Sammendrag

Følgende er en sammenfatning af de sikkerhedskrav, som fremgår af dokumentet ”Sammenfatning”. Krav fra ISO/IEC 27002 er ikke medtaget her, da de er almindelig kendte. Desuden er der sat yderligere krav ind fra egne risikovurderinger.

Alle sikkerhedskrav bør tage højde for opdelingen av sikrningsniveauer i henhold til Europa-Parlamentets og Rådets forordning 910/2014 – Artikel 8, hvor niveauerne opdeles i **»lav«**, **»betydelig«** og **»høj«** efter følgende metode:

1. En elektronisk identifikationsordning, der er anmeldt i henhold til artikel 9, stk. 1, skal angive sikringsniveauerne »lav«, »betydelig« og/eller »høj« for de elektroniske identifikationsmidler, der er udstedt under den pågældende ordning.

2. Sikringsniveauerne **»lav«**, **»betydelig«** og **»høj«** skal opfylde følgende kriterier:

    a. sikringsniveauet **»lav«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en begrænset grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

    b. sikringsniveauet **»betydelig«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en middelstor grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

    c. sikringsniveauet **»høj«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der giver en højere grad af tillid til en persons påståede identitet end elektroniske identifikationsmidler med sikringsniveauet »betydelig«, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten.

Sikkerhedskravene er opdelt efter strukturen i ISO/IEC 27002.

5 Informationssikkerhedspolitikker

Følgende EU-regler skal tilgodeses:

- Beskyttelse af datasikkerhed og fortrolighed i forbindelse med dataudveksling og vedligeholdelse af dataintegritet mellem knudepunkterne sikres ved hjælp af de bedste tilgængelige tekniske løsninger og beskyttelsespraksis.
- Knudepunkterne lagrer ingen personlige data med undtagelse af dem, der er nødvendige til det i artikel 9, stk. 3, beskrevne formal.
- Der skal tages stilling til, hvilke krav i ISO/IEC 27002 man vil følge og begrunde de, man evt. vælger fra.

Informationssikring og sikkerhedsstandarder (OCES)

- Det skal dokumenteres, at virksomheden opfylder kravene i standarden ISO/IEC 27001

Følgende regler bør overvejes (OCES):

- Der skal tages stilling til behov for en sertificeringspraksis (a la OCES 7.1)

6 Organisering af informationssikkerhed

Følgende regler bør implementeres (OCES):

- Der skal foreligge politikker og procedurer for håndtering af kundehenvendelser eller henvendelser fra signaturmodtagere.
- Der skal foreligge skriftlige aftaler med alle underleverandører af CA- tjenester.
- CA skal til enhver tid have tilstrækkelig med uddannet personale til at kunne drive alle udbudte tjenester på forsvarlig vis. Personalet skal til enhver tid have den kompetence, der foreskrives for de enkelte definerede betroede funktioner.
- CA skal sikre, at der foreligger skriftlige aftaler med alle underleverandører af CA- tjenester.

Nøglepersoner (fra risikovurdering)

- Der bør undgås, at der opstår nøglepersonsafhængighed

7 HR sikkerhed

Før ansættelse (OCES)

- Der skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv. Dette er ligeledes gældende for RA medarbejdere og medarbejdere hos leverandører til kritiske ydelser.

Under ansættelsesforløbet (EU)

- Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede og erfarne inden for de færdigheder, der er behov for, når de skal udfylde deres roller.
- Der skal være tilstrækkeligt med personale og underleverandører til at drive og vedligeholde tjenesten i henhold til de relevante politikker og procedurer.

Ved ansættelsens ophør eller ved ændrede arbejdsområder (God skik)

- Der bør vises en vis interesse for den forhenværende medarbejder med hensyn til dennes overholdelse af tavshedspligten efter ansættelsens ophør

Faciliteter og personale (EU)

Overholdelsen af kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende sikringsniveau.

- Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede og erfarne inden for de færdigheder, der er behov for, når de skal udfylde deres roller.
- Der skal være tilstrækkeligt med personale og underleverandører til at drive og vedligeholde tjenesten i henhold til de relevante politikker og procedurer.

Borgenes sikkerhedsbevidsthed (egen risikovurdering)

- Det skal sikres, at borgerne oplyses om betydningen af at overholde grundlæggende sikkerhedsforskrifter.

8 Håndtering af aktiver

Bortskaffelse af medier (NIST)

Medier bør bortskaffes på sikker vis og efter formelle procedurer, når disse ikke længere anvendes

- Før bortskaffelse skal alle medier opføres i en godkendt oversigt
- Bortskaffelsen skal ske i følge en formel procedure
- Medierne skal som minimum ødelægges ved sammenpresning i en dertil godkendt matrice, med en vægt på flere tons
  Der bør overvejes at anskaffe udstyr til at pulverisere medierne

9 Adgangskontrol

Krav til systemer (OCES)

CA skal tilvejebringe RA systemer, som sikrer, at det kun er bemyndigede medarbejdere hos RA, der har adgang til at betjene disse

Administration (egen risikovurdering)

Administration bør i mest muligt omfang udføres lokalt på de respektive maskiner og enheder og i mindst muligt omfang via fjernadgang.

10 Kryptering

Følgende EU-regler bør implementeres (detaljerede krav fremgår af forordningen):

- Krav til kvalificerede tillidstjenesteudbydere (detaljerede krav)
- Kravene til avancerede elektroniske signaturer
- Kvalificerede certifikater for elektroniske signaturer

Nøgleadministration (EU + OCES)

Virksomheden skal anvende udførlige, skriftlige procedurer, som skal leve op til EU-krav, for:

- Nøglehåndtering
  - Håndtering af kryptografiske moduler
  - Nøglehandtering leveret af CA
  - Nøglegenerering
- Certifikathåndtering
  - Udstedelse af certifikat og generering af certifikatindehavers nøgler
  - Certifikatfornyelse
  - Certfikatgenerering
  - Publicering af certifikater
  - Certifikatspærring
- Opbygningen af certifikat skal opfylde EU-krav

- Stjålne eller bortkomne mobiltelefoner / nøglekort (egen risikovurdering)

- Der skal udarbejders og implementeres procedurer for håndtering af bortblevne mobiltelefoner og nøglekort. Der skal også tages stilling til, hvem der er ansvarlig for mulige økonomiske tab i den forbindelse.

Krav til kvalificerede elektroniske signaturgenereringssystemer (EU)

Systemer til generering av kvalificerede elektroniske signaturer skal følge kravene i Europa-Parlamentets og Rådets forordning 910/2014. Disse er opsummeret her i punktform.

- Kvalificerede elektroniske signaturgenereringssystemer skal opfylde kravene i bilag II.
- Krav til certificering af kvalificerede signaturgenereringssystemer
- Krav til validering af kvalificerede elektroniske signaturer
- Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer
- Krav til kvalificerede elektroniske tidsstempler

Tilmelding (EU)

Procedurerne for tilmelding bør følge kravene i Europa-Parlamentets og Rådets gennemførelsesforordning 1502/2015. Disse krav, som i forordningen er opdelt i **»lav«**, **»betydelig«** og **»høj«**, er opsummeret her i punktform.

- Ansøgning og registrering
  - Godtgørelse og kontrol af identitet (fysiske personer)
  - Godtgørelse og kontrol af identitet (juridiske personer)
  - Forbindelser mellem elektroniske identifikationsmidler for fysiske og juridiske personer
- Håndtering af elektroniske identifikationsmidler
  - Elektroniske identifikationsmidler — egenskaber og udformning
  - Udstedelse, levering og aktivering
  - Suspendering, tilbagekaldelse og reaktivering
  - Fornyelse og erstatning
- Autentifikation
  - Autentifikationsmekanismen
- Håndtering og organisering
  - Generelle bestemmelser
  - Forvaltning af informationsikkerhed
  - Registerføring
  - Faciliteter og personale
  - Tekniske kontroller

11 Fysisk og miljømæssig sikkerhed

Sikre områder

Følgende EU-krav bør implementeres:

- Faciliteter kontrolleres løbende for og beskyttes mod skader forårsaget af miljøhændelser, uautoriseret adgang og andre faktorer, som kan påvirke tjenestens sikkerhed.
- Faciliteter sikrer, at adgang til de områder, hvor personlige, kryptografiske og andre følsomme oplysninger opbevares og behandles, er begrænset til autoriseret personale og autoriserede underleverandører.

