Skatteministeriet

23. februar 2015
J. nr. 14-0049152
Plannr. 114230

Intern Revision

Rapport 2014

Direktørområdet Økonomi

Fysisk sikkerhed

Modtager:
Departementschef Jens Brøchner

Kopi:
Direktør Karsten Juncher
Direktør Jesper Rønnow Simonsen

- ✓ **Revision**
- ✓ **Rådgivning**
- ✓ **Rapportering**

Forord

Intern Revision (IR) har som en del af den samlede revision for 2014 foretaget opfølgning på revisionsrapporten fra 2013 vedrørende "Fysiske sikkerhed".

Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på.

Rapportens bilag 1 indeholder en systematisk fremstilling af de observationer, som den udførte revision har givet anledning til. Bilaget indeholder tillige en vurdering af de tilknyttede risici samt Intern Revisions forslag til anbefalinger, der kan formindske de vurderede risici. Med udgangspunkt i risikovurderingerne har SKAT udarbejdet handleplaner med henblik på at formindske de vurderede risici. Intern Revisions anbefalinger har været anvendt som inspiration ved udarbejdelse af handleplaner. Vi vil løbende vurdere implementeringen af SKATs handleplaner.

Sidst i rapporten er medtaget en beskrivelse af de prioriteter, der er anvendt ved klassifikationen af de enkelte observationer. Bilaget indeholder herudover en beskrivelse af koblingen mellem observationernes prioriteringer og den samlede overordnede konklusion.

Rapporten har været fremsendt i udkast til den reviderede enhed med henblik på at tilsikre, at IR og den reviderede enhed har en ensartet opfattelse af de faktiske forhold. SKAT har efterfølgende udarbejdet handleplaner, som er indarbejdet i denne rapport.

København, den 23. februar 2015

Kurt Wagner
Revisionschef

Jens Lundgaard
Revisor

1. Formål

Intern Revision har i perioden januar til maj 2014 vurderet i hvilket omfang SKAT har implementeret anbefalingerne jf. tidligere fremsendt rapport benævnt "Revision af fysisk sikkerhed"

Ovennævnte revisionsrapport indeholder en række anbefalinger omfattende procedurer, forretningsgange, og kontroller i og omkring den fysiske adgang til SKATs lokaler og udstyr.

2. Omfang

Ved revisionen, har der været fokus på, følgende områder:

- Opfølgning på 19 anbefalinger, som er givet i forbindelse med tidligere fremsendt rapport "Revision af fysisk sikkerhed" (j.nr. 12-0192851). Opfølgningen indbefatter anbefalinger på disse områder:
    - Fysisk sikkerhed på lokationen "Sluseholmen"
    - Fysisk sikkerhed på lokationen "Nicolai Eigtveds gade"
    - Fysisk sikkerhed i relation til uafhentet print
    - Manglende makulering og anvendelse af skærmlås
    - Synlig identifikation

Revisionen er udført i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews, ved indsamling og stikprøvevis gennemgang af foreliggende materiale samt ved fysisk observation. I forbindelse med revisionen er der gennemført interviews af medarbejdere fra koncernservice, Skattecentrer Korsør, Skattecenter Køge og Skattecenter Sluseholmen. Der er i denne revision ikke foretaget test af kontroller.

3. Konklusion

På baggrund af vores opfølgning er det vores samlede konklusion, at den fysiske sikkerhed på de undersøgte enheder er på et **meget tilfredsstillende niveau**.

Dette begrunder vi på følgende observationer:

- SKAT har implementeret 19 af vores anbefalinger, hvilket har højnet kontrolmiljøet.

- Vi har ved vores opfølgning ikke konstateret nye svagheder, hvorfor der ikke er tilføjet nye anbefalinger.

De åbenstående anbefalinger kan opsummeres således:

Emner	**Prioritet 1** *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**I alt**
Fysisk sikkerhed i de undersøgte områder.	**0**	**0**	**0**	**0**
I alt 2014	**0**	**0**	**0**	**0**
I alt 2013	**5**	**6**	**8**	**19**

Prioriteringerne skal ses i forhold til det reviderede område og er nærmere defineret i bilag 2

Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
12-053 01 **Prioritet 1**	<u>Adgang til SKATs netværk fra receptionens venteområde</u> På adressen Sluseholmen observerede Intern Revision, at man fra opstillet udstyr til brug for borgerne i receptionens venteområde, kan tilgå SKATs systemer (som SKAT medarbejder). En nærmere undersøgelse har vist at de netværksstik i receptionens venteområde som benyttes af omtalte udstyr er en del at SKATs interne netværk. SKATs retningslinjer på området tilsiger at udstyr til brug for borgerne i offentligt tilgængelige områder, skal tilsluttes eget netværk, der går direkte til Internettet. **Status 2014:** Vi har ved fysisk inspektion konstateret, at der ikke længere er et kørende system i kundeområdet, ligesom der ikke længere er et stik, hvor it udstyr kan tilsluttes. **Vi anser punktet for lukket**	Den valgte løsning betyder at stik i offentligt område kan benyttes til at forsøge at skaffe sig uautoriseret adgang (Hacke) til SKATs systemer og data. En Hacker kan således udskifte udstyret med sit eget og forsøge at skaffe sig uautoriseret adgang til SKATs systemer og data.	Intern Revision anbefaler, at • SKAT omkonfigurerer receptionens venteområde således at stik går direkte til Internettet og ikke tillader adgang til SKATs interne netværk • SKAT gennemgår øvrige lokationers offentlige områder og sikrer, at der ikke findes tilsvarende svagheder andre steder.
	SKATs kommentar i 2013: Som Intern Revision har bemærket tog Koncernservice umiddelbart initiativ til at eliminere risikoen. I forbindelse med modtagelsen af dette udkast er der fulgt op med en henvendelse til servicecheferne, som har bekræftet at der er gennem-ført sikringsforanstaltninger på de berørte lokaliteter så uvedkommende ikke kan få adgang til de netværksstik der anvendes til kundepc´ere. I forbindelse med tidsbestillingsprojektet er hovedparten af SKATs ekspeditioner lukket. I forbindelse med sikring af de ændrede adgangsforhold for borgerne på de lokaliteter som anvendes til ekspeditioner efter tidsbestilling er der taget højde for dette.		

Nr.	Observationer	Risici	Anbefalinger
12-053 02 **Prioritet 1**	Uafhentet print Intern Revision har observeret, at det synes at være et generelt problem at uafhentet print ligger i eller omkring SKATs printere. **Status 2014:** Samtlige netværksprintere er udskiftet i november/december 2013, og med indførelse af "paper cut" har SKAT sikret sig, at medarbejderen selv skal initiere udskrifter ved printeren. Det betyder også, at der ikke vil være print, som fejlagtigt sendes til en forkert printer. **Vi anser punktet for lukket**	Dette print omfatter også print af fortrolig karakter og print som vedrører enkeltsager og derfor ikke bør komme andre end den sagsbehandlende medarbejder til kendskab. I yderste konsekvens kan datas beskaffenhed bevirke, at adgang til disse data er en overtrædelse af Persondataloven.	Intern Revision anbefaler, at SKAT overvejer at gennemføre en oplysningskampagne som overfor SKATs personale, ledere såvel som menige medarbejdere, gentager retningslinjerne: • At vi skal benytte lagerfunktionaliteten i printerne, således at fortroligt print først printes når vi står ved printeren. Intern Revision anbefaler desuden, at SKAT fortsætter overvejelserne omkring ”print on demand”, som selvfølgelig vil minimere den påpegede risiko.
	SKATs kommentar i 2013: Udskiftning af samtlige netværksprintere indgår i handleplanen for 2013. Med baggrund i forsøgene med ”print on demand” forventes dette indført på samtlige netværksprintere i forbindelse med udskiftningen.		
12-053 03 **Prioritet 1**	Fortroligt materiale i dagrenovation Intern Revision har observeret, at SKAT ikke på alle lokationer sikrer, at fortroligt materiale makuleres eller på anden måde destrueres på en sådan måde, at udenforstående ikke kan få adgang til data. Udskrifter m.v. bortskaffes typisk med dagrenovationen, hvilket også gælder fortroligt materiale. **Status 2014:** SIR har konstateret, at Skattecenter Korsør og Skattecenter Køge, har fået opstillet aflåselige affaldscontainere til fortroligt materiale. I forbindelse med besøg hos Skattecenter Køge, er det konstateret, at containeren til fortroligt materiale stod uaflåst på gangen, og blev først låst i forbindelse med afhentning. Forholdet blev	Fra udskrifter m.v. lægges til affald, med henblik på bortskaffelse, går affaldet gennem en række hænder, før det ender på forbrændingen eller endnu værre på en losseplads. Som eksempel kan nævnes, rengøringspersonale, interne servicefunktioner, renovationsfolk m.v. Hvert af disse led udgør en risiko for, at dokumenter og indhold kommer uvedkommende til kendskab. I yderste konsekvens kan datas beskaffenhed bevirke, at adgang til disse data medfører en overtrædelse af Persondataloven.	Intern Revision anbefaler, at der i tilslutning til printerrum opstilles aflåste containere til makulering af fortroligt materiale. Hvor der i mindre omfang er fortroligt materiale foreslås det, at der opstilles makulator.

