som følge af tiltagene.

PwC's opfølgning kan konkludere, at yderligere 10 observationer fra AMS-undersøgelsen nu er håndteret, således at den indirekte risiko forbundet med observationerne er nedbragt. UIM har derudover igangsat projekter relateret til governance af systemet samt etablering af tilsyns- og kontrolmekanismer for AMS, som adresserer de resterende oprindelige observationer med yderligere tiltag.

Baggrund:

Undersøgelsen af AMS skal ses i lyset af, at Rigsadvokaten den 1. december 2020 besluttede midlertidigt at suspendere brugen af data fra AMS som teknisk bevis i straffesager, da der ifølge Rigsadvokaten var konstateret uregelmæssigheder i dataene i en række sager.

AMS-undersøgelsen (2021) afdækkede, om der var forhold omkring AMS, som udgjorde risici for datatab, dataforvanskning eller forkerte eller manglende registreringer af data, så registreringerne ikke omfattede beboernes reelle færden og passager.

Undersøgelsen omfattede de primære aktiviteter i AMS; fra en udlænding oprettes i AMS ved indkvartering på et udrejsecenter (beboerregistrering), til hvordan de elektroniske registreringer foretages i praksis (indgangs-, udgangs-, og meldepligtsregistrering), samt hvordan disse registreringer overføres (dataflow), så der foreligger data i Hjemrejsestyrelsens sagsbehandlingssystemer til kontrol med udlændingenes opholds- og meldepligt. Selve pålægget af pligter var udenfor undersøgelsens genstandsfelt.

Sikkerhedsniveauet i systemets hardware og software, herunder fx kryptering af data, autentificeringsmekanismer, beskyttelse mod malware og lignende, var ligeledes ikke med i undersøgelsens genstandsfelt.

I forbindelse med AMS-undersøgelsen blev i alt 25 observationer undersøgt og kategoriseret efter væsentlighed.

Observationer med prioritet "1" betød, at der var tale om et teknisk eller systemmæssigt forhold, som kunne udgøre en direkte risiko for dataforvanskning eller tab, og at håndtering af disse observationer derfor var en forudsætning for at undgå risiko for dataforvanskning. I alt 7 prioritet "1" observationer blev undersøgt. Heraf blev 2 observationer vurderet til at udgøre en direkte risiko, og disse blev i forbindelse med undersøgelsen afhjulpet. For de resterende 5 prioritet "1"-observationer blev der enten

ikke observeret en problematik, eller det blev dokumenteret at den afledte risiko allerede var afhjulpel.

Observationer med prioritet ”2” og ”3” betød, at observationerne ikke selv kan give anledning dataforvanskning eller -tab. Dog er det observationer, som kan udgøre en indirekte risiko, idet de omhandler problematikker relateret til AMS, herunder fx organisering og procedurer, som er med til at opretholde driften af AMS.

I alt 18 prioritet ”2” og ”3” observationer blev undersøgt. Heraf blev 12 prioritet ”2”-observationer og 5 prioritet ”3”-observationer vurderet som forhold, som burde blive inkluderet i UIM’s arbejde med videreudvikling AMS på længere sigt, idet der var tale om forhold som i nogen grad kunne udgøre en indirekte risiko for datatab eller forvanskning. I forhold til den resterende ”prioritet ”3”-observation blev der ikke identificeret en problematik.

Fokus for opfølgning på tiltag (nærværende bilag):

Fokus for nærværende opfølgende bilag har været at verificere de tiltag, som UIM har foretaget mhp. at håndtere de 17 prioritet ”2” og ”3” observationer, som blev identificeret i den oprindelige AMS-undersøgelse.

I nærværende bilag gennemgås således for hver af disse observationer:

- Beskrivelse af observationen og den afledte risiko (opsummering fra AMS-undersøgelsen)
- Beskrivelse af tiltag samt dokumentation herfor
- Vurdering af tiltagets design (hensigten)
- Vurdering af tiltagets implementering (effekten)
- Konklusion ift. nedbringelse af risiko.

Nærværende opfølgning er således ikke en gentagelse af en fuld undersøgelse af AMS som system, men en fokuseret opfølgning på de tiltag, som UIM har gennemført siden afslutning af AMS-undersøgelsen i foråret 2021.

Dokumentationen for tiltag er indsamlet i perioden oktober og november 2022. I forbindelse hermed er der foretaget en opfølgende besigtigelse på udrejsecenter Kærshovedgaard i november 2022. Sjælsmark har fra marts 2022 ikke været anvendt som udrejsecenter, og der er derfor ikke foretaget en opfølgende besigtigelse på Sjælsmark i forbindelse med PwC’s gennemgang af UIM’s tiltag.

Nærværende bilag skal læses i sammenhæng med AMS-undersøgelsen fra 2021, som indeholder den fulde beskrivelse af AMS-processerne, de oprindelige observationer,

samt af de afledte risici. Nærværende bilag gentager ikke disse beskrivelser i fuld længde, men gengiver disse gennem kortere opsummeringer.

PwC’s vurderinger af UIM’s tiltag afspejler status som dokumenteret i efteråret 2022.

Sammenfatning:

PwC’s opfølgning i efteråret 2022 har verificeret, at der er gennemført tiltag, som håndterer de 8 ud af de 12 oprindelige prioritet ”2”-observationer fra AMS-undersøgelsen.

Af de resterende 4 prioritet ”2”-observationer omhandlede de 3 hhv. uklart procesejerskab, systemejerskab, samt tilsyns- og kontrolkoncept. Forhold, som gjorde at der i processerne omkring AMS kunne være tvivl om ”hvem gør hvad”, samt at der var manglende systematisk opfølgning på, om processerne understøttede et passende kontroltryk i forhold til pligterne. For disse tre forhold gælder, at Hjemrejsestyrelsen har fået det overordnede ejerskab for system, processer, samt internt tilsyn og kontrol med AMS. Hjemrejsestyrelsen arbejder i skrivende stund i særskilte projekter med at forankre system- og procesejerskabet (roller og ansvar) i organisationen samt med udarbejdelse af internt tilsyns- og kontrolsystem. PwC har derfor ikke i regi af denne rapport verificeret disse tiltag, da de er under udarbejdelse.

Den 4. prioritet ”2”-observation omhandlede, at der på Udrejsecenter Sjælsmark i perioder kunne være åbentstående døre, hvormed der var en risiko for at udlændinge, som havde ophold på centeret, kunne passere udenom de autoriserede adgange, hvor deres passager bliver elektronisk registreret. Sjælsmark bliver dog ikke for nuværende anvendt, som udrejsecenter, og problematikken er således ikke længere relevant.

PwC’s opfølgning har ligeledes verificeret at der er gennemført tiltag, som håndterer 2 ud af 5 prioritet ”3”-observationer.

For de resterende 3 prioritet ”3”-observationer (observation 16, 18 og 19) er tiltag under udarbejdelse.

For de i alt 17 observationer, som denne opfølgende undersøgelse vedrører, er i alt 10 observationer således håndteret, 1 observation er ikke pt. aktuel, og tiltag er under udarbejdelse for de resterende 6 observationer. Tabel 1 på næste side giver et samlet og opdateret overblik over de oprindelige 25 observationer fra AMS-undersøgelsen.

Tabel 1. Overblik over observationer identificeret i forbindelse med undersøgelsen af AMS

#	Titel	Prioritet (1-3)*	Delområde	**Tilstand
1	Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG	1	Arkitektur	Valideret afhjulpet i undersøgelse 2021
2	Uklar proces for tilmelding og tilkobling af nye registreringsenheder	1	Governance	Valideret afhjulpet i undersøgelse 2021
3	Uhensigtsmæssig placering af streghedescanner (uden biometri)	2	Arkitektur	Valideret afhjulpet i efteråret 2022
4	Manglende organisatorisk forankring af proces for håndtering af incidents	2	Governance	Valideret afhjulpet i efteråret 2022
5	Lav kritikalitetsscore	2	Governance	Valideret afhjulpet i efteråret 2022
6	Uklart procesejerskab for AMS-processen	2	Governance	Tiltag under udarbejdelse
7	Uklart systemejerskab for AMS-komplekset	2	Governance	Tiltag under udarbejdelse
8	Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere	2	Adfærd	Valideret afhjulpet i efteråret 2022
9	Anti-passback ikke implementeret for streghedekort	2	Validering/Kontrol	Valideret afhjulpet i efteråret 2022
10	Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentrene	2	Adfærd	Valideret afhjulpet i efteråret 2022
11	Periodevist åbne døre ved personsłuse	2	Adfærd	Pt. ikke relevant, da observationen vedrører Sjælsmark
12	Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre	2	Validering/Kontrol	Tiltag under udarbejdelse
13	Mangelfuld automatisk advisering ved driftsproblemer	2	Arkitektur	Ingen problematik observeret i efteråret 2022
14	Anti-passback ikke aktiveret for biometriske kort	2	Validering/Kontrol	Valideret afhjulpet i efteråret 2022
15	Fejlregistreringer ved bruger meldt som udeblevet	3	Validering/Kontrol	Ingen problematik observeret i efteråret 2022
16	Kort slettefrist for øvrige logoplysninger i driftsmiljøet	3	Arkitektur	Tiltag under udarbejdelse
17	Forkert brug af datamodel (fx brug af statuskoder i beboers navnefelt)	3	Adfærd	Valideret afhjulpet i efteråret 2022
18	Uhensigtsmæssige roller og adgange i relation til ændring af stamdata	3	Validering/Kontrol	Tiltag under udarbejdelse
19	Mangelfuldt testmiljø	3	Arkitektur	Tiltag under udarbejdelse
20	Datatab ved nedbrud eller menneskelige fejl	1	Arkitektur	Valideret afhjulpet i undersøgelse 2021
21	Problemer ved systemopdatering og genstart	1	Arkitektur	Valideret afhjulpet i undersøgelse 2021
22	Risiko for datatab, når serveren er utilgængelig for online registreringsenheder	1	Arkitektur	Valideret afhjulpet i undersøgelse 2021
23	Manglende bekræftelse på beskedmodtagelse	1	Arkitektur	Ingen problematik observeret i undersøgelse 2021
24	Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data	1	Arkitektur	Ingen problematik observeret i undersøgelse 2021
25	Dobbeltregistreringer på meldestandere	3	Adfærd	Ingen problematik observeret i undersøgelse 2021

