Digitaliserings-
styrelsen

Høringsnotat

28. juni 2024

Behandling af indkomne høringssvar i forbindelse med revidering af National Standard for Identiteters Sikringsniveauer (NSIS) samt vejledning og revisionsvejledning hertil

Digitaliseringsstyrelsen har ved høringsfristens udgang den 2. juni 2024 modtaget høringssvar fra i alt 12 organisationer og myndigheder, hvoraf 3 parter ingen bemærkninger havde.

Nedenstående parter har indsendt høringssvar med generelle og/eller tekstnære kommentarer:

- BDO
- Cryptomathic A/S
- Datatilsynet
- EY Danmark A/S
- Ikast-Brande Kommune
- Lakeside A/S
- Region Syddanmark
- Signaturgruppen A/S
- Sundhedsdatastyrelsen

Nedenstående parter har svaret, at de ingen bemærkninger har til høringen:

- Finanstilsynet
- Forbrugerrådet Tænk
- Sikkerhedsstyrelsen

Alle tekstnære høringssvar er gengivet i deres fulde ordlyd i sektionen nedenfor og er opdelt i Generelle bemærkninger, National Standard for Identiteters Sikringsniveauer, Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS) og Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS), Digitaliseringsstyrelsens besvarelser er indsat i sammenhæng med høringssvarene. De tre NSIS-dokumenter er efter høringsfristen justeret på baggrund af høringssvarene fra ovenstående parter. I bilag 1 fremgår oversigt over de primære ændringer i de reviderede NSIS-dokumenter.

Generelt har høringsparterne været positive ift. ændringerne, som var foreslået i høringsversionerne, og Digitaliseringsstyrelsen har modtaget mange konstruktive forslag og ønsker til de endelige NSIS-dokumenter. De endeligt

reviderede NSIS-dokumenter publiceres ultimo juni 2024 på Digitaliseringsstyrelsens hjemmeside om NSIS. Høringsnotat og bilag 1 publiceres på Høringsportalen.

Kravene i de reviderede NSIS-dokumenter træder i kraft den 30. juni 2024. Er en organisation allerede i gang med revision og anmeldelse på denne dato, er det tilladt at anvende de tidligere versioner af standard, vejledninger og skabeloner i denne proces. Kontakt gerne NSIS Tilsynet på tilsyn_nsis@digst.dk ved udfordringer ift. allerede opstartet revision og anmeldelse.

Indholdsfortegnelse

Modtagne høringssvar og besvarelser fra Digitaliseringsstyrelsen

Generelle bemærkninger

BDO

Bemærkninger	Generelt rigtig fine præciseringer og uddybninger i de reviderede dokumenter.
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret og den positive modtagelse. Behandlingen af de enkelte forslag er beskrevet nedenfor.

Datatilsynet

Bemærkninger	Ved e-mail af 7. maj 2024 har Digitaliseringsstyrelsen anmodet om Datatilsynets bemærkninger til Digitaliseringsstyrelsens reviderede version af NSIS (v. 2.1) sammen med tilhørende vejledning (v. 2.5) og revisionsvejledning (v. 1.0.0). Datatilsynet bemærker, at tilsynet ikke er NSIS-anmeldt, hvorfor denne udtalelse – ligesom Datatilsynets tidligere udtalelse vedrørende NSIS af 3. september 2018 – alene er afgivet som led i Datatilsynets status som særmyndighed inden for de databeskyttelsesretlige regler, jf. herved databeskyttelseslovens[1] § 28. Datatilsynet skal – i overensstemmelse med tilsynets tidligere udtalelse – generelt bemærke, at tilsynet også går ud fra, at den behandling af personoplysninger, som den nu reviderede version af NSIS (og det dertilhørende vejledningsmateriale) indebærer, sker inden for rammerne af databeskyttelsesforordningen[2] og databeskyttelsesloven. Datatilsynet skal hertil fortsat understrege, at tilsynet med afgivelsen af denne udtalelse ikke har foretaget en

[1] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
[2] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandlings af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF.

	vurdering af de omtalte eksisterende løsninger, herunder af hvorvidt den behandling af personoplysninger, som disse anvendes ved, lever op til databeskyttelsesforordningens krav om sikkerhed mv. Datatilsynet har i øvrigt ikke tekstnære bemærkninger til det fremsendte materiale.
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret og bekræfter, at intet er ændret i relation til overholdelse af databeskyttelsesforordningen og databeskyttelsesloven.