Nr.	Observationer	Risici	Anbefalinger
	drøftet med anvisning om, at containere skal være aflåst både ude og indendørs. Forholdet blev medtaget i Koncernservices rapport om sikkerhedsrunderingen til senere opfølgning. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: Den anbefalede løsning forefindes allerede på nogle lokaliteter, men da risikoen vil være forskellig på de enkelte lokaliteter vil dette indgå som et punkt i Sikkerhed og Miljøs opfølgning på denne rapport og den planlagte risikovurdering af alle SKATs lokaliteter. Sikkerhed og Miljø igangsætter risikovurderingen sammen med Servicecheferne ca. 1. september 2013.		
12-053 04 **Prioritet 1**	<u>Manglende brug af skærmlås</u> Intern Revision har observeret, at SKATs medarbejdere kun i et vist omfang benytter skærmlåsen - når pc'en forlades. Retningslinjerne foreskriver at: "når it-arbejdspladsen forlades, selv for en kortere periode, skal der logges af samtlige systemer eller anvende Windows' password-beskyttede skærmlås, for at undgå misbrug af brugerens rettigheder". **Status 2014:** Vi har set dokumentation for, at Group Policy for "Screen saver timeout" er sat til 900 sekunder (15 min). Dermed aktiveres pauseskærmen automatisk for alle klienter i AD efter 15 min. **Vi anser punktet for lukket**	Manglende brug af skærmlås betyder at en medarbejder kan anvende en anden medarbejders pc og adgange. Konsekvensen heraf kan være at funktionsadskillelsen ikke kan opretholdes. Desuden vil det ikke være muligt entydigt at bestemme, hvem der f.eks. har tilgået et fortroligt dokument.	Intern Revision anbefaler, at SKAT overvejer at gennemføre en oplysningskampagne som overfor SKATs personale, ledere såvel som menige medarbejdere, indskærper: • At vi skal benytte skærmlås når pc'en forlades selv for en kortere periode. • At lokale PC ér generelt opsættes til aflåsning efter 15 minutters ikke anvendelse.
	SKATs kommentar i 2013: Emnet har været et punkt i flere af de kampagner som Kontoret for Informations-sikkerhed har afviklet de senere år, og emnet indgik bl.a. i konkurrencen op til jul 2012. Senest har Kontoret for Informationssikkerhed indarbejdet det i de mussemåtter som er udleveret til samtlige medarbejdere. Emnet vil også ved fremtidig kampagner indgå i overvejelserne. Ved leveringen af PC´er er de alle sat op med automatisk skærmlåsning efter 15 minutter. Opsætningen kan ikke ændres af den enkelte medarbejder, så anbefalingen er således allerede efterlevet.		

Nr.	Observationer	Risici	Anbefalinger
12-053 05 **Prioritet 1**	<u>Manglende synlig identifikation</u> Intern Revision har observeret, at det ikke på alle lokationer er obligatorisk at bære personligt legimitationskort synligt. **Status 2014:** I forbindelse med, at alle ansatte i SKAT fik nye ID-kort primo januar 2014, blev princippet om synlig ID udbredt til alle i SKAT. Sammen med det nye kort blev der udleveret et infobrev, hvoraf det fremgik, at det nye ID kort skal bæres synligt hele tiden, når man er på arbejde. **Vi anser punktet for lukket.**	Manglende synlig identifikation øger risikoen for at udefrakommende kan få adgang til SKATs lokationer, og dermed fortrolige informationer.	Intern Revision anbefaler, at: • SKAT gennemgår retningslinjer for personlig identifikation og sikrer at det fremgår at alle medarbejdere skal bære synlig identifikation når de opholder sig på SKATs lokationer. • SKAT overvejer at gennemføre en oplysningskampagne som overfor SKATs personale, ledere såvel som menige medarbejdere, indskærper reglerne.
	SKATs kommentar i 2013: I forlængelse af bl.a. drøftelser i Hovedarbejdsmiljøudvalget er Sikkerhed og Miljø, i samarbejde med Kontoret for Informationssikkerhed, ved at udarbejde en indstilling om dette til Direktionen.		
12-053 06 **Prioritet 3**	<u>Mobile container scannere</u> SKAT har erhvervet 2 mobile scannere til scanning af 20" og 40" containere. Scannerne repræsenterer en betydelig værdi. Intern Revision har fået oplyst, at Scannerteamet fra politiet er gjort opmærksom på at kriminelle i aflyttede telefonsamtaler har drøftet mulighederne for at sabotere container scannerne. Intern Revision har fået oplyst, at container scannerne i enkelte tilfælde har været parkeret på hotel parkering i forbindelse med opgaver - der har varet flere dage. **Status 2014:** SIR har fået oplyst, at som udgangspunkt parkeres scanneren på SKAT lokaliteter i aflåste garager. Scanneren parkeres aldrig på raste-	Hvis container scannerne parkeres på offentligt område øges risikoen for hærværk. Hvis kriminelle er opmærksomme på eksistensen af container scannerne og ydermere opfatter disse som en trussel, øges risikoen for hærværk betragteligt.	Intern Revision anbefaler, at SKAT til stadighed vurderer trusselsbilledet og implementerer fornødne forholdsregler, dels for at beskytte udstyret, men også i særdeleshed for at beskytte medarbejderne. Intern Revision anbefaler desuden, at SKAT overvejer at indføre retningslinjer, der sikrer, at container scannerne ikke parkeres på offentligt område uden opsyn.