*Prioritet er opgjort i en skala i forhold til væsentligheden i at håndtere den tilknyttede risiko for dataforvanskning. Prioritet afspejler vurdering af risiko fra AMS-undersøgelsen 2021. **Tilstand angiver hvorvidt der ved undersøgelse af observationen enten "ikke blev identificeret nogen problematik", eller hvorvidt en identificeret problematik er "valideret afhjulpet" enten i forbindelse med AMS-undersøgelsen 2021 eller i forbindelse med PwC's opfølgende verificering af UIM's tiltag i 2022.

4.7.1 Metode

For hver af de 17 observationer, som denne opfølgning omhandler, er der taget udgangspunkt i, hvad den konkrete problematik omhandlede, samt hvorvidt problematikken medførte en indirekte risiko for dataforvanskning eller tab i AMS.

Tiltag, som er iværksat af UIM, mhp. at afhjælpe den konkrete observation, er verificeret ud fra følgende trin:

1. Det er **dokumenteret**, at et tiltag er gennemført. Dvs. at PwC har set dokumentation for tiltaget enten via besigtigelse eller tilsendt materiale fra UIM, Hjemrejsestyrelsen, Udlændingestyrelsen eller Kriminalforsorgen.
2. Det er herefter vurderet, om tiltaget er **designet** således, at det imødegår den problematik, som blev identificeret i PwC's oprindelige undersøgelse. Dvs. hvorvidt tiltaget er målrettet observationen og den afledte risiko fra undersøgelsen.
3. Derpå er det vurderet, om tiltaget er **implementeret** således, at tiltaget effektivt imødekommer den problematik, som blev identificeret i PwC's oprindelige undersøgelse. Dvs. hvorvidt, det kan demonstreres at løsningen er implementeret i praksis.

Slutteligt er der for de enkelte observationer foretaget en samlet vurdering af, hvorvidt eventuel risiko for dataforvanskning eller tab i AMS, som var afledt af den konkrete observation, er blevet nedbragt tilstrækkeligt som følge af tiltagene.

4.7.2 Dokumentation og vurdering af tiltag

Opfølgning på observation 3 - Uhensigtsmæssig placering af streghkodescanner

Observationen omhandler, at ud- og indgangsscannerne i portvagten på KHG (streghkodescanner uden biometri) var placeret tæt på hinanden, hvilket indebar en risiko for, at en medarbejder kunne komme til at foretage en registrering af en passage i den forkerte retning, fx registrering af en indgang, som skulle have været en udgang. Registreringen ville i så fald ikke stemme overens med udlændingens faktiske færden (fx en indgang som en udgang).

Problematikken er relevant, da to på hinanden følgende passager i samme retning gør det vanskeligt at koble ind- og udgange korrekt i AMS-data, ligesom at observationen kan medføre, at der ikke ville fremgå et retvisende billede af beboerens færden ud fra disse AMS-data.

3. Opfølgende kontrol af streghkodescanner	
UIM tiltag	UIM har flyttet streghkodescannerne på KHG, således at den ene nu er monteret ved centerpersonalets indgangsvindue (her henvender udlændinge med streghkodekort sig, når de skal lukkes ind på centeret), mens den anden er monteret ved centerpersonalets udgangsvindue (her henvender udlændinge med streghkodekort sig, når de skal lukkes ud ad centeret). På denne måde udføres scanningshandlingen i naturlig sammenhæng med kontrol af udlændingens passage. Der er ligeledes påsat klistermærker på ind- og udgangsscannerne, så disse klart kan skelnes fra hinanden.
Fremgangs- måde og dokumentation for tiltag	PwC har ved besigtigelse på KHG set at streghkodescanner er placeret som beskrevet ovenfor og har dokumenteret dette med fotos.
Vurdering af tiltagets design	Det vurderes, at tiltaget om flytte streghkodescanneren ved portvagten er hensigtsmæssigt og tilstrækkeligt ift. at minimere risikoen for, at en medarbejder ved en fejl kan komme til at foretage en registrering i forkert retning. Det vil således med de nye placeringer være en direkte unaturlig bevægelse at foretage en forkert registrering.

Vurdering af tiltagets implementering	Implementeringen ift. streghkodescanner er udført i overensstemmelse med ovenstående og vurderes effektiv.
Konklusion ift. nedbringelse af risiko	Det vurderes at risikoen for at en medarbejder ved en fejl laver en forkert registrering (fx en udgang fremfor en indgang), som derved kan nedbringe validiteten af data i forhold til beboerens færden ind og ud ad centeret, er nedbragt tilstrækkeligt ved at flytte streghkodescanneren.

Opfølgning på observation 4 - Manglende organisatorisk forankring af proces for håndtering af incidents

Observationen omhandler et tidligere enkeltstående dokumenteret tilfælde af en konkret incident (driftsforstyrrelse), hvor UIM ved en fejl ikke blev orienteret om hændelsen eller udbedring af fejlen. Observationen blev i AMS-undersøgelsen gennem interviews med UIM KIT, HJEMST samt udrejsecentrene vurderet som udtryk for en generel problematik omkring uklarhed om processen for håndtering af incidents.

Problematikken er relevant, da uklarhed omkring rolle-/ansvarsfordelingen i processen for håndtering af incidents kan medføre, at der ikke reageres rettidigt ved systemnedbrud, samt at der ikke iværksættes procesmæssige “workarounds” for at sikre, at AMS-processen kan fortsætte med en alternativ proces, mens eventuelle systemnedbrud pågår. Samtidig kan det have som konsekvens, at der bruges fejlbehæftede data i retsmæssig sammenhæng, hvis HJEMST og/eller UIM ikke er bevidste om, at der har været problemer med systemet i den periode, hvor en incident har fundet sted.

4. Opfølgende kontrol af manglende organisatorisk forankring af proces for håndtering af incidents	
UIM tiltag	- UIM har en incident-proces, som hensigtsmæssigt og tilstrækkeligt redegør klart for ansvars- og rollefordelingen i forbindelse med incident-håndtering (dette blev ligeledes dokumenteret i AMS-undersøgelsen 2021). - HJEMST har som tiltag implementeret instruks i hele koncernen vedrørende advisering af HJEMST i forbindelse med incidents, således at HJEMST kan

	tage højde for eventuelle hændelser i forbindelse med deres konkrete behandling af anmeldelser af brud på pligter. Instruksen er til UIM KIT mhp. at orientere HJEMST om incidents, som UIM KIT bliver opmærksomme på, herunder også fra Statens IT. Instruksen er ligeledes sendt til Kriminalforsorgens medarbejdere på udrejsecentrene, således at HJEMST bliver orienteret om eventuelle incidents, som bliver identificeret på udrejsecentrene fx hvis streghedescanner ikke virker. HJEMST har udarbejdet en tjekliste, som skal anvendes i forbindelse med sagsbehandling, hvori det indgår, at sagsbehandleren i forbindelse med en konkret anmeldelse af brud på pligter kontrollerer, hvorvidt der har været driftsforstyrrelse på de datoer, som indgår i datagrundlaget for anmeldelsen.
Fremgangs- måde og dokumentation for tiltag	- PwC har gennemgået UIM's Koncern It's generelle procedure for håndtering af hændelser: "Proces for incident management" af 2017 samt tilhørende "Bilag 1: Kommunikationsflow ved prioritet 1 og 2 incidents", samt "Guide til oprettelse af it-driftsnyheder på intranettet" af 2016 (Disse er uændrede siden AMS-undersøgelsen 2021). - PwC har gennemgået HJEMST's instruks til UIM Koncern-It og Kriminalforsorgen angående advisering af HJEMST i forbindelse med driftsforstyrrelser, "Instruks vedrørende hændelser i forbindelse med opholds- og meldepligtsregistreringer" (senest opdaterede udgave er fra 20. september 2022). - PwC har observeret, at kontaktoplysninger i HJEMSTs instruks fra september af 2022 er opdaterede. - PwC har gennemgået HJEMST's tjekliste, som anvendes i forbindelse med anmeldelser. PwC har ligeledes foretaget en gennemgang af processen hos en HJEMST-medarbejder. - Endeligt har PwC udført stikprøvekontrol af processen ved at gennemgå konkrete incidents fra 2022, for at verificere, at den beskrevne incident-proces er blevet fulgt i de konkrete tilfælde, herunder at HJEMST er blevet underrettet om tilfældene.
Vurdering af tiltagets design	- Det er PwC's vurdering, at HJEMSTs instruks om advisering om driftsforstyrrelser er klar og forståelig, og det fremgår tydeligt af instruksen, at HJEMST skal orienteres straks ved eventuelle driftsforstyrrelser i AMS. Det er oplyst, at der ved eventuelle systemforstyrrelser foretages en vurdering fra UIM KIT ift. om der har været databas som følge af forstyrrelsen. - HJEMST's tjekliste i forbindelse med anmeldelser er en step-by-step-guide i forhold til at foretage eventuel anmeldelse i forbindelse med en udlændings brud på sine pligter (opholds-, underretnings- og meldepligt). Det fremgår af guiden tydeligt, at der i forbindelse med en anmeldelse skal tjekkes, hvorvidt der har været hændelser i SALTO eller øvrige driftsforstyrrelser, som gør, at der ikke skal anmeldes for bestemte tidspunkter eller dage i anmeldelsesperioden. Det fremgår desuden af tjeklisten, at dette kan tjekkes på konkrete sager i P630 (en sag til hvert år).