Lakeside A/S

Bemærkninger	[Lakeside] har ikke nogen høringssvar at give – andet end at det virker til at være en række fornuftige ændringer I foretager. [Bemærkning fra DIGST: Lakeside A/S har desuden indsendt kommentarer i en PDF med ændringsmarkeringer. Disse ændringer er primært af redaktionel karakter.]
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret og den positive modtagelse. De redaktionelle forslag er indarbejdet i dokumenterne.

Region Syddanmark

Bemærkninger	Overordnet er det Region Syddanmarks forståelse, at der er kommet en del hensigtsmæssige præciseringer med, der i det fremtidige arbejde med opfyldelse af NSIS krav giver god mening. *Indledningsvis afklaring: Er det korrekt forstået at denne revidering vil træde i kraft pr. d. 30/6-24 og derved vil skulle opfyldes pr. 30/6-24 og fremadrettet?*
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret og den positive modtagelse. Opdateringen træder i kraft ved publicering af de opdaterede dokumenter. Dette forventes at ske ultimo juni 2024. Den opdaterede standard og tilhørende vejledninger skal som udgangspunkt anvendes for

	anmeldelser og revisioner, der opstartes efter denne dato. Igangværende revisioner kan således gennemføres efter den tidligere version af standard og vejledninger. Skulle dette give anledning til problemer bedes man kontakte NSIS Tilsynet.

Signaturgruppen A/S

Bemærkninger	NSIS standarden, og Vejledningen til NSIS FullService begrebet forstås som en service fra en ID-tjeneste, hvorved modtageren ikke selv skal NSIS anmeldes. FullService begrebet anvendes dog ikke helt entydigt og konsistent i høringsudgaverne af "NSIS standarden" og "Vejledning til NSIS". FullService bør forstås som et gensidigt aftaleforhold mellem to parter, og ikke en variant af selve ID-tjenesten eller en rolle hos ID-tjenesten. Et FullService vilkår indgået mellem ID-tjenesten og modtager er fx den ansvarsfordeling, som NSIS tillader, jf. "NISS standarden" Kapitel 1.5 side 11. Det anbefales, at FullService beskrives samlet ud fra service/vilkår forståelsen, samt at hele "NSIS standarden" og "Vejledning til NSIS" genbesøges i den forståelse. I princippet er FullService en allerede eksisterende mulighed i ID-tjenesternes servicekatalog. Det som mangler i NSIS høringsudgaverne er en større klarhed omkring det aftalegrundlag, som ID-tjeneste skal sikre og anvende, for at kunne indgive en NSIS anmeldelse på vegne af modtageren, baseret på ID-tjenestens egen NSIS-anmeldte tjeneste. Af "Vejledning til NSIS" Kapitel 5.2 side 54, fremgår, at procedurer, der sikrer FullService ansvarsfordelingen, skal være beskrevet. Her kunne det fx tydeligere fremgå, at det forventede outcome til sikring af ansvarsfordeling er en indgået aftale mellem begge parter, som sikrer, at samarbejdet omkring FullService er i overensstemmelse med NSIS.
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret. En FullService IdP skal ikke betragtes som et gensidigt aftaleforhold men som en leverancemodel, hvor FullService IdP'en varetager ansvaret for opfyldelse af samtlige krav i NSIS på vegne af de brugerorganisationer, der måtte anvende FullService IdP'en. Der gælder således de samme

	krav i NSIS til en FullService IdP som til 'almindelige' Lokale IdP'er, om end nogle af kravene skal fortolkes i en lidt anden kontekst som beskrevet i vejledningen. Digitaliseringsstyrelsen er ikke enig i betragtningen om, at en FullService IdP indgiver en NSIS-anmeldelse på vegne af en modtager. En FullService IdP anmeldes separat og uafhængigt af de brugerorganisationer, som den betjener. Beskrivelsen af FullService IdP'er er indført i standardens terminologiafsnit, da konstruktionen har givet anledning til mange spørgsmål til Digitaliseringsstyrelsen, hvorfor det findes relevant at tydeliggøre især ansvarsforholdet og kravene om vandtætte skodder til brugerorganisationen. Digitaliseringsstyrelsen har på baggrund af høringssvaret præciseret i vejledningen til kapitel 5.2 punkt 9), at der bør foreligge en aftale eller vilkår mellem FullService IdP og brugerorganisationer, der beskriver ansvarsforholdet. Herved imødekommes høringssvaret delvist.