Følgende OCES-krav bør implementeress:

- CA skal tydeligt beskrive, på hvilke lokaliteter medarbejdere og datacentre i forbindelse med CA's virke er placeret. De lokaler, hvor udstyr til nøglegenerering er placeret, benævnes CA driftslokaler. Alle lokaler, der benyttes til medarbejdere hos CA, skal være defineret som særligt sikkerhedsområde.

- CA driftslokaler
  - CA driftslokalet skal være fysisk adskilt fra CA's øvrige lokaler.

- I tilfælde af evakuering skal CA's driftslokaler kunne fungere med uændret drift via fjernbetjening. Ved fjernbetjening forstås mulighed for f.eks. via en PC at betjene CA-funktionerne fra et fra CA-driften fysisk adskilt lokale, f.eks. hvor CA har etableret reservesystem.

Fysiske adgangskontroller

Følgende krav bør implementeres:

Fysisk adgang (OCES)

- CA skal sikre, at alle lokaler har en perimeterbeskyttelse svarende til DS 471 eller bedre.
- CA skal sikre, at der etableres vagt 24 timer i døgnet.

Krav til fysisk sikkerhed (indbrudssikerhed - DS 471)

- Der skal defineres detaljerede krav til:
- Bygningslayout
- Adgangsveje og stier
- Krav til døre og porte i skallen
- Krav til vinduer og ruder i skallen
- Krav til gitre i skallen
- Vægkonstruktioner
- Tagkonstruktioner
- Etageadskillelse
- Krav til låse- og nøglesystemer
- Krav til adgangskontrolanlæg
- Kriminalpræventiv belysning
- Sammenstillede sikringsforanstaltninger
- Kategorisering af områder
- Fastlæggelse af barrierer

CA-driftslokaler (OCES)

- CA skal sikre, at adgang til og ophold i de centrale driftslokaler videoovervåges.

Ryddelige serverrum (egen risikovurdering)

- Alle serverrum skal holdes ryddelige, og unødvendigt materiale skal ikke forefindes i lokalerne.

12 Sikkerhed vedrørende drift

Driftsprocedurer og pligter

Følgende EU krav bør implementeres:

Tekniske kontroller

- **Lav**
  - Der skal findes rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed og sikrer de behandlede oplysningers fortrolighed, integritet og tilgængelighed.
  - Elektroniske kommunikationskanaler, der bruges til at udveksle personlige eller følsomme oplysninger, beskyttes mod aflytning, manipulation og gengivelse.
  - Adgang til følsomt kryptografisk materiale er, hvis det bruges til at udstede elektroniske identifikationsmidler eller autentifikation, begrænset til de roller og anvendelsesområder, der absolut skal have adgang. Det skal sikres, at den slags materiale aldrig lagres permanent som klartekst.
  - Der er indført procedurer, som garanterer, at sikkerheden bevares over tid, og at der er mulighed for at reagere på ændringer i risikoniveau, sikkerhedshændelser og brud på sikkerheden.

- Alle medier, som indeholder personlige, kryptografiske eller andre følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.

- **Betydelig**
  - Samme niveau som »lav«, samt:
  - Følsomt kryptografisk materiale er, hvis det anvendes til at udstede elektroniske identifikationsmidler eller autentifikation, beskyttet mod manipulation.

- **Høj**
  - Samme niveau som »betydelig«.