	- Det fremgår ligeledes tydeligt af HJEMST's tjekliste, at der ikke skal foretages anmeldelse for dage, hvor der har været driftsforstyrrelser, og at HJEMST foretager vurderingen ud fra et forsigtighedsprincip. - Det er PwC's vurdering, at såfremt disse instrukser og vejledninger følges, vil HJEMST være orienteret om eventuelle driftsforstyrrelser.
Vurdering af tiltagets implementering	- HJEMST's instruks om advisering om driftsforstyrrelser opdateres jævnligt, og kontaktoplysninger i instruksen er derfor opdaterede. - Det er desuden erfaret, at registreringspraksis i det tilfælde hvor den elektroniske registrering som følge af en incident er sat ud af kraft, vil overgå til en manuel proces, hvor indgange, udgange og meldepligtsregistreringer noteres i et papir-skema, som indsendes til HJEMST. - Ud fra stikprøvekontrollen er det observeret, at der i 2022 havde været 3 konkrete hændelser, hvor incidentprocessen og incidentinstruksen er blevet aktiveret. - PwC har gennemgået forløbet omkring de 3 hændelser, og det er PwC's samlede vurdering at incidentprocessen fungerer efter hensigten, og at HJEMST underrettes om incidents, således at der kan tages højde herfor i sagsbehandlingen.
Konklusion ift. nedbringelse af risiko	Det vurderes, at den organisatoriske forankring af incident-processen er gennemført i organisationen, og at der kommunikeres mellem de relevante parter (Udrejsecenteret, HJEMST, UIM KIT og SIT) omkring håndtering af incidents. Herunder er det vurderingen, at HJEMST orienteres, når der har været driftshændelser, hvorpå HJEMST fører oversigt over sådanne tilfælde, således at det indgår i sagsbehandlingen af, om der grundlag for at foretage anmeldelse. Den indirekte risiko for databas i forbindelse med incident-proceduren er således nedbragt.

Opfølgning på observation 5 - Lav kritikalitetsscore

Observationen omhandler, at Salto i kundeaftalen mellem UIM og SIT havde en kritikalitetsscore vurderet til niveau "D", som er det laveste niveau i SIT's kundeaftaler.

Problematikken er relevant, da kritikalitetsvurderingen af AMS til niveau "D" kan medføre, at medarbejdere i SIT nedprioriterer incidents, der er relateret til AMS, og at der dermed ikke følges op i tide på disse incidents med risiko for databas.

5. Opfølgende kontrol ang. Lav kritikalitetsscore

UIM tiltag	Statens IT har primo november 2021 ændret kritikalitetsniveauet fra D til A.
-------------------	--

Fremgangsmåde og dokumentation for tiltag	UIM Koncern-It kan selv tilgå et system hos Statens IT, hvor grundlæggende oplysninger om UIM's It-systemer kan ses. PwC har fra UIM KIT modtaget det såkaldte "systemkort" for Salto, som UIM har trukket fra Statens It. Af systemkortet fremgår det at kritikalitetsscoren er opdateret fra D til A.
Vurdering af tiltagets design	Kritikalitetsscore A er den højest mulige kritikalitetsscore, og dette betyder, at SIT prioriterer driftsforstyrrelser/nedbrud i AMS før systemer med lavere kritikalitetsscore. "Designmæssigt" er kritikalitetsscore A således det bedst mulige.
Vurdering af tiltagets implementering	Tiltaget vurderes implementeret effektivt.
Konklusion ift. nedbringelse af risiko	Det vurderes, at risikoen for at SIT nedprioriterer incidents relateret til Salto, er nedbragt ved at opjustere kritikalitetsscoren.

Opfølgning på observation 6 - Uklart procesejerskab for AMS-processen

Observationen omhandler, at det var uklart, hvilken organisation eller aktør, der havde det samlede procesejerskab for AMS på tværs af dataflowet.

Problematikken er relevant, idet der er risiko for, at den samlede AMS-proces ikke lever op til de forretningsmæssige og forvaltningsmæssige mål om at opretholde kontroltrykket i forhold til beboernes pligter. Det kan igen have en effekt på tilstedeværelse samt kvalitet og validitet af data.

Det overordnede procesejerskab er blevet tildelt Hjemrejestyrelsen, og arbejde med at udarbejde og implementere roller og ansvarsfordeling i procesejerskab pågår hos Hjemrejestyrelsen.

PwC har derfor ikke vurderet tiltag, da arbejdet er igangværende.

Opfølgning på observation 7 - Uklart systemejerskab for AMS-processen

Observationen omhandler at den samlede systemdokumentation og viden om systemet var fragmenteret og fordelt på mange forskellige personer fra forskellige organisationer (særligt US, HJEMST, leverandøren Sanistål, Koncern IT, SIT, udrejsecentrene samt de lokale leverandører Actas og Holstebro Låseteknik). Endvidere blev observeret manglende formalisering og usystematisk kontrakt- og leverandørstyring.

Problematikken er relevant for at sikre, at data også over tid er tilstrækkelig sikret mod databas og forvanskning i takt med, at systemet opdateres og tilrettes, og at der sker udskiftning af medarbejdere på vigtige poster.

Det overordnede systemejerskab er blevet tildelt Hjemrejestyrelsen, og arbejdet med at udarbejde og implementere roller og ansvarsfordeling i relation til systemejerskabet pågår hos Hjemrejestyrelsen.

PwC har derfor ikke vurderet tiltag, da arbejdet er igangværende.

Opfølgning på observation 8 - Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere

Observationen omhandler, at anti-passback-funktionen ikke automatisk var aktiveret for manuelt oprettede brugere i AMS, hvorved et biometrisk kort kunne anvendes til to på hinanden følgende passager enten ind eller ud ad udrejsecentret.

Problematikken er relevant, da to på hinanden følgende passager i samme retning gør det vanskeligt at koble ind- og udgange korrekt i AMS-data, og herved ville der ikke fremgå et retvisende billede af beboerens færd ud fra disse AMS-data.

8. Opfølgende kontrol ang. Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere

UIM tiltag

Brugere oprettes som udgangspunkt ikke manuelt, og hvis det alligevel skulle ske, er der en vejledning om den manuelle oprettelse. Af vejledningen fremgår bl.a., at anti-passback skal slås til for manuelt oprettede brugere, ligesom det fremgår, hvordan det slås til.

Fremgangs- måde og dokumentation for tiltag	- PwC har set vejledning til Kriminalforsorgens medarbejdere på udrejsecentrene (af november 2022) - PwC har fået gennemgået processen for manuel oprettelse brugere af en medarbejder fra Kriminalforsorgen ved besigtigelse på udrejsecenter Kærshovedgård 22. november 2022.
Vurdering af tiltagets design	I vejledning til Kriminalforsorgens medarbejdere på udrejsecentrene (af november 2022) (jf. Opfølgning på Observation 10), fremgår det: - At oprettelse af en bruger foregår ved at hente stamdata via IBS. Ved oprettelse af brugere efter denne proces er anti-passback automatisk slået til. - Det beskrives desuden i vejledningen, at Kriminalforsorgens medarbejdere skal kontrollere, at anti-passback er slået til. - Endeligt beskrives det også, hvordan anti-passback slås til, hvis brugeren undtagelsesvist bliver nødt til at blive oprettet manuelt.
Vurdering af tiltagets implementering	Tiltaget vurderes at være effektivt.
Konklusion ift. nedbringelse af risiko	Tiltaget vurderes at være tilstrækkelig effektivt ift. at sikre, at anti-passback funktionen er slået til for de biometriske kort. Det kan evt. indgå i UIM's tilsyns og kontrol-koncept, at udføre opfølgende kontrol med, om anti-passback er slået til for alle brugere.

Opfølgning på observation 9 - Anti-passback ikke implementeret for strejkodekort

Observationen omhandler, at anti-passback funktionen ikke blev aktiveret, da passage blev afprøvet to gange i samme retning med scanning af strejkodekort hos portvagten.

Problematikken er relevant, da to på hinanden følgende passager i samme retning gør det vanskeligt at koble ind- og udgange korrekt i AMS-data, og herved vil der ikke fremgå et retvisende billede af beboerens færdens ud fra disse AMS-data.