Sundhedsdatastyrelsen

Bemærkninger	Sundhedsdatastyrelsen finder de foreslåede præciseringer i standarden og den uddybende tekst i vejledningen nyttige. [...] Der er et stærkt ænske om, at i hvert fald standarden fortsat udgives på engelsk, da styrelsn har brug for at kunne være i dialog med andre parter i EU-projekter (EHDS) om krav til bl.a. brokere (hvilket ikke fremgår af eIDAS).
Svar fra DIGST	Digitaliseringsstyrelsen takker for høringssvaret og den positive modtagelse. Den nye version af standarden oversættes til engelsk, når teksten foreligger i en endelig udgave.

National Standard for Identiteters Sikringsniveauer (NSIS)

BDO

Bemærkninger	4.1.1 krav 2 "udgår fra revision" – betyder det at kravet helt udgår, dvs. at organisationen kan se bort fra det, eller er det blot at revisor ikke skal udtale sig om kravet? 4.1.4: Her kan man med fordel omtale kravene til integritetsbeskyttelse af logs. Henvisning til "god praksis" er generelt for bredt. (skal måske med i Vejledningen i stedet.) 4.1.6 krav 4: Bør flyttes til 4.1.3 da dette krav er en af grundpillerne i ISO27001. 4.1.7 krav 4: Hvem og hvordan måles om godkendt revisor har «relevante kompetencer indenfor it-revision»? Det er noteret, at det delvist er beskrevet i ny vejledning i udkast.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback vedrørende krav 4.1. og imødekommer jeres forslag med følgende rettelser: Ad 4.1.1 krav 2: baggrunden for formuleringen er, at revisor ikke længere skal erklære sig om opfyldelsen af krav vedr. lovmedholdelighed, når det ikke længere står i kapitel 4. Reference skulle have været til kapitel 7.3 og ikke 7.2, hvor lovmedholdelighed er nævnt. Dette er rettet. Ad 4.1.4:Der er i vejledningen indført en reference til kapitel 6 krav 7 som foreslået. I vejledningen findes endvidere overvejelser om god praksis for logning, herunder overvejelser om opbevaringsperiode, bevisværdi, adskillelse af forskellige datatyper og GDPR. Ad 4.1.6 krav 4: Der er i vejledningen indsat en reference til krav 4.1.3 og beskrevet, at det kan håndteres som en del af redegørelsen for ISMS. Ad 4.1.7 krav 4: Digitaliseringsstyrelsen har justeret standarden, så kravene i kapitel 4.1.7 ikke skal indgå i anmelders revisionserklæring, revisor skal således ikke erklære sig om sit eget arbejde.

Cryptomathic A/S

Bemærkninger	I standarden refereres i afsnit 8 til eIDAS ved 910/2014. Jeg vil anbefale at I får det rettet til seneste version 1183 fra 2024.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og opdaterer referencen som foreslået. Det bemærkes, at den nye version af eIDAS-forordningen er trådt i kraft 20. maj 2024, dvs. efter høringsversionen blev udsendt.

EY Danmark A/S

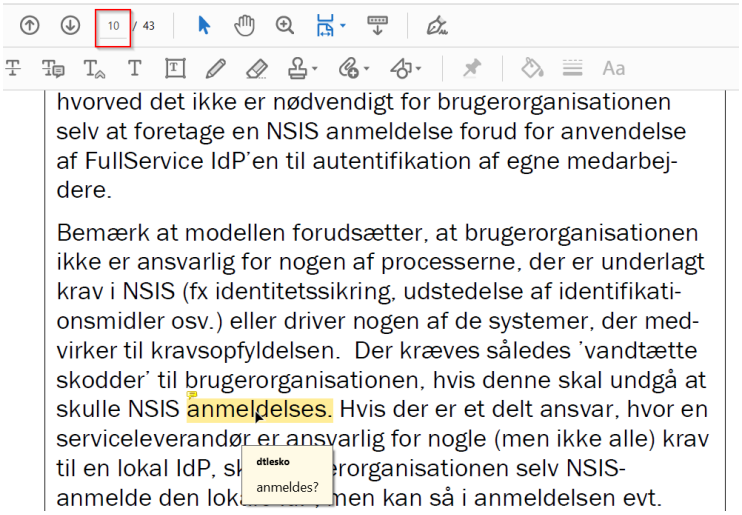
Bemærkninger	Afsnit 5.2, underkrav 9 Kravet er "Procedurer til grund for etableringen af forbindelsen er underlagt revision" Da alle kravene er underlagt revision og afgivelse af erklæring omkring efterlevelse af kravene, så vil vi anbefale at der ikke anvendes ordet 'revision' for at undgå misforståelser. I stedet kan formuleringen "Procedurer til grund for etableringen af forbindelsen er underlagt løbende og minimum årlig reevaluering og opdateringer" anvendes i stedet. Afsnit 7.3 Ansvar og forsikring I afsnittet er der nu opdateret med at anmeldere skal "have evne til at bære erstatningsansvar, hvilket fx opnås gennem forsikringsordninger (evt. selvforsikringsordninger for offentlige myndigheder)." Af afsnittet kan det tolkes som at det kun er offentlige myndigheder der har muligheden for at vælge selvforsikringsordninger. Bør elementet med 'for offentlige myndigheder' ikke fjernes, således at det er tydeligt at det også er en mulighed for private aktører, eksempelvis banker,