Nr.	Observationer	Risici	Anbefalinger
	pladser eller andre offentlige områder. Hvis der undtagelsesvis ikke er mulighed for at få scanneren parkeret indenfor et aflukket område i forbindelse med hotelovernatning, bliver scanneren parkeret på en oplyst parkeringsplads på hotellets område. I de situationer, hvor scanneren bliver parkeret på en hotelparkering, vil scannerteamet altid kontakte funktionslederen for en konkret vurdering af trusselsbilledet. SIR finder dette tilfredsstillende og lukker anbefalingen. **Vi anser punktet for lukket.**		
	SKATs kommentar i 2013: Temaet vil indgå i de løbende arbejdsmiljø- og sikkerhedsdrøftelser som Sikkerhed og Miljø har med toldledelsen. Forud for denne drøftelse vil Sikkerhed og Miljø sammen med de ansvarlige funktionsledere få konkretiseret og kvalificeret risikobilledet.		
12-053 07 **Prioritet 2**	<u>Adgang via kantine</u> På adressen Østhavnsvej observerede Intern Revision, at kantinefaciliteter og et enkelt mødelokale blev delt med Veterinærstyrelsen. Adgang til kantinefaciliteter og mødelokalet er ikke beskyttet af adgangskontrol, hvilket betyder, at Veterinærstyrelsens medarbejdere har adgang til SKATs lokaler gennem kantinen. Intern Revision har fået oplyst, at SKAT har valgt at det skal være sådan. Dette skal ses i lyset af, at SKAT samarbejder med Veterinærstyrelsen i hverdagen. **Status 2014:** Vi har fået oplyst, sikringen af SKATs lokaler er genetableret, således at Veterinærstyrelsen medarbejdere ikke længere på egen hånd kan færdes i SKATs lokaler.	Den valgte løsning gør det muligt for Veterinærstyrelsens medarbejdere at tilgå SKATs lokaler på lokationen. Den valgte løsning betyder, at den fysiske sikkerhed hos SKAT til dels er afhængig af Veterinærstyrelsens fysiske sikkerhed. Dette øger risikoen for uautoriseret adgang til dokumenter, systemer og data.	Intern Revision anbefaler, at SKAT genovervejer om man ønsker at leve med den påpegede risiko.

Nr.	Observationer	Risici	Anbefalinger
	Vi anser punktet for lukket		
	SKATs kommentar i 2013: Sikkerhed og Miljø vil sammen med Service Herning få sikringen retableret således at denne adgang ikke længere er mulig. Forinden vil vi via drøftelser med funktionslederne på adressen skabe forståelse for de hensyn som ligger bag.		
12-053 08 **Prioritet 2**	<u>Adgang til kontorområder for borgere</u> På adressen Sluseholmen observerede Intern Revision, at borgere gennem receptionsområderne i åbningstiden har adgang til dele af kontorområderne. Områder borgerne ikke må tilgå er tydeligt markeret med et "Indkørsel forbudt" skilt. Lokationen har en gruppe vagtpersonale som altid kan tilkaldes i åbningstiden, hvilket selvfølgelig har en vis formildende virkning. Dørene er desuden en del af de officielle flugtveje. **Status 2014:** Vi har den ¼-2014 gennemgået den fysiske sikkerhed i stueetagen og i kælder på Sluseholmen, og konstateret at døren indtil kontorområdet ved receptionen holdes åben. Det er endvidere oplyst, at der altid er mere en tre ansatte i området og borgerne skal forbi receptionen med vagt for at få adgang til lokalet.	Den valgte løsning gør det muligt for borgerne at tilgå dele af SKATs lokaler på lokationen. Dette øger risikoen for uautoriseret adgang til dokumenter, systemer og data. Der er endvidere en øget risiko for, at en person uden lovligt ærinde kan tilgå lokaler med henblik på at finde en bestemt medarbejder.	Intern Revision anbefaler, at SKAT genovervejer, om SKAT ønsker at acceptere den påpegede risiko.

Nr.	Observationer	Risici	Anbefalinger
	Vi anser punktet for lukket		
	SKATs kommentar i 2013: I henhold til sikringsnotatet skal en sådan sikring gennemføres, og dette vil derfor indgå i risikovurderingerne i forlængelse af de ændringer der er en konsekvens af lukningen af nummerpladeekspeditionen samt flytningerne i forbindelse med de igangværende organisationsændringer. Foreligger der på dette tidspunkt en tidsplan for den forventede lukning af SKATs kundeekspeditionerne vil dette indgå i vurderingerne.		
12-05309 **Prioritet 2**	<u>Meget trangt lokale</u> Intern Revision har observeret, at SKATs kontrolarbejde i Københavns lufthavn, i forbindelse med sikkerhedskontrollens mistanke om forsøg på at udbringe store kontantmængder eller lignende, foregår under meget trange forhold. Kontrollerne foregår i et meget lille rum (ca. 1,2m * 4m) uden udluftning eller vinduer. Ofte vil der være 2 Toldere, 1 Securitas, 2 Politifolk i rummet foruden den eller de rejsende. Der er ingen undvige- eller flugtmuligheder, hvis der skulle opstå en tilspidset situation. **Status 2014:** SIR har i 2014 set på lokaleforholdene, og vurderet at disse forhold nu er i orden. **Vi anser punktet for lukket.**	Der er ingen undvige- eller flugt-muligheder, hvis der skulle opstå en tilspidset situation. Intern Revision er ikke bekendt med arbejdsmiljølovgivningen på området, men må påpege at der er en risiko for at arbejdsforholdene ikke lever op til arbejdsmiljølovgivningen på området.	Intern Revision anbefaler, at • SKAT undersøger om arbejdsmiljølovgivningen på området er formelt overholdt i de beskrevne situationer • SKAT overvejer om arbejdsforholdene, ud fra en medarbejder sikkerhedssynsvinkel, er sikkerhedsmæssigt i overensstemmelse med SKATs retningslinjer og ønsker.
	SKATs kommentar i 2013: Sikkerhedsforholdene følger ikke de retningslinjer SKAT normalt anvender, men i den givne situation er det dog en formildende omstændighed at		