9. Opfølgende kontrol ang. Anti-passback ikke implementeret for strejkodekort

UIM tiltag	Anti-passback er i november 2022 implementeret for strejkodekort. Hjemrejsestyrelsen har i forbindelse med udrulningen af nye FUSE-kort i november 2022 udarbejdet en vejledning til Kriminalforsorgens medarbejdere, hvori det beskrives, hvordan det tjekkes, at anti-passback-funktionen er slået til
-------------------	--

	for alle kort. Når en beboer oprettes via IBS, slås anti-passback-funktionen automatisk til. Hvis en beboer i få tilfælde oprettes manuelt, skal anti-passback ligeledes aktiveres manuelt. Der er udarbejdet en vejledning herom, jf. observation 8. Hjemrejsestyrelsen har ligeledes oprettet en log i form af et excel-ark, hvor det noteres, hvis et kort har været låst som følge af anti-passback og efterfølgende låses op af centerpersonalet. HJEMST har oplyst, at loggen sendes fra KRFO til HJEMST hver 14. dag, så disse oplysninger kan indgå i styrelsens sagsbehandling.
Fremgangs- måde og dokumentation for tiltag	PwC har i december 2022 via. fået demonstreret afprøvningen af to på hinanden følgende indgange med strejkodekort. Kontrollen viste, at anti-passback funktionen blev slået til, da to indgange uden mellemliggende udgang blev forsøgt, og brugeren blev nægtet adgang. PwC har ligeledes set vejledningen, som er udarbejdet og dennes beskrivelser af håndtering af anti-passback. PwC har december 2022 set loggen, som er tiltænkt at dokumentere tilfælde, hvor kort genoplåses. Denne ligger i udprintet form synligt hos portvagten til registrering af tilfælde, hvor kort skal låses op.
Vurdering af tiltagets design	Det er vurderingen, at oprettelsesproceduren som beskrevet i vejledningen effektivt sikrer, at anti-passback er slået til for alle kort. Det er vurderingen, at loggen over genoplåsning af kort bidrager til at gøre data for indgange og udgange mere gennemskueligt, i tilfælde af at kort er blevet låst som følge af anti-passback og senere genoplåst.
Vurdering af tiltagets implementering	Det er vurderingen, at anti-passback fungerer og er slået til på strejkodekort, og at vejledningen sikrer, at anti-passback er slået til for alle kort. PwC har ikke haft mulighed for at verificere implementeringen og effektiviteten af loggen for genoplåste kort, idet HJEMST oplyser, at der ikke har været tilfælde af kort, som skulle låses op og derfor registreres i loggen.
Konklusion ift. nedbringelse af risiko	PwC's vurdering er, at anti-passback fungerer efter hensigten for strejkodekort, og at risikoen for at der kan foretages to på hinanden følgende passager i samme retning, uden at dette noteres, er nedbragt.

Opfølgning på observation 10 - Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentre

I AMS-undersøgelsen blev det observeret, at der på tværs af AMS-processen var mangelfuld vejledning, oplæring og opfølgning til Kriminalforsorgens medarbejdere. Problematikken er relevant, idet der er risiko for, at manglende træning og forståelse af AMS kan medføre menneskelige fejl og uhensigtsmæssigheder i anvendelsen af systemet.

10. Opfølgende kontrol ang. Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentre	
UIM tiltag	Der er i forbindelse med udrulningen af nye FUSE-kort udarbejdet en vejledning til Kriminalforsorgens medarbejdere på udrejsecentre (af november 2022), som omfatter vejledning i: - Oprettelse af nye beboere på udrejsecentre i Salto - Udstedelse af FUSE-kort (biometriske kort) til indgange, udgange og registrering af meldepligt - Udstedelse af ID-kort med billede (ingen adgange på kortet) - Udstedelse af nøglebrikker til indvendige døre - Udstedelse af stregkodekort til de få beboere, som af fysiske årsager ikke kan anvende FUSE-kort - Eventuel flytning af beboere mellem udrejsecentre - Anti-passback funktionen og procedure for, hvordan en beboers kort genaktiveres, hvis kortet som følge af anti-passback-funktionen er blevet låst - Genaktivering af kort, hvis bruger er genopdukket efter at være udeblevet - Håndtering af incidents
Fremgangs-måde og dokumentation for tiltag	• PwC har gennemgået Vejledning til Kriminalforsorgens medarbejdere på Udrejsecenter Kærshovedgård. • PwC har ved besigtigelse på Kærshovedgård fået oprettet kort til test-personer, samt fået gennemgået de forskellige processer i praksis ved Kriminalforsorgens medarbejdere på centeret. • HJEMST har ligeledes redegjort for oplæringsprocessen i forbindelse med udrulning af de nye FUSE-kort
Vurdering af tiltagets design	Det er PwC's vurdering, at vejledningen er fyldestgørende og dækker processerne på tværs af AMS

Vurdering af tiltagets implementering	HJEMST har oplyst, at der i forbindelse med udrulningen af nye FUSE-kort og indførelsen af en ny praksis for oprettelse af beboere har været iværksat en 3-dages oplæring af kriminalforsorgens medarbejdere på udrejsecenteret, hvor både HJEMST og Udlændingestyrelsen også har været tilstede for at sikre sig, at det nye system fungerer efter hensigten. KRFO har ligeledes fokus på, at alle medarbejdere får gennemgået og anvender vejledningen.
Konklusion ift. nedbringelse af risiko	Det vurderes, at vejledningen på tværs af AMS-processerne reducerer risikoen for menneskelige fejl og uhensigtsmæssigheder i anvendelsen af systemet.

Opfølgning på observation 11 - Periodevist åbne døre ved personsłuse

Observationen omhandler, at dørene ved personsłusen på SJM til tider stod åbne, idet lukkemekanismen i døren er langsom.

Sjælsmark er dog ikke længere et udrejsecenter, og denne specifikke problematik er således kun relevant, hvis Sjælsmark genetableres som udrejsecenter.

Tiltag er derfor for nærværende ikke relevante, hvorfor tiltag ikke er vurderet i forbindelse med dette opfølgende bilag.

Opfølgning på observation 12 - Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre

Observationen omhandler, at Udlændingestyrelsens tilsyn med Kriminalforsorgens drift af udrejsecentre i henhold til operatørkontrakten, ikke havde fokus på kvalitetssikring eller kontrol med adgangs- samt ind- og udgangsregistreringer i relation til dataforvanskning.

Problematikken er relevant, idet der er risiko for, at manglende fysiske og adfærdsmæssige tilsyn kan medføre, at Kriminalforsorgens drift af udrejsecentre og kontrol med indgangs-, udgangs- og meldepligtsregistreringer, ikke i tilstrækkelig grad tager højde for håndteringen af risici relateret til dataforvanskning og databas.

Arbejdet med at udarbejde og implementere et koncept for interne tilsyn og kontroller, som løbende kan følge op på kontrolniveauet, pågår i dag hos Hjemrejsestyrelsen og i

samarbejde med Udlændingestyrelsen. Tiltag er derfor ikke vurderet i forbindelse med dette opfølgende bilag.

Opfølgning på observation 13 - Mangelfuld automatisk advisering ved driftsproblemer

Observationen omhandler, at Hjemrejsestyrelsen og Kriminalforsorgens medarbejdere ikke får automatisk besked om driftsforstyrrelser fra Statens IT eller UIM KIT.

Problematikken er relevant, idet en manuel proces kræver korrekt ageren af medarbejdere på tværs af UIM's styrelser og operatører for at incidents bliver håndteret rigtigt.

13. Opfølgende kontrol ang. mangelfuld automatisk advisering ved driftsproblemer	
UIM tiltag	Der er ikke foretaget nogen automatiseringer af incidentsprocessen. Incident-håndtering i forhold til AMS er fortsat en manuel proces, men den manuelle proces er til gengæld styrket betydeligt (jf. observation 4).
Fremgangs-måde og dokumentation for tiltag	Pwc har kontrolleret om den eksisterende manuelle proces for incident-håndtering fungerer efter hensigten, jf. opfølgning på observation 4.
Vurdering af tiltagets design	Det er PwC's vurdering, at den manuelle proces for incidenthåndtering er designet, således at den nedbringer risici for dataforvanskning eller tab som følge af incidents, jf. observation 4.
Vurdering af tiltagets implementering	Det er PwC's vurdering, at den manuelle proces for incidenthåndtering er tilstrækkelig og fungerer efter hensigten jf. observation 4.
Konklusion ift. nedbringelse af risiko	Det er PwC's vurdering, at den manuelle proces håndtering af incidents er styrket (jf. Observation 4), hvorved den indirekte risiko for datatab i forbindelse med incident-proceduren er nedbragt. En automatisk proces vurderes derfor ikke at være nødvendig.

Opfølgning på observation 14 - Anti-passback ikke aktiveret for biometriske kort

Observationen omhandler, at anti-passback funktionen ikke blev aktiveret, da passage blev afprøvet gennem den selvbetjente indgangsregistrering ved karrusel (med biometrisk kort).

Problematikken er relevant, da to på hinanden følgende passager i samme retning gør det vanskeligt at koble ind- og udgange korrekt i AMS-data og herved ville der ikke fremgå et retvisende billede af beboerens færd ud fra disse AMS-data.