	og derudover evt. stille krav til at hvis der ikke er en forsikringsordning på xx mio. kr., så skal anmelder have en egenkapital over xx mio. kr. Således vil finansielle virksomheder der ofte har meget store egenkapitaler have muligheden for at vælge selvforsikringsordninger, mens mindre organisationer vil være nødt til at have en forsikringsordning.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback. Der er indført en formulering i afsnit 7.3 om, at regulerede sektorer kan anvende selvforsikring efter en nærmere vurdering. Der er ligeledes indført krav til dækningen i ansvarsforsikringen. Det er ikke vurderet hensigtsmæssigt at fastsætte krav til egenkapital.

Ikast-Brande Kommune

Bemærkninger	Krav 4.1.1 overholdelse af lovgivningen undtaget fra revisionspligten Punkt 1.6 Terminologi – Identitet (Elektronisk). *"En Identitet kan rumme Personidentifikationsdata men kan også være pseudonym"* Dækker dette over en brugerkonto til en robot som skal kunne tilgå fagsystemer (f.eks. et KOMBIT fagsystem) som kræver login på niveau betydeligt (på sigt). Brugerkontoen er en systemkonto og har derfor ikke tilknyttet et CPR nummer. P.t. forhindrer dette ibrugtagning af CH2 på f.eks. KY, hvor en del kommuner (incl. Ikast-Brande) har en robot som håndterer Flekssløn (fagsystem = Marc Flekssløn)

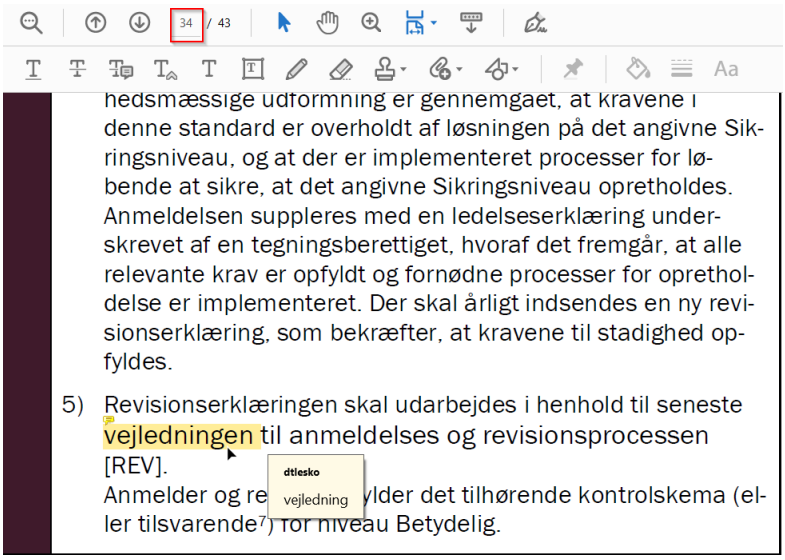
Korrektioner tekstmæssige:



hvorved det ikke er nødvendigt for brugerorganisationen selv at foretage en NSIS anmeldelse forud for anvendelse af FullService IdP'en til autentifikation af egne medarbejdere.

Bemærk at modellen forudsætter, at brugerorganisationen ikke er ansvarlig for nogen af processerne, der er underlagt krav i NSIS (fx identitetssikring, udstedelse af identifikationsmidler osv.) eller driver nogen af de systemer, der medvirker til kravsopfyldelsen. Der kræves således 'vandtætte skodder' til brugerorganisationen, hvis denne skal undgå at skulle NSIS anmeldelses. Hvis der er et delt ansvar, hvor en serviceleverandør er ansvarlig for nogle (men ikke alle) krav til en lokal IdP, sk erorganisationen selv NSIS-anmelde den lok men kan så i anmeldelsen evt.