Nr.	Observationer	Risici	Anbefalinger
	såvel CPH Security som Politiet deltager. Spørgsmålet har gentagne gange været drøftet med CPH som har afslået ændringer med henvisning til at formålet med lokalerne er et andet samt at de fysiske rammer ikke giver mulighed for ændringer. Under besøget tog afdelingslederen problematikken op med sikkerhedschefen som kunne konstatere at anvendelsen er i strid med arbejdsmiljølovgivningen. Sikkerhedschefen henviste til at opgaven måttet løses i SKATs lokaler ved rød/grøn sluse, og hvor faciliteterne er til det – security/politiet må følge passageren. Arbejdstilsynets besøg i Lufthavnen har givet anledning til kommentarer fra dem.		
12-053 10 **Prioritet 2**	<u>Nøglefortegnelse - NEG</u> Intern Revision har på lokationen NEG observeret, at nøglefortegnelsen ikke er fyldestgørende samt at adskillige adgangskort er udstedt og udleveret uden at registrere indehaveren. **Status 2014:** Vi har fået oplyst, at der ikke længere udleveres nøgler til medarbejderne, hvorfor en egentlig nøglefortegnelse nu er mindre relevant. Samtidig har vi kendskab til, at der er sket udskiftning af de gamle kort som alle blev lukket og nye kort er udleveret mod behørig underskrift. **Vi anser punktet for lukket.**	Manglende kontrol med adgangs-nøgler og adgangskort øger risikoen for uautoriseret adgang til lokationen. Dette øger risikoen for uautoriseret adgang til SKATs dokumenter, systemer og data. Desuden øges risikoen for, at en udefrakommende kan henvende sig direkte til ministeren eller medarbejdere i Skatteministeriet uden lovligt forehavende.	Intern Revision anbefaler, at • SKAT etablerer en nøglefortegnelse der redegør for alle væsentlige nøgler. • hvis SKAT ikke kan redegøre for alle væsentlige nøgler, da overvejer at udskifte centrale låse og derigennem danner grundlag for etablering af en fuldstændig nøglefortegnelse. • SKAT sikrer at alle udstedte adgangskort er registreret med korrekt indehaver. Kort uden korrekt indehaver bør lukkes. • SKAT sikrer at alle kort som ikke er anvendt i en længere periode, f.eks. 2 måneder, automatisk bliver lukket.
	SKATs kommentar i 2013: I forbindelse med den gennemførte fysiske opdeling mellem Departementet og SKAT blev der pr. 1. januar 2013 gennemført en række ændringer, herunder lukning af alle gamle kort samt visse ændringer i forhold til anvendelse af nøgler. Herudover er der drøftelser i gang med ATP Ejendomme og Mærsk om sikkerhedsniveauet omkring bygningen. Temaet vil indgå i den tidligere nævnte opfølgning og sikkerhedsvurdering som gennemføres af Sikkerhed og Miljø efter sommerferien.		
12-053 11 **Prioritet 2**	<u>Passwordlister – AIX</u> Intern Revision har på lokationen IT-Center Høje Tåstrup observeret en række papkasser med påtegningen ”passwordlister” opbevaret i aflåst serverrum. En nærmere undersøgelse viste, at der er tale om output fra en intern kontrol (et AIX script),	De udskrevne krypterede passwords kan dekrypteres ved brug af forskellige hacker værktøjer, og derigennem give adgang til administration af AIX miljøet. Det må således forudsættes, at kun personer, der i forvejen er bekendte med disse passwords har adgang til udskrifterne.	Intern Revision anbefaler, at • SKAT sikrer at kun personer der i forvejen er bekendte med disse passwords har adgang til udskrifterne. • Dette gælder både gamle og nye udskrifter. Som følge heraf kan udskrifterne ikke udskrives på printer hvortil andre end