14. Opfølgende kontrol ang. Anti-passback ikke aktiveret for biometriske kort	
UIM tiltag	I forbindelse med implementeringen af biometriske FUSE-kort på Kærshovedgård i november 2022, er anti-passback-funktionen aktiveret på alle kort. Hjemrejsestyrelsen har i forbindelse med udrulningen af FUSE-kort i november 2022 udarbejdet en vejledning til Kriminalforsorgens medarbejdere vedrørende implementering af FUSE-kort, hvori det beskrives, hvordan det tjekkes at anti-passback-funktionen er slået til. Når en beboer oprettes via. IBS, slås anti-passback-funktionen automatisk til. Hvis en beboer i få tilfælde oprettes manuelt, skal anti-passback ligeledes aktiveres manuelt. Hjemrejsestyrelsen har ligeledes oprettet en log i form af et excel-ark, hvor tilfælde noteres, hvis kort har været låst som følge af anti-passback og efterfølgende låses op. HJEMST har oplyst, at loggen skal sendes fra KRFO til HJEMST hver 14. dag, så disse oplysninger kan indgå i arbejdet med anmeldelser af brud på opholdspligt.
Fremgangs-måde og dokumentation for tiltag	Ved besigtigelse på Kærshovedgård d. 22. november 2022 afprøvede PwC at foretage to på hinanden følgende registreringer af passager i samme retning gennem karrusellen med et biometrisk kort. Resultatet af kontrollen var, at dør nr. 2 låste, da det blev forsøgt at foretage passagen i samme retning anden gang. Dvs., at man bliver låst inde i slusen, når anti-passback funktionen slår til. PwC har ligeledes set vejledningen, som er udarbejdet og dennes beskrivelser af håndtering af anti-passback. PwC har set loggen, som er tiltænkt at dokumentere tilfælde, hvor kort genoplåses. Denne ligger i udprintet form synligt hos portvagten til registrering af tilfælde, hvor kort skal låses op.

Vurdering af tiltagets design	Det er vurderingen, at oprettelsesproceduren som beskrevet i vejledningen effektivt sikrer, at anti-passback er slået til for alle kort. Det er vurderingen, at loggen over genoplåsning af kort bidrager til at gøre data for indgange og udgange mere gennemskueligt, i tilfælde af at kort er blevet låst som følge af anti-passback og senere genoplåst.
Vurdering af tiltagets implementering	Det er vurderingen, at anti-passback fungerer og er slået til på de nye FUSE-kort, og at vejledningen sikrer, at anti-passback er slået til for alle kort. PwC har ikke haft mulighed for at verificere implementeringen og effektiviteten af loggen for genoplåste kort, idet HJEMST oplyser, at der ikke har været tilfælde af kort, som skulle låses op og derfor registreres i loggen.
Konklusion ift. nedbringelse af risiko	PwC's vurdering er, at anti-passback fungerer efter hensigten for de biometriske kort, og at risikoen for at der kan foretages to på hinanden følgende passager i samme retning, uden at dette noteres, er nedbragt.

Opfølgning på observation 15 - Fejlregistreringer ved bruger meldt som udeblevet

Observationen omhandler, at såfremt en beboer har været registreret som værende uden for udrejsecentret i for lang tid, så registreres beboeren automatisk som udeblevet med statussen "forbyd bruger" i AMS. Herefter kan beboeren ikke længere foretage ind- og udgangsregistrering med hverken streghodekort eller biometrisk kort. Hvis beboeren senere genopdukker vil der – når personen forsøger at passerede indgang med sit kort – stå "Åbning ikke tilladt: Nogle ugyldig". Denne logmeddelelse virker imidlertid kun for de biometriske kort og ikke for streghodekort.

15. Opfølgende kontrol ang. fejlregistreringer ved bruger meldt som udeblevet

UIM tiltag	HJEMST har oplyst, at leverandøren Sanistål pr. 9. maj 2022 har implementeret og bekræftet, at der ved brug af streghodekort i loggen vil stå "Åbning ikke tilladt: nogle ugyldig", hvis en beboer har været udeblevet.
Fremgangsmåde og	PwC har modtaget skærbillede af AMS-hændelsesloggen fra en bruger, som har anvendt streghodekort, hvor denne bruger har været udeblevet.

dokumentation for tiltag	
Vurdering af tiltagets design	Logoplysningen sikrer, at det fremgår tydeligt og letforståeligt af loggen, hvis en beboer har været udeblevet for længe og overtrådt sin opholdspligt, hvorfor kortet låses.
Vurdering af tiltagets implementering	Tiltaget er nu implementeret for streghodekort, således, at der ikke er forskel på logoplysningerne ved biometriske kort og streghodekort.
Konklusion ift. nedbringelse af risiko	Logoplysningen er en servicemeddelelse til kriminalforsorgens medarbejdere, og ikke et forhold, som kan medføre at en udlændings indgangs- eller udgangsregistreringer vil fremgå forkert af AMS-data. En bruger meldes som udeblevet af Kriminalforsorgen, når beboeren er konstateret udeblevet i 72 timer. Dette foregår ved at Kriminalforsorgens medarbejdere melder brugeren som udeblevet i IBS, som HJEMST sagsbehandlere ligeledes tilgår i forbindelse med sagsbehandlingen. Data om udlændingens indgange og udgange fra centeret og herunder deres udeblivelse i længere tid vil altså fremgå korrekt af AMS - også når personen senere måtte genopdukke og i den forbindelse skal have genaktiveret sit kort ved at blive registreres i systemet som "genopdukket". Der er således ingen risiko for datatab eller -forvanskning i forhold beboerens indgangs- og udgangsregistreringer. Observationen er en prioritet "3"-observation og handler om at sikre, at systemet kan fungere smidigt ift. indgange og udgange på centeret.

Opfølgning på observation 16 - Kort slettefrist for øvrige logoplysninger i driftsmiljøet

Observationen omhandler, at nogle typer af logs (applikations-, system- og SQL-log) slettes efter relativt kort tid (fx ca. 9 mdr. for applikationsloggen).

Problematikken er relevant i forbindelse med gennemgang af retslige sager, såfremt historiske hændelser i logoplysningerne kan bidrage til efterforskning.

UIM har oplyst, at tiltag er under udarbejdelse vedrørende slettefrister. PwC har derfor ikke vurderet tiltag i forbindelse med denne observation.

Opfølgning på observation 17 - Forkert brug af datamodel

Observationen omhandler, at der ved undersøgelsen blev fundet eksempler på, at Kriminalforsorgens medarbejdere anvendte navnefeltet i datamodellen som et notefelt til at angive, at en beboer var flyttet fra centret.

Problematikken er relevant, fordi det kan være vanskeligt at føre sager tilbage i tid for beboere, som ikke længere opholder sig på udrejsecentret, hvis det ikke længere vil være muligt at fremsøge beboerens data, fordi navnet på beboeren er ændret i databasen.

17. Opfølgende kontrol ang. forkert brug af datamodel	
UIM tiltag	HJEMST har pålagt Kriminalforsorgen, at alle nye beboere oprettes via stamdata fra CARL2 via IBS, og der er udarbejdet vejledning i dette. Der er ligeledes via leverandøren Sanistål blevet indført et ekstra felt i datamodellen i Salto, således, at der er et felt hvor KRFO-medarbejderne kan skrive bemærkninger i.
Fremgangs-måde og dokumentation for tiltag	PwC har set "Vejledning til Kriminalforsorgens medarbejdere på Udrejsecenter Kærshovedgård" af november 2022 (jf. Opfølgning på observation 10. Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentrene). PwC har ligeledes set skærbillede fra Salto, hvor der som supplement til beboerens stam-data er et bemærkningsfelt til noter.
Vurdering af tiltagets design	I vejledningen beskrives, hvordan en bruger oprettes ved, at beboerens stamdata hentes i IBS og herved eksporteres til Salto. Der kan således, hvis beboeren oprettes via IBS ikke forekomme fejl i fx brugerens navn i første omgang. Derudover betyder det ekstra bemærkningsfelt, at der nu er et sted, hvor Kriminalforsorgens medarbejdere kan skrive bemærkninger som "frihedsberøvet" eller "flyttet", sådan at navnefeltet ikke anvendes til dette.
Vurdering af tiltagets implementering	Det vurderes at være en effektiv og tilstrækkelig løsning, at brugere ikke længere oprettes manuelt (jf. opfølgning på observation 10), samt at der er indført et ekstra bemærkningsfelt i datamodellen.
Konklusion ift. nedbringelse af risiko	Risiko for forkert brug af datamodel vurderes at være nedbragt.

Opfølgning på observation 18 - U hensigtsmæssige roller og adgange i relation til ændring af stamdata

Observationen omhandler, at der på KHG ikke var indarbejdet en begrænsning af medarbejdernes rettigheder til at oprette beboere og ændre i stamdata. Alle kriminalforsorgens medarbejdere havde de samme rettigheder.

Problematikken er relevant, idet det medfører en øget risiko for fejloprettelser, fejlindtastninger eller fejltildeling af adgange, hvis ikke det sikres, at alene medarbejdere med rette viden, erfaring og fokus kan oprette beboere.