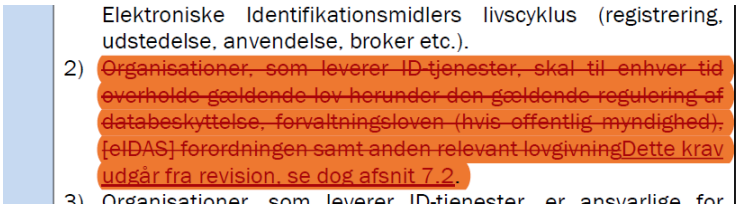
dtlesko
anmeldes?



hedsmæssige udformning er gennemgået, at kravene i denne standard er overholdt af løsningen på det angivne Sikringsniveau, og at der er implementeret processer for løbende at sikre, at det angivne Sikringsniveau opretholdes. Anmeldelsen suppleres med en ledelseserklæring underskrevet af en tegningsberettiget, hvoraf det fremgår, at alle relevante krav er opfyldt og fornødne processer for opretholdelse er implementeret. Der skal årligt indsendes en ny revisionserklæring, som bekræfter, at kravene til stadighed opfyldes.

5) Revisionserklæringen skal udarbejdes i henhold til seneste vejledningen til anmeldelses og revisionsprocessen [REV].
Anmelder og re ylder det tilhørende kontrolskema (eller tilsvarende[7]) for niveau Betydelig.

dtlesko
vejledning



Elektroniske Identifikationsmidlers livscyklus (registrering, udstedelse, anvendelse, broker etc.).

2) ~~Organisationer, som leverer ID-tjenester, skal til enhver tid overholde gældende lov herunder den gældende regulering af databeskyttelse, forvaltningsloven (hvis offentlig myndighed), [eIDAS] forordningen samt anden relevant lovgivningDette krav udgår fra revision, se dog afsnit 7.2~~.

3) Organisationer, som leverer ID-tjenester, er ansvarlige for

Ift. det som er markeret, hvornår er det gældende fra, at det ikke længere er et krav?

Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad 4.1.1: Formuleringen er justeret, så den er klarere – se svar ovenfor i høringssvar fra BDO om samme. Ad Afsnit 1.6: Identiteter i NSIS kan ikke være robotidentiteter, da de altid er knyttet til en entitet (fx fysisk person) jævnfør figur 1 i standardens afsnit 1.6, og som er i fuld kontrol med identifikationsmidlerne jævnfør standardens afsnit 3.2.1. Korrekturforslag er indarbejdet. I forhold til krav 4.1.1 punkt 2) skal kravet stadig overholdes (se afsnit 7.3 – henvisningen til 7.2 var beklageligvis forkert), men dette er ikke længere i scope for revisionen.

Lakeside A/S

Bemærkninger	1. I afsnit 1.2. Skrives der at det er muligt at tilmelde sig NSIS-nyhedsbrevet. Er det ikke netop blevet nedlagt? 2. Generelt ellers lidt formulering: side 10, 17, 18, 19, 28 3. Ved fjernelse af 4.1.1.2 henvises til afsnit 7.2 - denne reference er ikke umiddelbart forståelig. 4. Skal side 45 være blank?
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad 1.2: Det er efter udsendelse af høringsversionen blev udsendt blevet besluttet, at information om NSIS fremover vil være indeholdt i nyhedsbrevet vedr. MitID Erhverv. Henvisningen er tilpasset. Ad 2: Korrekturforslag er indarbejdet. Ad 3: Beskrivelsen er opdateret – se også svar til BDO og Ikast-Brande Kommune om samme.

	Ad 4: Tak for bemærkning. Det er ikke intentionen at have blanke sider. Versionen med ændringsmarkering har desværre haft nogle formateringsmæssige 'finurligheder' også vedr. afkortning af tekstbokse mv.

Sundhedsdatastyrelsen

Bemærkninger	I afsnit 1.5: "Eksempler på ID-tjenester og Sikringsniveauer" s. 12 er teksten vedr. sundhedsområdet upræcis/fejlagtig og ikke up to date. Teksten foreslås erstattet af følgende: "På sundhedsområdet har nationale tjenester tillid til de tokenservices, der er etableret i den nationale sundheds-it-infrastruktur. Hvor man tidligere havde etableret en national autentifikationstjeneste baseret på medarbejder OCES og NIST sikringsniveauer, vil autentifikation fremover alene ske lokalt eller ved MitID og tilliden til disse identifikationsordninger vil baseres på NSIS. Der vil fortsat ske en udstedelse af tokens fra nationale tillidstjenester på sundhedsområdet, men disse vil alene fungere som identitetsbrokere (samt berige med attributter relevant for sundhedsområdet)."
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og har indsat jeres tekstforslag som foreslået.

Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

BDO

Bemærkninger	4.1.1 krav 3: Her kan det misforstås til, at såfremt leverandøren er på positivlisten, så skal der ikke følges løbende op på denne. Jeg antager, at der stadig skal udføres løbende leverandørmonitorering, eks. via driftsmøder, SLA-rapporteringer etc, og at man ikke kan bero kontrollen på en årlig erklæring? 4.1.3 krav 2: Det kan med fordel præciseres, at der skal foreligge it-risikovurdering vedr. IdP-tjenesten. 4.1.5 krav 5: Det fremgår, at en brugeradministrator ikke betragtes som betroet medarbejder. Det forudsætter vel for det første, at denne ikke kan oprette nye administratorer i IdP setuppet (at rollen er meget begrænset, hvilket det ikke altid er i praksis), men er det derudover så ikke en væsentlig risiko, at denne "kan komme til" eks. at lukke eller slette (alle) brugeres erhvervsidentiteter? Eller "kan komme til", at oprette brugere, som ikke bør have en erhvervsidentitet? Det skrevne modsiger også lidt sig selv under beskrivelsen af underleverandører, hvor disse kan anses for betroede, hvis de selv kan oprette brugere – forskellen er ikke umiddelbart til at se. Det er endvidere lidt uklart ift. 5.2, hvor der også omtales administratorer og brugeradm. som vel anses for betroede opgaver i den sammenhæng? 5.1.5 krav 5: Følgende kan evt. tolkes ift. om kontrollen er årlig: "Organisationen kan indhente straffeattester årligt…". Da jeg tænker, at det er hensigten, at kontrollen udføres årligt, bør det omformuleres. 4.1.5 krav 5: Ift. omfanget af betroede medarbejdere, så er der forskelligheder i, hvorvidt organisationerne vurderer, at eks. adgang til datacenter eller generel Windows AD systemadministration er betroet – når begge dele er i IdP-scopet. Så det vil være fint, hvis der kan ske yderligere eksemplificering af, hvad en betroet medarbejder er.

	Vi italesætter det ofte ift. om vedkommende kan yde væsentlig skade på funktionen og drift af IdP - ift. fortrolighed men særligt ift. tilgængelighed og integritet. 4.1.5 krav 5: I praksis er der stor forskel på om leverandører foretager årligt baggrundtjek eller kun ifm. ansættelse. Det kan således ikke antages, at det er omfattet af erklæringerne, og der bør ses eksplicit efter, at kontrollen hos leverandøren er årlig. 4.1.6 krav 1: Her kan man med fordel henvises til at der skal forelægge en SOA, jf. 4.1.3, for de organisationer, som er på minimum Betydelig. Eller måske blot supplere med en henvisning til 4.1.3 for overblikkets skyld. 6 krav 5: Den anbefalede praksis med 60 min. kan med fordel underbygges af mere forklaring/risikovurdering, idet risikoappetitten i organisationerne er meget forskellig, formentlig delvist pga. manglende reel indsigt i risikoen for kæden.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad 4.1.1 krav 3: Hensigten er, at en anmelder fx kan bruge en løsning som MitID til identitetssikring og forudsætte opfyldelse af kravene på et givet NSIS-niveau ved at henvise til positivlisten. Opfølgningen består så ikke i at se revisionserklæringer fra MitID (som ved en 'normal' underleverandør) men ved at monitorere, at MitID fortsat er på positivlisten på det givne sikringsniveau. Opfølgningen på MitID's forhold sker gennem MitID's egen NSIS-anmeldelse og revisionserklæring. Ovenstående er præciseret i vejledningen. Ad 4.1.3 krav 2: Dette er præciseret som foreslået. Ad 4.1.5 krav 5: Beskrivelsen af betroede medarbejdere er yderligere præciseret. Terminologien er endvidere skiftet til den almene betegnelse 'privilegeret adgang', når der refereres til den systemiske adgang i 4.1.5 punkt 7, og det er præciseret, at sådanne administratorer ikke nødvendigvis er betroede.