Nr.	Observationer	Risici	Anbefalinger
	dokumenteret i EDB-Håndbog – Drift og Sikkerhed – afsnit 3-3-1-7. Kontrollen udføres automatisk hver måned og udskrives til prædefineret printer. Output skal efter vejledningen opbevares i 3 år. Output fra kontrollen indeholder bl.a. de krypterede password fra centrale konti i AIX miljøet. Output udskrives i dag til It-Center Haderslev. **Status 2014:** Vi har fået oplyst, at bruger dokumentation fra AIX-miljøet, ikke længere udskrives på papir efter aftale med Informationssikkerhed. **Vi anser punktet for lukket.**	Krypterede password på gamle udskrifter burde blive forældede, idet passwords kræves skiftet hver 90 dage. Dette sker dog ikke konsekvent for systemkonti.	personer der i forvejen er bekendte med disse passwords har adgang. • SKAT overvejer, om det er nødvendigt at udskrive det krypterede password, eller om denne værdi kunne erstattes af noget andet, for derigennem at øge sikkerheden. • Af sikkerhedsmæssige årsager bør password ikke ned- eller udskrives. • SKAT overvejer, om kontrollen kunne gennemføres uden at output udskrives.
	SKATs kommentar i 2013: Listerne udskrives i Haderslev, hvor den anvendte printer står i et aflåst serverrum med alarmsikret adgangskontrol, og hvor kun en begrænset personkreds har adgang. Printeren anvendes kun til formål som relaterer sig til overvågning af servernes og TP systemernes drift. De udskrevne lister opbevares i samme serverrum. En procedureændring er under overvejelse, således at der ikke længere skal udskrives lister men at kontrollen foretages online. Dette sker i dialog med Kontoret for Informationssikkerhed.		
12-053 12 **Prioritet 3**	<u>Interne kontrolpunkter</u> Intern Revision har observeret, at SKAT kun i begrænset omfang udfører det obligatoriske interne kontrolpunkt - S44501000000 - adgang til netværk og krydsfelter. **Status 2014:** Vi har i 2014 deltaget i Koncerncervices sikkerhedsrundering på lokaliteterne SC Korsør og SC Køge. Begge steder holdes serverrum og krydsfelter låste. Det er vores vurdering, at kontrolpunktet nu udføres som forventet, og at der er fokus på sikkerheden på området. **Vi anser punktet for lukket.**	Manglende gennemførelse af de interne kontroller omkring adgang til netværk og krydsfelter, øger risikoen for at opståede fejl (f.eks. manglende aflåsning) ikke opdages.	Intern Revision anbefaler, at det interne kontrolpunkt udføres som forudsat.

Nr.	Observationer	Risici	Anbefalinger
	SKATs kommentar i 2013: Sikkerhed og Miljø tager initiativ til en nærmere undersøgelse af baggrunden for Intern Revisions observationer, med henblik på at det fremover indgår og udføres korrekt.		
12-053 13 **Prioritet 3**	Brandbart materiale i serverrum På adressen Lyseng Allé observerede Intern Revision, at der i serverrummet fandtes en del pap og flamingo. **Status 2014:** Vi har ved deltagelse i sikkerhedsrunderingen den 2. maj i Korsør og Køge konstateret, at kontrollen fungerer, og at der er sket oprydning i serverrum. **Vi anser punktet for lukket.**	Brandbart materiale øger konsekvensen ved en brand og i et vist omfang også risikoen for brand i det hele taget. Brandbart materiale bør ikke findes i større mængder i serverrum.	Intern Revision anbefaler, at SKAT foretager en oprydning i serverrummet.
	SKATs kommentar i 2013: umiddelbar forlængelse af Intern Revisions besøg blev forholdene bragt i orden. Er bekræftet ved besigtigelse 7. februar 2013. Vil indgå i den kommende sikkerhedsrundering på alle lokaliteter.		
12-053 14 **Prioritet 3**	Printserver direkte på gulv På 2 adresser, Lyseng Allé og Sluseholmen, observerede Intern Revision, at printserverne stod direkte på gulvet. **Status 2014:** Vi har ved deltagelse i sikkerhedsrunderingen den 2. maj i Korsør og Køge konstateret, at runderingen opfylder kravet til kontrol, og at printserverne ikke længer står direkte på gulvet. **Vi anser punktet for lukket.**	Kritisk udstyr bør af flere årsager ikke stå direkte på gulvet: • Står udstyr direkte på gulvet øges risikoen for at selv mindre vandskader eller oversvømmelser vil kunne ødelægge og / eller kortslutte udstyr. • Står udstyr direkte på gulvet øges risikoen for at medarbejdere kommer til f.eks. at sparke til udstyret og at det deraf tager skade.	Intern Revision anbefaler, at kritisk udstyr placeres mindst 10 cm over gulvhøjde.
	SKATs kommentar i 2013: I umiddelbar forlængelse af Intern Revisions besøg blev forholdene bragt i orden. Er bekræftet på Lyseng Allé ved besigtigelse 7. februar 2013. Vil indgå i den kommende sikkerhedsrundering på alle lokaliteter.		
12-053	Åben nødudgang udefra	Nødudgangen gav direkte adgang til SKATs lokati-	Intern Revision opfatter denne hændelse