18. Opfølgende kontrol ang. uhensigtsmæssige roller og adgange i relation til ændring af stamdata	
UIM tiltag	UIM har på tidspunktet for udarbejdelsen af dette bilag ikke iværksat tiltag mhp. at begrænse antallet af medarbejdere, som kan rette i udlændingenes brugerprofiler. Arbejdet med oprettelse og flytning af beboere er dog beskrevet i "Vejledning til Kriminalforsorgens medarbejdere på Udrejsecenter Kærshovedgård" af november 2022.
Fremgangs-måde og dokumentation for tiltag	PwC har set "Vejledning til Kriminalforsorgens medarbejdere på Udrejsecenter Kærshovedgård" af november 2022. PwC har ligeledes ved besigtigelse på KHG d. 22. november 2022 fået gennemgået processen ved en af Kriminalforsorgens medarbejdere.
Vurdering af tiltagets design	I vejledningen beskrives, hvordan en bruger oprettes og evt. senere flyttes, herunder er der en vejledning med screenshots af, hvordan beboerens stamdata hentes i IBS og herved eksporteres til Salto, hvordan udlændingen tildeles forskellige adgange på centeret mv. Den udarbejdede vejledning vurderes delvist at nedbringe risikoen for datatab og/eller -forvanskning.
Vurdering af tiltagets implementering	Proceduren for at oprette en nye beboer på centeret incl. tildeling af de rigtige adgange, samt evt. senere behov for tilrettelse i data i forbindelse med flytning eller frihedsberøvelse, vurderes at være kompleks. Det vurderes således, at ikke alle Kriminalforsorgens medarbejdere vil kunne gennemskue processen eller føle sig komfortable med at foretage procedurer, hvor beboerens stamdata skal tilgås, ikke mindst oprettelse af brugeren.

**Konklusion ift.
nedbringelse af
risiko**

At der er udarbejdet en vejledning medfører, at risikoen for fejloprettelser, fejlindtastninger eller fejltildeling af adgange mindskes. Problemstillingerne relateret til observationen vurderes derfor delvist afhjulpet.

Det er dog PwC's vurdering, at processer, som vedrører ændringer i udlændingens stamdata, samlet set er for kompleks til at alle medarbejdere bør have rettigheder til at foretage disse processer. Det vil derfor forsat være en anbefaling, at kun udvalgte medarbejdere (superbrugere) må oprette beboere og ændre i beboeres stam-data, og at der følges systematisk op på tildeling af roller og adgange, samt disses anvendelse.

Opfølgning på observation 19 – Mangelfuldt testmiljø

Observationen omhandler, at der ikke var et testmiljø, hvor det kunne sikres, at ændringer i systemlandskabet blev implementeret og testet, inden de blev rullet ud i produktionsmiljøet.

Problematikken er relevant, da nye systemopdateringer kan udgøre en risiko for at fejl og uventede hændelser indtræffer i selve produktionsmiljøet, hvis ændringerne i systemet ikke forinden er testet i et testmiljø.

UIM har oplyst, at arbejdet med indførelsen af et testmiljø er under igangsæt. Der er derfor på tidspunktet for udarbejdelsen af dette bilag ikke foretaget nogen tiltag.

© 2023 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed.



4.8 Vurdering af gennemførte ændringer (november 2023)

Hjemrejsestyrelsen (HJEMST) har i 2023 arbejdet med yderligere opfølgning på nogle af de oprindelige observationer fra undersøgelsen af Adgangs og meldepligtssystemet (AMS). PwC har gennemført en gennemgang og vurdering af tiltagene for disse observationer.

Observationerne omhandler procesejerskab, systemejerskab, samt internt tilsyn. Disse observationer er håndteret i et samlet governance-projekt, hvor der er udarbejdet processer, samt fordelt roller og ansvar for den fremadrettede håndtering af disse opgaver.

PwC har bistået HJEMST med at designe koncepter for håndtering af procesejerskab, systemejerskab og tilsyn. PwC har efterfølgende fulgt op på, at koncepterne er implementeret i overensstemmelse med det, der blev aftalt i projektets styregruppe. I det følgende bilag er design, samt implementering kort beskrevet efter samme metode som anvendt til verificering af tiltag i Bilag 4.7 med henblik på at vurdere, hvorvidt disse tiltag nedbringer risici for forvanskning og/eller -tab af AMS-data.

Derudover, har Hjemrejsestyrelsen i foråret 2023 opdaget et teknisk problem med hensyn til anti-passback-funktionen på stregkodekort, og vurderingen af tiltag for observation 9 er derfor opdateret og indgår ligeledes i dette bilag.

Tabel 1. Overblik over to observationer udvalgt til opfølgende analyse (november 2023)

#	Titel	Prioritet (1-3)*	Delområde	**Tilstand
6	Uklart procesejerskab for AMS-processen	2	Governance	Valideret afhjulpet november 2023
7	Uklart systemejerskab for AMS-komplekset	2	Governance	Valideret afhjulpet november 2023
9	Anti-passback ikke implementeret for stregkodekort	2	Validering/Kontrol	Valideret afhjulpet i marts 2023
12	Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre	2	Validering/Kontrol	Valideret afhjulpet november 2023

*Prioritet er opgjort i en skala i forhold til væsentligheden i at håndtere den tilknyttede risiko for dataforvanskning. Prioritet afspejler vurdering af risiko fra AMS-undersøgelsen 2021. **Tilstand angiver, hvorvidt der ved undersøgelse af observationen enten "ikke blev identificeret nogen problematik", eller hvorvidt en identificeret problematik er "valideret afhjulpet" enten i forbindelse med AMS-undersøgelsen 2021 eller i forbindelse med PwC's opfølgende verificering af UIM's tiltag i 2022 og 2023.

Opfølgning på observation 6 - Uklart procesejerskab for AMS-processen

Observationen omhandler, at det var uklart, hvilken organisation eller aktør, der havde det samlede procesejerskab for AMS på tværs af data-flowet.

Problematikken er relevant, idet der er risiko for, at den samlede AMS-proces ikke lever op til de forretningsmæssige og forvaltningsmæssige mål om at opretholde kontroltrykket i forhold til beboernes pligter. Det kan igen have en effekt på tilstedeværelse samt kvalitet og validitet af data.

6. Opfølgende kontrol ang. uklart procesejerskab for AMS-processen	
UIM tiltag	Det overordnede procesejerskab er blevet tildelt HJEMST. PwC har på opdrag fra HJEMST understøttet konkretisering af governance i relation til AMS på udrejsecenter Kærshovedgård. Der er udarbejdet overblik over AMS-processerne opdelt på tre niveauer, samt udarbejdet beskrivelser af de enkelte processer. Herefter er roller og ansvar for de enkelte processer fordelt blandt aktørerne i AMS gennem et RACI-diagram. For hver enkelt opgave i forbindelse med AMS-processerne er det således defineret hvilke aktører, som henholdsvis er ansvarlige for at udføre opgaver (R = Responsible), overordnede ansvarlige for at igangsætte og efterfølgende godkende det udførte arbejde (A = Accountable), hvem der skal konsulteres (C = Consulted), samt hvem der skal holdes informeret (I = Informed). Endeligt er der udarbejdet en køreplan for implementering samt årshjul for aktiviteter, så implementeringen og den efterfølgende driftssituation struktureres og tidsfastsættes. Dette arbejde blev afsluttet i marts 2023. HJEMST har efterfølgende taget initiativ til at formalisere samarbejderne gennem konkrete aftaler, samt effektueret samarbejdet i en koordinationsgruppe mellem Hjemrejsestyrelsen (HJEMST), Udlændingestyrelsen (US) og Koncern-IT (KIT).
Fremgangsmåde og dokumentation for tiltag	Som dokumentation for design af tiltag foreligger afrapporteringen for Governance og Tilsyn for Adgangs og Meldepligtssystemet (AMS) af marts 2023, hvor projektet blev afsluttet. Herunder procesbeskrivelser, samt fordeling af roller og ansvar mellem aktørerne Hjemrejsestyrelsen, Udlændingestyrelsen, Kriminalforsorgen, Koncern-IT, Statens IT, Sanistål og LåseteknikMidt. Som dokumentation for organisatorisk implementeringen har PwC set:

	• Samarbejdsaftale mellem HJEMST og US (august 2023). • Overblik over samarbejdsgrundlag omkring AMS (udarbejdet af KIT). • Beskrivelse af koordinationsgruppen for AMS.
Vurdering af tiltagets design	Det vurderes at processerne, såfremt de er implementeret, sikrer, at der på tværs af AMS tages højde for risici for dataforvanskning og/eller -tab, samt at aktørerne er koordinerede i forhold til løbende håndtering af risici.
Vurdering af tiltagets implementering	- Samarbejdsaftalen mellem HJEMST og US fra august 2023 formaliserer ansvarsfordeling og roller i forhold til AMS, således at HJEMST har det overordnede ansvar for AMS, herunder proces- og systemansvar samt ansvar for tilsyn med systemet. Mens US har ansvar at påse drift og vedligehold af den fysiske indretning på et udrejsecenter, herunder ansvar for, at der er funktionsdygtige standere og scannere samt en tilstrækkelig beholdning af nye adgangskort. Det er US, der indkøber og vedligeholder fysiske enheder, der understøtter AMS. - Samarbejdet mellem HJEMST og KIT er formaliseret igennem den eksisterende infrastrukturbeskrivelse, databehandlersaftale samt eksisterende proces for håndtering af sikkerhedshændelser. - Samarbejdet mellem KIT og Statens IT (SIT) er formaliseret igennem den eksisterende kundeaftale og databehandlersaftale. - Koordinationsgruppen for AMS består af repræsentanter fra HJEMST, US og KIT, og afspejler dermed de forskellige myndigheder under Udlændinge- og Integrationsministeriet, som på tværs af koncernen har opgaver og roller relateret til AMS. HJEMST har ansvaret for at indkalde til møder i gruppen hvert kvartal, samt for at udarbejde forslag til mitigerende handlinger, når problemstillinger opstår. HJEMST har ligeledes ansvar for at udarbejde årsrapport som opsummerer beslutninger, mitigerende handlinger og tilsynsresultater for året. Det første møde i koordinationsgruppen er afholdt, hvor bl.a. tilsynskonceptet blev vedtaget og det første tilsyn planlagt.
Konklusion ift. nedbringelse af risiko	Det vurderes, at tiltagene både i design om implementering nedbringer risikoen for dataforvanskning og tab, idet HJEMST har påtaget sig et mere tydeligt samlet ansvar for processerne på tværs af AMS, samt sikrer koordinering mellem alle de involverede aktører og håndtering af problemstillinger i koordinationsgruppen.