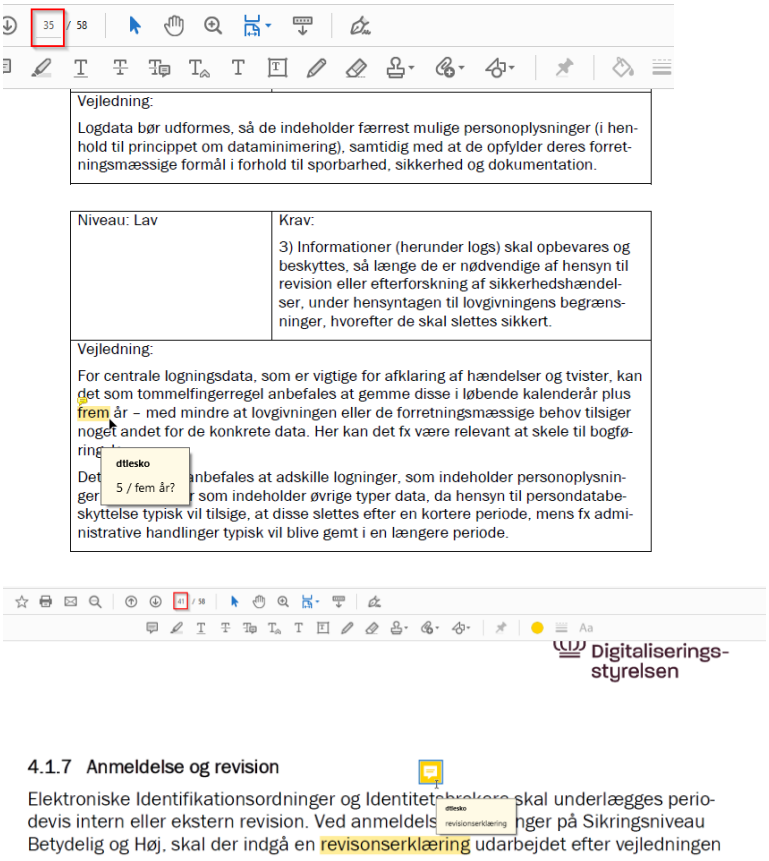
	Ad 5.1.5 krav 5: Vejledningen er præciseret som foreslået. Ad 4.1.6 krav 1: Henvisning til 4.1.3 er indsat. Ad 6 krav 5: Vejledningen er udbygget med beskrivelse af risikofaktorer.

Cryptomathic A/S

Bemærkninger	I vejledningen refereres under afsnit 4.1.6 til dokumenter fra SOGIS og Enisa. Jeg vil anbefale at i anvender seneste version fra SOGIS som er 1.3, i vejledningen refereres til version 1.2. Enisa vedligeholder ikke anbefalinger til kryptografiske algoritmer, jeg vil derfor helt anbefale at udelade denne reference.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og har opdateret henvisningen som foreslået.

Ikast-Brande Kommune

Bemærkninger	Krav 4.1.5, punkt 5: Det kunne være rart, hvis I udarbejdede en nem og overskuelig oversigt over, hvem der skal anses som betroet medarbejder, og hvem der ikke skal. Opstilling i tabelform vil gøre det meget mere overskueligt Krav 4.1.7: ROS: bilag A tilgængeligt i Word-format. Vil være meget tidsbesparende for os ift. nuværende Excel udgave med låste felter.

	Korrektioner tekstmæssige: 
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad 4.1.5 punkt 5): Vejledningen er udbygget ganske betydeligt på dette punkt, herunder med overvejelser der kan lægges til grund for vurderingen af, om medarbejdere skal anses som betroede. Da der er tale om vurderinger afhængig af den enkelte organisations lokale forhold og ikke en "fast opskrift" egner fremstillingen sig efter vores opfattelse ikke til tabelform. Ad 4.1.7: Digitaliseringsstyrelsen vil fremover publicere en Word-version af kontrolskemaet også. Korrekturforslag er indarbejdet.

Lakeside A/S

Bemærkninger	Der er stadig en vejledning til punkt 4.1.1.2 - den bør vel fjernes når punktet udgår fra standarden?
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og har slettet vejledningen til det udgåede krav.

Region Syddanmark

Bemærkninger	**Side:** 36-37 **Krav 4.1.5:** "Faciliteter og personale" **krav 5** **Bemærkning:** Præcisering af betroede medarbejdere. Kan dette krav fortolkes således at betroede medarbejdere alene er medarbejdere, der qva deres udvidede rettigheder kan omgå kontroller og dermed har mulighed for at: a. svindle med (med andre ord overtage eller impersonere) en anden medarbejders Erhvervs Identitet, eller b. oprette en fiktiv medarbejder og tilknytte en erhvervsidentitet? Og hermed at privilegerede brugere, der administrerer rettigheder og dermed medarbejdernes rettighed til at have en erhvervs-identitet, samt medarbejdere der administrerer tilhørende ID-midler (oprettelse, ændringer, nedlæggelse) ikke anses for betroede medarbejdere? *I Region Syddanmark får medarbejderen en erhvervsidentitet ved at medarbejderens it-bruger tilknyttes AD-gruppen for erhvervsidentiteter tilknyttes af en privilegeret bruger.*
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback. Rettighedsadministratorer er, som beskrevet i vejledningen, ikke 'betroede' i NSIS-forstand, da NSIS ikke regulerer rettighedstildeling men alene digitale identiteter. Der kan være andre grunde (end NSIS) til at det kan være relevant at foretage baggrundstjek på rettighedsadministratorer – eksempelvis som følge af risikovurderinger (ISO 27000) eller andre compliance-regimer.