Nr.	Observationer	Risici	Anbefalinger
15 **Prioritet 3**	På adressen Lyseng Allé observerede Intern Revision en afsides nødudgang, som ikke var behørig låst udefra. Udgangen havde været benyttet af håndværkere som tilsyneladende havde glemt at låse efter sig. Intern Revision kontrollerede den efterfølgende dag, at døren var behørig aflåst, hvilket den var. **Status 2014:** Vi har deltaget i sikkerhedsrunderingen den 2. maj i Korsør og Køge konstateret, at alle nødudgange var behørigt aflåste. **Vi anser punktet for lukket.**	on. Dette øger risikoen for uautoriseret adgang til dokumenter, systemer og data. Desuden øges risikoen for tyveri.	som en enlig hændelse og har ingen anbefalinger i den anledning.
	SKATs kommentar i 2013: Nødudgang konstateret aflåst og med tydelig forbud mod åbning ved besøg på lokaliteten den 7. februar 2013.		
12-053 16 **Prioritet 3**	<u>Mangelfulde revisorerklæringer</u> En gennemgang af modtagne revisorerklæringer vedrørende vore hostingpartnere har vist, at disse er meget overordnede og ikke i detaljer underbygger, at den fysiske sikkerhed er betryggende på vore hostingpartneres lokationer. **Status 2014:** SIR er bekendt med SKATs vurdering og holdning til modtaget revisorerklæringer. Risikoen og anbefalingen vil blive stilet til anden enhed i SKAT, hvorfor vi betragter denne anbefaling for lukket. **Vi anser punktet for lukket.**	Det betyder formelt, at Intern Revision egenhændigt bør revidere den fysiske sikkerhed hos vore hostingpartnere. Dette er ikke i praksis muligt. Intern Revision må lægge til grund at SKATs hostingpartnere er anerkendte virksomheder som naturligt har en betryggende fysisk sikkerhed.	Intern Revision anbefaler, at SKAT, overfor SKATs hosting partnere, insisterer på at få mere fyldestgørende og specifik revisorerklæringer.
	SKATs kommentar i 2013: Hvorvidt SKAT skulle kræve mere fyldestgørende revisorerklæringer har tidligere været drøftet og forelagt Direktionen. Konklusionen blev dengang at vi anvender den form for erklæringer som SKAT kræver i dag.		
12-053	<u>Adgangskort – fratrådte medarbejdere</u>	Adgangskort, der benyttes af ældre adgangssy-	Intern Revision anbefaler, at

Nr.	Observationer	Risici	Anbefalinger
17 **Prioritet 2**	Intern Revision har på flere lokationer (Lyseng Alle, Sluseholmen og Nicolai Eigtveds Gade) observeret, at der eksisterer aktive adgangskort som har tilhørt tidligere medarbejdere. Efter det oplyste er disse fysisk inddraget i forbindelse med at vedkommende ansættelsesforhold er bragt til ophør. **Status 2014:** SIR har fået oplyst, at når en medarbejder ophører (afsked/tjenestefrihed), får personalelederen en meddelelse fra Koncernservice, Personale om, hvad han/hun skal sørge for i forbindelse med at medarbejderen fratræder. Af denne info fremgår det bl.a., at han/hun skal sikre, at nøgle/adgangskort bliver inddraget og afleveret til Koncernservice, Serviceenheden. Som supplement til denne procedure er der nu indført en proces, hvor Servicechefen får en orientering direkte fra sagsbehandleren i Koncernservice, Personale om at en medarbejder stopper pr. xx.xx. SIR har modtaget kopi af arbejdsgangsbeskrivelser, hvoraf det fremgår at Servicechefen skal orienteres med henblik på indsamling af adgangskort. **Vi anser punktet for lukket.**	stemer, baseret på enten magnetstribe eller RFID, kan nemt kopieres. For argumentets skyld fandt vi en RFID Card Copier på Internettet til $35,99, en kortlæser/skriver til magnetstribekort kan fås i samme prisniveau. For god ordens skyld skal vi oplyse at Intern Revision ikke har testet ovenstående mod SKATs adgangssystemer. En forretningsgang, hvor virksomheden indsamler adgangskort når medarbejderen stopper, og en gang imellem eller slet ikke lukker disse kort, øger risikoen for at en medarbejder kopier sit kort før vedkommende afleverer originalen.	• SKAT etablerer en fratrædelsesproces hvorefter adgangskort inaktiveres straks når medarbejderen fratræder, uanset om adgangskortet er inddraget eller ikke. • SKAT sikrer, at alle kort som ikke er anvendt i en længere periode, f.eks. 2 måneder, automatisk bliver lukket. • SKAT gennemfører en kontrol med allerede udstedte adgangskort og sikrer at aktive kort tilhører ansatte medarbejdere eller andre med legitim adgang til den enkelte lokation. Intern Revision er bekendt med, at SKAT overvejer at anskaffe nyt adgangskontrol system. SKAT bør i den forbindelse medtage disse overvejelser.
	SKATs kommentar i 2013: Muligheden for maskinelle udtræk undersøges som supplement til den i Serviceboksen beskrevne procedure, hvor den enkelte afdelingsleder/kontorchef har ansvaret for at informere Servicechefen om medarbejderes ophør. Koncernservice er bekendt med at proceduren ikke efterleves til fulde, og det har ikke været muligt for servicecheferne at sikre det 100 %, specielt svært i situationen hvor medarbejdere fra andre lokaliteter qua hyppig gang på lokaliteten har fået udstedt adgangskort.		
12-053	Adgangskort	Indehaver af et givet adgangskort skal entydigt	Intern Revision anbefaler, at SKAT overvejer