Opfølgning på observation 7 - Uklart systemejerskab for AMS-processen

Observationen omhandler at den samlede systemdokumentation og viden om systemet var fragmenteret og fordelt på mange forskellige personer fra forskellige organisationer (særligt US, HJEMST, leverandøren Sanistål, KIT, SIT, udrejsecentrene samt de lokale leverandører Actas og Holstebro Låseteknik). Desuden blev der observeret manglende formalisering og usystematisk kontrakt- og leverandørstyring.

Problematikken er relevant for at sikre, at data også over tid er tilstrækkelig sikret mod datatab og forvanskning i takt med, at systemet opdateres og tilrettes, og at der sker udskiftning af medarbejdere på vigtige poster.

7. Opfølgende kontrol ang. uklart systemejerskab for AMS-komplekset	
UIM tiltag	Det overordnede systemejerskab er blevet tildelt Hjemrejestyrelsen. PwC har på opdrag fra HJEMST understøttet konkretisering af governance, herunder governance af systemunderstøttelsen, i relation til AMS på udrejsecenter Kærshovedgård. Der er udarbejdet overblik over AMS-processerne, herunder alle processer relateret til systemunderstøttelse, opdelt på tre niveauer, samt udarbejdet beskrivelser af de enkelte processer. Herefter er roller og ansvar for de enkelte processer fordelt blandt aktørerne i AMS gennem et RACI-diagram. Endeligt er der udarbejdet en køreplan for implementering samt årshjul for aktiviteter, så implementeringen og den efterfølgende driftssituation struktureres og tidsfastsættes. Dette arbejde blev afsluttet i marts 2023. HJEMST har efterfølgende i samarbejde med KIT udarbejdet et opdateret overblik over systemlandskab og data-flow, samt påbegyndt en struktureret indsamling af systemdokumentation for at have et samlet overblik over systemdokumentationen hos HJEMST.
Fremgangs-måde og dokumentation for tiltag	Som dokumentation for design af tiltag foreligger afrapporteringen for Governance og Tilsyn for Adgangs og Meldepligtssystemet (AMS) af marts 2023, hvor projektet blev afsluttet. Herunder opgavebeskrivelser i relation til systemunderstøttelsen af AMS-komplekset, samt fordeling af roller og ansvar mellem aktørerne Hjemrejestyrelsen, Udlændingestyrelsen, Kriminalforsorgen, Koncern-IT, Statens IT, Sanistål og LåseteknikMidt. Som dokumentation for organisatorisk implementeringen har PwC set: • Samarbejdsaftaler som nævnt i observation 6 ang. procesejerskab

	• Tilsynskoncept angående årlig kontrol med opdatering af systemdokumentation • Opdateret overblik over systemlandskab og data-flow • Høring af KIT og US angående systemdokumentation • Indsamlet systemdokumentation
Vurdering af tiltagets design	Det vurderes, at roller og ansvarsfordeling for systemlandskabet, opfølgning i koordinationsgruppen, samt tilsynskonceptet for kontrol med opdatering af systemdokumentation, sikrer at risici for dataforvanskning og/eller -tab holdes nede også over tid.
Vurdering af tiltagets implementering	- I samarbejdsaftalen mellem HJEMST og US er det konkretiseret at placering af standere, opgradering af udstyr m.v. sker efter dialog mellem US og HJEMST, samt at det er US, der indkøber og vedligeholder fysiske enheder. - I tilsynskonceptet er det præciseret at US har ansvaret for at holde systemdokumentation for hardware opdateret, samt at KIT har ansvaret for at holde systemdokumentation for software opdateret. KIT og US indberetter løbende systemændringer til HJEMST, og HJEMST fører kontrol med vedligeholdelse af systemdokumentation på tværs af AMS gennem et årligt skriftligt tilsyn. HJEMST har sat første tilsyn med systemdokumentationen i gang.
Konklusion ift. nedbringelse af risiko	Det vurderes, at tiltagene både i design om implementering nedbringer risikoen for dataforvanskning og tab også over tid, idet HJEMST har påtaget sig det samlede systemejerskab og har implementeret årlig kontrol med at systemdokumentationen er opdateret på tværs af AMS.

Opfølgning på observation 9 - Anti-passback ikke implementeret for streghodekort

Observationen omhandler, at anti-passback-funktionen ikke blev aktiveret, da passage blev afprøvet to gange i samme retning med scanning af streghodekort hos portvagten.

Problematikken er relevant, da to på hinanden følgende passager i samme retning gør det vanskeligt at koble ind- og udgange korrekt i AMS-data, og herved vil der ikke fremgå et retvisende billede af beboerens færden ud fra disse AMS-data.

9. Opfølgende kontrol ang. anti-passback ikke implementeret for streghodekort	
UIM tiltag	Anti-passback er i november 2022 implementeret for streghodekort. HJEMST har i forbindelse med udrulningen af nye FUSE-kort i november 2022 udarbejdet en vejledning til Kriminalforsorgens medarbejdere, hvori det beskrives, hvordan det tjekkes, at anti-passback-funktionen er slået til for alle kort. Når en beboer oprettes via. IBS, slås anti-passback-funktionen automatisk til. Hvis en beboer i få tilfælde oprettes manuelt, skal anti-passback ligeledes aktiveres manuelt. Der er udarbejdet en vejledning herom, jf. observation 8. HJEMST har ligeledes oprettet en log i form af et excel-ark, hvor det noteres, hvis et kort har været låst som følge af anti-passback og efterfølgende låses op af centerpersonalet. HJEMST har oplyst, at loggen løbende sendes fra KRFO til HJEMST, så disse oplysninger kan indgå i styrelsens sagsbehandling. Efter implementeringen af anti-passback på streghodekort er HJEMST i februar 2023 dog blevet opmærksomme på flere IT-tekniske udfordringer mht. anti-passback for streghodekort, som gør anti-passback-funktionen mangelfuld. Bl.a. er det observeret at anti-passback-funktionen kun opretholdes på streghodekortet i 24 timer efter den seneste passage. Problemerne kan ikke løses uden omfattende udskiftning af software, og HJEMST har derfor valgt at implementere en ekstra manuel kontrol med brugere af streghodekort. Kontrollen indebærer, i følge internt notat fra HJEMST af d. 10. marts 2023, at der for hver beboer med streghodekort (i marts 2023 11 beboere), føres en individuel optegnelse over disse beboeres passager. I følge HJEMST noteres passagen i logbogen, herunder om det er en ind- eller udgang og klokkeslæt herfor. Den særskilte log fungerer således som et supplement til de elektroniske registreringer, så Kriminalforsorgen, kan være opmærksom på, hvis en beboer måtte have en passage i samme retning to gange i træk.
Fremgangs-måde og	PwC har i december 2022 via. videoopkald fået demonstreret afprøvningen af to på hinanden følgende indgange med streghodekort. Kontrollen viste, at

dokumentation for tiltag	anti-passback-funktionen blev slået til, da to indgange uden mellemiggende udgang blev forsøgt, og brugeren blev nægtet adgang. PwC har ligeledes set vejledningen, som er udarbejdet og dennes beskrivelser af håndtering af anti-passback. PwC har december 2022 set loggen, hvori tilfælde af genoplåste kort dokumenteres. Denne ligger i udprintet form synligt hos portvagten til registrering af tilfælde, hvor kort skal låses op. PwC er bekendt med de tekniske udfordringer observeret ift. opretholdelsen af anti-passback-funktionen op streghodekort via. HJEMST interne notat a marts 2023. Efter at HJEMST og KRFO i marts 2023 har indført en individuel optegnelse for hver streghodekortbrugers passager, har PwC d. 28. marts igen set anvendelsen af streghodekort demonstreret i praksis, herunder hvordan de indførte optegnelser for de individuelle brugere anvendes i praksis.
Vurdering af tiltagets design	Det er vurderingen, at oprettelsesproceduren som beskrevet i vejledningen effektivt sikrer, at anti-passback er slået til for alle kort. Det er dog vurderingen på baggrund af HJEMST senere observationer, at anti-passback-funktionen ikke altid forbliver aktiv på streghodekortet. Det er vurderingen, at loggen over genoplåsning af kort bidrager til at gøre data for indgange og udgange mere gennemskueligt, i tilfælde af at kort er blevet låst som følge af anti-passback og senere genoplåst. Det er vurderingen, at de ekstra tiltag, som HJEMST og KRFO har indført mht. at føre manuel kontrol med streghodekort-brugernes passager, ligeledes bidrager til at gøre data for indgange og udgange mere gennemskuelige, og at der ved denne ekstra kontrol er muligt at kompensere for de tekniske mangler ved antipass-back-funktionen for streghodekort.
Vurdering af tiltagets implementering	Det er vurderingen, at vejledningen sikrer, at anti-passback er slået til for alle kort. Men at anti-passback-funktionen ikke fungerer optimalt for streghodekort, idet den ikke forbliver aktiveret mere end 24 timer efter den seneste passage. De ekstra foranstaltninger, som HJEMST har foretaget i forhold at føre en manuel optegnelse over den enkelte streghodekortbrugers passager, vurderes derfor at være den bedst mulige løsning mhp. at sikre kvaliteten af registreringerne og opretholde en anti-passback mekanisme. Optegnelserne over de individuelle brugers passager ligger udprintet hos portvagten. Som supplement til den elektroniske registrering, registrerer portvagten for streghodebrugere således deres passager ind og ud ad centeret manuelt i denne optegnelse. Hver 14. dag scannes disse optegnelser og sendes

	via. mail til HJEMST, som kan bruge disse overblik i tillæg til de elektroniske registreringer.
Konklusion ift. nedbringelse af risiko	PwC's vurdering at risikoen for at der kan foretages to på hinanden følgende passager i samme retning, uden at dette noteres, er nedbragt.