Opbevaring af certifikatinformation (OCES)

- CA er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendige for sikker drift af CA i overensstemmelse med denne CP. CA skal desuden sikre, at:
  - alle informationer om registrering, herunder certifikatfornyelser, logges,
  - alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, logges,
  - al information beskyttes mod uretmæssig adgang,
  - alle aktiviteter, der kræver deltagelse af mere end en person, logges,
  - al videoovervågning lagres,
  - der er skriftlige regler for regelmæssig gennemgang af alle logs,
  - alle audit-logs signeres elektronisk og tidsstemples,
  - audit-logs behandles som fortroligt materiale samt
  - der foretages backup af audit-logs med regelmæssige mellemrum.
- CA skal sikre, at back-up-data opbevares i overensstemmelse med EU-krav
- CA skal sikre, at den relevante myndighed informeres om væsentlige uregelmæssigheder i logningsproceduren samt notificeres en gang årlig i alle andre tilfælde.

CA skal sikre, at følgende information arkiveres (**OCES)**

- alle logs
- certifikatanmodninger og tilhørende kommunikation,
- signerede ordrer og skriftlige aftaler,
- certifikatfornyelser samt
- CPS og CP.
- CA skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af tvister, og at alt arkiveret materiale opbevares i mindst løbende kalenderår + 5 år. Dette er også gældende for evt. data fra RA's it-systemer, som er relevante for dokumentation af CA's virke.

- CA og RA skal sikre, at alt materiale i arkiv opbevares i overensstemmelse med kravene i DS 484.

- CA og RA skal sikre, at alt elektronisk arkivmateriale sikkerhedskopieres med regelmæssige mellemrum.

- CA og RA skal sikre, at alt elektronisk arkivmateriale påføres elektronisk tidsstempling på arkiveringstidspunktet. Andet arkivmateriale indføres i en log.

Sikkerhedskopiering

Opbevaring af sikkerhedskopier (egen risikovurdering)

- Sikkerhedskopier bør forefindes i passende generationer tilbage i tid i henhold til en forretningsgang, således at gamle versioner af data kan genskabes.

Logning og overvågning

Logning af anvendelse af Mobil ID (Risikovurdering)

- Anvendelse af Mobil ID logges i en central log. Der skal udarbejdes procedurer for, hvorledes denne log håndteres, arkiveres, gennemgås, hvorledes det sikres, at loggen ikke overskrives, og krav til fysisk og logisk sikkerhed.

Helpdesk **(egen risikovurdering)**

- Der bør være en passende helpdeskfunktion til at varetage kommunikation og brugerservice til borgerne.

13 Sikkerhed vedrørende kommunikation

Datasikkerhed og fortrolighed (**EU**)

- Beskyttelse af datasikkerhed og fortrolighed i forbindelse med dataudveksling og vedligeholdelse af dataintegritet mellem knudepunkterne sikres ved hjælp af de bedste tilgængelige tekniske løsninger og beskyttelsespraksis.
- Knudepunkterne lagrer ingen personlige data med undtagelse af dem, der er nødvendige til det i artikel 9, stk. 3, beskrevne formal.

Dataintegritet og kommunikationens ægthed (**EU**)

- Kommunikation mellem knudepunkter sikrer datas integritet og ægthed, samt at alle anmodninger og svar er ægte og ikke er blevet manipuleret. Med henblik herpå bruger knudepunkterne løsninger, som med succes er blevet anvendt til grænseoverskridende operationer.

Kommunikationens format (**EU**)

- Knudepunkter gør til syntaks brug af fælles beskedformater, der er baseret på standarder, som allerede er blevet anvendt i flere tilfælde mellem medlemsstater, og som har vist sig at virke i et operationelt miljø. Syntaksen giver mulighed for:
  a) korrekt behandling af det minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person
  b) korrekt behandling af det elektroniske identifikationsmiddels sikringsniveau
  c) at skelne mellem offentlige myndigheder og modtagerparter
  d) fleksibilitet til at opfylde kravene til yderligere attributter i forbindelse med identifikation.