Nr.	Observationer	Risici	Anbefalinger
18 **Prioritet 3**	Intern Revision har observeret, at ikke alle adgangskortsystemer gør det muligt entydigt at identificere den enkelte medarbejder, på enten CPR-nr. eller medarbejdernr. For de lokationer, der har været omfattet af nærværende revision drejer det sig om Nicolai Eigtveds gade og Helgeshøj Alle. **Status 2014:** SIR har modtaget fortegnelse over udleverede lånekort og har kendskab til, at der er anskaffet et nyt adgangskontrolsystem i SKAT, hvor den enkelte medarbejder entydigt identificeres. **Vi anser punktet for lukket.**	kunne identificeres, således at der ikke opstår fejl hvis et kort f.eks. lukkes eller skal tildeles yderligere autorisationer. Dette forhold er ydermere en forudsætning for implementering af straks lukning af kort for fratrådte medarbejdere.	at registrere alle kortsystemer med en entydig identifikation. Intern Revision er bekendt, med at SKAT overvejer at anskaffe nyt adgangskontrol system. SKAT bør i den forbindelse medtage disse overvejelser.
	SKATs kommentar i 2013: Temaet vil indgå som et element i Sikkerhed og Miljøs opfølgning og sikkerhedsrundering.		
12-053 19 **Prioritet 3**	<u>Nøglefortegnelse – Sluseholmen</u> Intern Revision har observeret, at nøglelisten fra Sluseholmen indeholder fratrådte medarbejdere, uden at man af listen kan se at nøglen er inddraget. Efter det oplyste er disse fysisk inddraget i forbindelse med at vedkommende er stoppet. **Status 2014:** Vi har modtaget en opdateret nøglefortegnelse, samt information om, at låsesystemet er udskiftet i marts 2014. Vi har ved en fysisk gennemgang af alle eksterne ind- og udgange konstateret, at låse er skiftet til det nye system. Der mangler dog fortsat en cylinder i en nødudgang i kælderen. SKAT har orienteret os om, at dette vil ske i løbet af en uge. **Vi anser punktet for lukket.**	For til stadighed at have overblik over hvor mange nøgler der er indkøbt og hvem der har fået disse udleveret er det vigtigt at nøgleoversigter bliver løbende ajourførte.	Intern Revision anbefaler, at SKAT for Sluseholmen gennemfører en ajourføring af nøgleoversigten.

Nr.	Observationer	Risici	Anbefalinger
	SKATs kommentar i 2013: Opfølgningen og ajourføringen er gennemført, men endvidere vil temaet vil indgå i Sikkerhed og Miljøs opfølgning og sikkerhedsrundering.		

Bilag 2: Anvendt skala

Ved vurderingen i konklusionen er følgende skala anvendt:	
Meget tilfredsstillende	Intern Revision har ikke konstateret svagheder i de forretningsgange og processer, der understøtter det reviderede område. Samtlige observationer kan henføres til prioritet 3. Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer Prioritet 3: Samtlige observationer
Tilfredsstillende	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 3. Enkelte observationer med prioritet 2 kan dog forekomme. Samlet set udgør de implementerede forretningsgange et "tilfredsstillende" grundlag for administration af området. Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer Prioritet 3: Hovedparten af observationer
Ikke helt tilfredsstillende	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 2 eller 3 med hovedvægten på prioritet 2. Enkelte observationer i prioritet 1 kan dog forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør "et ikke helt tilfredsstillende" grundlag for administration af området. Der er som følge heraf en forøget risiko for: • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" Prioritet 1: Enkelte observationer Prioritet 2: Hovedparten af observationer Prioritet 3: Et mindre antal observationer
Ikke tilfredsstillende	Intern Revision har observeret flere væsentlige svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 1 eller 2 med hovedvægten på prioritet 1. Enkelte observationer i prioritet 3 kan forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør et "ikke tilfredsstillende grundlag" for administration af området. Der er som følge heraf en væsentlig forøget risiko for: • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" • Manglende realisering af forretningsmålene for det reviderede område. Prioritet 1: Hovedparten af observationer Prioritet 2: Et mindre antal observationer Prioritet 3: Enkelte observationer

Prioritet skal ses i forhold til det reviderede område og er defineret således:

1. ***Kritisk for forretningen:*** Væsentlig svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er en væsentlig forøget risiko for, at processens målopfyldelse ikke realiseres som følge af den konstaterede svaghed. Der bør straks iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

2. ***Væsentlig for forretningen:*** Svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er forøget risiko for, at processens målopfyldelse ikke realiseres i fuldt omfang som følge af den konstaterede svaghed. Der bør iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

3. ***Mindre betydning for forretningen:*** Ingen væsentlige svagheder i de etablerede forretningsgange/processer. Det er dog muligt at designe de enkelte processer på en mere hensigtsmæssig måde, således at eksekveringen forbedres.

Observationer, som vi har lukket i denne revision, er markeret med ”Grå”.