Opfølgning på observation 12 - Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre

Observationen omhandler, at Udlændingestyrelsens tilsyn med Kriminalforsorgens drift af udrejsecentre i henhold til operatørkontrakten ikke havde fokus på kvalitetssikring eller kontrol med adgangs- samt ind- og udgangsregistreringer i relation til dataforvanskning.

Problematikken er relevant, idet der er risiko for, at manglende fysiske og adfærdsmæssige tilsyn kan medføre, at Kriminalforsorgens drift af udrejsecentre og kontrol med indgangs-, udgangs- og meldepligtsregistreringer, ikke i tilstrækkelig grad tager højde for håndteringen af risici relateret til dataforvanskning og datatab.

12. Opfølgende kontrol ang. manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre

UIM tiltag	PwC har på opdrag fra HJEMST understøttet konkretisering af tilsynsbehov i forbindelse med AMS. HJEMST har efterfølgende udarbejdet et komplet tilsynskoncept, som omfatter følgende: 1) Halvårligt uanmeldt tilsyn med operatøren (Kriminalforsorgen)’s administration af AMS-systemet Herunder stikprøvekontrol med brugeroprettelse af biometriske kort, komplet gennemgang af logs for streghodekortbrugere, observation af operatørens generelle opgavevaretagelse, interviews af operatørens medarbejdere, samt kontrol af manuelle registreringer. 2) Årlig kontrol af systemdokumentation Kontrollen indebærer årligt skriftligt tilsyn med systemdokumentation fra US og KIT med henblik på at sikre et samlet opdateret overblik. Ændringer skal løbende indberettes til HJEMST. 3) Insidenthåndtering Tilsynet gennemføres halvårligt ved en fuld gennemgang af hændelser i perioden (idet der er meget få hændelser i løbet af et år). Med hensyn til gennemgang af de konkrete hændelser i perioden er der i forhold til KIT tale om et skriftligt tilsyn, mens der i forhold til Kriminalforsorgen gennemføres tilsyn ved samtale med ledelsen på udrejsecenteret. Ved en gennemgang af de hændelser, der har været i perioden, følges op på hvorvidt HJEMST’s instruks for håndtering af hændelser er fulgt korrekt. Gennemgangen af hændelser holdes desuden op mod den tilsvarende oversigt over hændelser, som modtages fra KIT gennem det skriftlige tilsyn. Dette er samme

	metode, som PwC tidligere har anvendt til at verificere HJEMST’s tiltag i forbindelse med at styrke håndteringen af hændelser i AMS (observation 4 i AMS-undersøgelsen).
Fremgangsmåde og dokumentation for tiltag	Som dokumentation for design af tiltag foreligger afrapporteringen for Governance og Tilsyn for Adgangs og Meldepligtssystemet (AMS) af marts 2023, herunder konkretisering af tilsynsbehov. Derudover har PwC set det færdigt udarbejdede tilsynskoncept, samt relevante bilag. Som dokumentation for organisatorisk implementering har PwC set: • At tilsynskonceptet udarbejdet af HJEMST fastsætter konkret metode for tilsyn, samt roller: 1) udføres af medarbejdere fra US med bistand fra HJEMST, 2) udføres af HJEMST og 3) udføres af US på baggrund af samarbejdsaftalen mellem HJEMST og US. • HJEMST har desuden bekræftet, at det første tilsyn foretaget af HJEMST og US i fællesskab er gennemført i november 2023. • At årlig kontrol med systemdokumentation er igangsat. PwC har set høring afsendt til KIT og US, samt den systemdokumentation, som HJEMST har modtaget indtil videre i forbindelse med høringen.
Vurdering af tiltagets design	Tilsynskonceptet vurderes at dække de centrale processer og arbejdsgange omkring AMS.
Vurdering af tiltagets implementering	Tilsynskonceptet vurderes at være implementeret i organisationen.
Konklusion ift. nedbringelse af risiko	Det er vurderingen, at tilsynskonceptet sikrer, at risici for dataforvanskning og/eller -tab holdes nede over tid, idet regelmæssige tilsyn medfører løbende fokus og opmærksomhed på håndtering af risici relateret til dataforvanskning og datatab.

Tabel 2. Samlet overblik over status på observationer identificeret i forbindelse med undersøgelsen af AMS (november 2023)

#	Titel	Prioritet (1-3)*	Delområde	**Tilstand
1	Dataforvanskning i forbindelse med anvendelse af offlineenheder på KHG	1	Arkitektur	Valideret afhjulpnet i undersøgelse 2021
2	Uklar proces for tilmelding og tilkobling af nye registreringsenheder	1	Governance	Valideret afhjulpnet i undersøgelse 2021
3	Uhensigtsmæssig placering af streghedescanner (uden biometri)	2	Arkitektur	Valideret afhjulpnet i efteråret 2022
4	Manglende organisatorisk forankring af proces for håndtering af incidents	2	Governance	Valideret afhjulpnet i efteråret 2022
5	Lav kritikalitetsscore	2	Governance	Valideret afhjulpnet i efteråret 2022
6	Uklart procesejerskab for AMS-processen	2	Governance	Valideret afhjulpnet i november 2023
7	Uklart systemejerskab for AMS-komplekset	2	Governance	Valideret afhjulpnet i november 2023
8	Anti-passback ikke automatisk aktiveret for manuelt oprettede brugere	2	Adfærd	Valideret afhjulpnet i efteråret 2022
9	Anti-passback ikke implementeret for streghedekort	2	Validering/Kontrol	Valideret afhjulpnet i marts 2023
10	Mangelfuld vejledning, oplæring og opfølgning til medarbejdere på udrejsecentre	2	Adfærd	Valideret afhjulpnet i efteråret 2022
11	Periodevist åbne døre ved personsłuse	2	Adfærd	Pt. ikke relevant, da observationen vedrører Sjælsmark
12	Manglende opfølgning på og tilsyn af kontrolparadigme på udrejsecentre	2	Validering/Kontrol	Valideret afhjulpnet i november 2023
13	Mangelfuld automatisk advisering ved driftsproblemer	2	Arkitektur	Ingen problematik observeret i efteråret 2022
14	Anti-passback ikke aktiveret for biometriske kort	2	Validering/Kontrol	Valideret afhjulpnet i efteråret 2022
15	Fejlregistreringer ved bruger meldt som udeblevet	3	Validering/Kontrol	Ingen problematik observeret i efteråret 2022
16	Kort slettefrist for øvrige logoplysninger i driftsmiljøet	3	Arkitektur	I følge UIM forventes observationen afhjulpnet ultimo Q2 2024
17	Forkert brug af datamodel (fx brug af statuskoder i beboers navnefelt)	3	Adfærd	Valideret afhjulpnet i efteråret 2022
18	Uhensigtsmæssige roller og adgange i relation til ændring af stamdata	3	Validering/Kontrol	Delvist mitigeret af vejledning (se observation 10 i bilag 4.7)
19	Mangelfuldt testmiljø	3	Arkitektur	I følge UIM forventes observationen afhjulpnet primo Q3 2024
20	Datatab ved nedbrud eller menneskelige fejl	1	Arkitektur	Valideret afhjulpnet i undersøgelse 2021
21	Problemer ved systemopdatering og genstart	1	Arkitektur	Valideret afhjulpnet i undersøgelse 2021
22	Risiko for datatab, når serveren er utilgængelig for online registreringsenheder	1	Arkitektur	Valideret afhjulpnet i undersøgelse 2021
23	Manglende bekræftelse på beskedmodtagelse	1	Arkitektur	Ingen problematik observeret i undersøgelse 2021
24	Datatab eller -forvanskning i forbindelse med udtræk, transformation eller indlæsning af data	1	Arkitektur	Ingen problematik observeret i undersøgelse 2021
25	Dobbeltregistreringer på meldestandere	3	Adfærd	Ingen problematik observeret i undersøgelse 2021

*Prioritet er opgjort i en skala i forhold til væsentligheden i at håndtere den tilknyttede risiko for dataforvanskning. Prioritet afspejler vurdering af risiko fra AMS-undersøgelsen 2021. **Tilstand angiver hvorvidt der ved undersøgelse af observationen enten "ikke blev identificeret nogen problematik", eller hvorvidt en identificeret problematik er "valideret afhjulpnet" enten i forbindelse med AMS-undersøgelsen 2021 eller i forbindelse med PwC's opfølgende verificering af UIM's tiltag i 2022 og 2023.