Forvaltning af sikkerhedsoplysninger og metadata (**EU**)

- Knudepunktsoperatøren kommunikerer metadata vedrørende knudepunktets forvaltning på en standardiseret måde, hvor de kan behandles af en maskine, og på en sikker og pålidelig måde.
- Som minimum kan de parametre, der er relevante for sikkerheden, indhentes automatisk.
- Knudepunktsoperatøren lagrer data, som i tilfælde af en hændelse giver mulighed for at gendanne beskedudvekslingssekvensen med henblik på at fastslå, hvor og hvordan hændelsen fandt sted. Disse data lagres i den periode, der er angivet i national lovgivning, og består som minimum af følgende elementer:
  a) identifikation af knudepunktet
  b) identifikation af beskeden
  c) dato og tidspunkt for beskeden.

Denial of service (egen risikovurdering)

- Der skal forberedes procedurer for omdirigering af netværkstrafik, såfremt virksomheden bliver udsat for denial of service angreb

Krypteret datakommunikation (egen risikovurdering)

- Der skal anvendes stærk kryptering for datatrafik, som indeholder autenifikeringsoplysninger.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

Udvikling, anskaffelse og vedligeholdelse af it-systemer (OCES)

- CA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer. Produkterne skal overholde en tilstrækkelig beskyttelsesprofil i henhold til ISO/IEC 15408 eller tilsvarende.

- CA skal sikre, at der forud for enhver systemudvikling (dvs. egenudvikling eller udvikling ved tredjemand) foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne.

Systemdokumentation (egen risikovurdering)

- For alle systemer skal der sikres, at der er passende systemdokumentation

15 Leverandørforhold

Kontrol af underleverandører (OCES)

CA skal sikre, at personale hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som CA's egne medarbejdere i de funktioner, underleverandørens personale varetager for CA.

- CA skal ved adgangsprocedurerne sikre, at personale hos underleverandører ikke kan arbejde uovervåget hos CA.

- RA personale skal gennemføre en uddannelse, som sætter dem i stand til at udføre deres arbejde korrekt og sikkert.

16 Styring af sikkerhedshændelser

Sikkerhedskrav til tillidstjenesteudbydere (EU)

- Kvalificerede og ikke kvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser.

- De kvalificerede og ikkekvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, skal hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

- Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

17 Informationssikkerhedsmæssige aspekter ved beredskabsstyring

Beredskabsplanlægning (OCES)

Følgende hændelser skal betragtes som alvorlige:

- kompromittering af CA's private nøgle,
- mistanke om kompromittering af CA's private nøgle,
- nedbrud og kritiske fejl på CA's driftskomponenter (spærrelister etc.) samt
- stop af CA-driftsmiljøet som følge af brand, elforsyningssvigt osv.

CA skal i tilfælde af kompromittering af CA's private nøgle eller mistanke herom straks informere alle certifikatindehavere via den registrerede e-mailadresse. CA skal ligeledes straks informere IT- og Telestyrelsen med en uddybende beskrivelse af den opstående situation.

CA skal ligeledes på sin hjemmeside og i det omfang det vurderes relevant under hensyntagen til den opstående situation, via offentlige medier eller ved direkte kontakt, straks informere signaturmodtagere.

CA skal i tilfælde af alvorlige hændelser på databehandlingsudstyr, programmel og/eller data orientere certifikatindehavere herom i det omfang, det er relevant for deres brug af CA-tjenesterne. Under hensyntagen til den opståede situation, skal signaturmodtagere informeres via offentlige medier og ved annoncering i dagspressen.

CA skal sikre, at alle procedurer med relation til spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange efter et driftsnedbrud.

No-break og generator (egen risikovurdering)

- Systemernes koninuerlige drift skal beskyttes med passende no-break anlæg og dieselgenerator.

18 Overensstemmelse

Overensstemmelse med lovgivningen (OCES)

- CA og RA skal sikre overensstemmelse med lovgivningen, herunder særligt lov om behandling af personoplysninger.

Særlige forpligtelser med henblik på beskyttelse af fortrolig information (OCES)

- Information, som ikke indgår i certifikater og spærrelister, anses som fortrolig. Information, som indgår i certifikater, anses som ikke fortrolig og ikke privat.

- Personrelateret information, som ikke indgår i certifikatet, anses som privat information. CA skal sikre, at en certifikatindehaver har mulighed for at kræve, at navne- og adresseinformation, herunder e-postadresse ikke fremgår af certifikatet (gælder kun personcertifikat). CA og RA skal sikre, at fortrolig information er beskyttet mod kompromittering og må ikke benytte fortrolig information til andet, end hvad der er påkrævet for driften af CA.

- CA og RA skal sikre, at privat information er beskyttet mod kompromittering og må ikke benytte privat information udover, hvad der er påkrævet for drift af CA.

- CA og RA skal sikre, at statistiske oplysninger om anvendelse af OCES- personcertifikater ikke kan henføres til det enkelte OCES-certifikat.

- Kan en tvist ikke løses forligsmæssigt, kan enhver af parterne vælge at indbringe tvisten for de almindelige domstole. Værneting er København. Dansk ret er gældende.

Placering af datacentre (OCES)

- Kravene i denne CP gælder uanset, at CA placerer hele eller dele af driftsmiljøet i udlandet. Den løbende kontrol, der er fastsat i CP'en, skal således kunne gennemføres, uanset hvor CA geografisk er placeret.

18.2 Gennemgang af informationssikkerhed

Systemrevision (OCES)

- Der skal gennemføres systemrevision hos CA. Ved systemrevision forstås revision af:
    - Generelle it-kontroller i virksomheden,
    - It-baserede brugersystemer m.v. til generering af nøgler og nøglekomponenter samt registrering, udstedelse, verificering, opbevaring og spærring af certifikater og
    - It-systemer til udveksling af data med andre.

Valg af systemrevisor - dennes beføjelser og pligter (OCES)

- CA skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen hos CA. Den relevante mynighed kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor. CA skal senest en måned efter valg af systemrevisor anmelde dette til den relevante myndighed.

- CA skal udlevere de oplysninger, som er nødvendige for systemrevisionen i CA. Herunder skal CA give den valgte systemrevisor adgang til ledelsesprotokollen.

- CA skal give den valgte systemrevisor adgang til ledelsesmøder under behandling af sager, der har betydning for systemrevisionen. Ved et ledelsesmøde forstås et møde mellem den øverste ledelse af CA, i praksis ofte et bestyrelsesmøde. Ved udtrykket CA's ledelse forstås i denne sammenhæng den øverste ledelse af CA, dvs. bestyrelse eller tilsvarende ledelsesorgan afhængigt af, hvorledes CA er organiseret. CA skal sikre, at den valgte systemrevisor deltager i ledelsens behandling af pågældende sager, såfremt det ønskes af blot et ledelsesmedlem.

- I CA'er, hvor der afholdes generalforsamling, finder årsregnskabslovens bestemmelser om revisionens pligt til at besvare spørgsmål på et selskabs generalforsamling tilsvarende anvendelse for den valgte systemrevisor.

- CA skal gøre den valgte systemrevisor bekendt med, at denne i overensstemmelse med god revisionsskik skal foretage den nedenfor nævnte systemrevision, herunder at påse, at:
    - CA's systemer er i overensstemmelse med kravene i denne CP,
    - CA's sikkerheds-, kontrol- og revisionsbehov tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af CA's systemer,
    - CA's forretningsgange såvel de edb-baserede som de manuelle er betryggende i sikkerheds- og kontrolmæssig henseende og i overensstemmelse med CA's certificeringspraksis (CPS).

- CA skal sikre, at der i forbindelse med systemrevisionen foretages en sårbarheds- vurdering af logningsproceduren.

Overholdelse og revision (EU)

Lav

Der gennemføres jævnlige interne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

Betydelig

Der gennemføres jævnligt interne eller eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

Høj

1. Der gennemføres jævnligt uafhængige eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.
2. Hvis en ordning forvaltes direkte af et statsorgan, foretages revision i henhold til national lovgivning.