Signaturgruppen A/S

Bemærkninger	Kapitel 4.1.6, krav 7, Vejledning: Vi anbefaler at man skriver konkrete algoritmer og nøglelængder ud af vejledningen, da man ved ændring af disse vil være nødsaget til at opdatere dokumentet tilsvarende.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback. Digitaliseringsstyrelsen er principielt enig, men der har været mange forespørgsler til, hvad der er tilstrækkeligt, og et ønske om mere konkret vejledning, så fortolkningen af 'tilstrækkelighed' ikke alene var overladt til revisor. På den baggrund har styrelsen indført nogle forsigtige formuleringer som 'tommelfingerregler' og i øvrigt henvist til mere dybdegående kilder. Styrelsen er opmærksom på risikoen for, at vejledningen skal opdateres, hvis der skulle ske landvindinger inden for kryptografien, men risikoen for at AES (128 bit) eller RSA (3072 bit) pludseligt vurderes som utilstrækkelige forventes at være temmelig lille.

Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

BDO

Bemærkninger	Sektion 2, afsnit 1: Det fremgår ikke helt klart om Excel-arket explicit skal vedlægges, såfremt relevante kolonner, linjer og information fremgår af erklæringens kapitel 3 (Se en af BDO's erklæringer). Såfremt vores template anvendes er Excelarket vel overflødigt? Sektion 3.3, afsnit 3: Der kan med fordel suppleres med flere eksempler på signifikante ændringer ud fra de spørgsmål, som kommuner har stillet DIGST om dette.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer jeres forslag med følgende rettelser: Ad Sektion 2, afsnit 1: Såfremt indholdet fra kontrolskemaet er bevaret i et andet format, er det ikke nødvendigt at vedlægge det originale kontrolskema. Dette er gjort tydeligere i vejledningen. Ad Sektion 3.3, afsnit 3: Der er tilføjet yderligere eksempler til afsnittet med eksempler på signifikante ændringer.

EY Danmark A/S

Bemærkninger	**Afsnit 2.1.1 Eksempel på udfyldelse af skema** Der er i eksemplet i underafsnittet "Kolonne k – Revisionshandlinger ved udført revision" anført et eksempel, som umiddelbart ikke lever op til revisionshandlingerne, der i øvrigt anbefales i vejledningen på side 5, hvor der er angivet følgende revisionshandlinger: Forespørgsel, observation, inspektion eller genudførsel af kontrol. Eksemplet der er anført i vejledningen på side 6 i underafsnittet "Kolonne k – Revisionshandlinger ved udført revision", kan give anledning til upræcise formuleringer af revisionshandlinger og vi vil anbefale, at der anføres eksempler, som understøtter, revisionshandlinger der udføres ved test af kontrollers effektivitet/implementering, som er i

	overensstemmelse med de anførte principper i udvælgelsesprocessen i vejledningen. Ligeledes kan resultat af test eksemplet kortes ned, således at der anvendes enten "Ingen afvigelser konstateret", eller "Ingen yderligere afvigelser konstateret" som anført ovenfor. Dette er den traditionelle måde for revisorer at rapportere i denne type af erklæringer. Afsnit 3 Anmeldelser på niveau Betydelig og Høj I afsnittet er der tilføjet at: "Det skal tydeligt fremgå …, og revisor skal eksplicit henvise til den dokumentation, som ligger til grund for revisionen, og der skal gives en eksplicit konklusion for hvert enkelt NSIS-krav." Revisor anfører aldrig eksplicit hvilken dokumentation der har ligget til grund for revisionen. Ved erklæringer med sikkerhed (eksempelvis ISAE 3000 erklæringer), står revisor inde for at den dokumentation der er modtaget er tilstrækkelig til at kunne konkludere på kontrollens udførelse og kravets efterlevelse. Som følge af revisors tavshedspligt, kan revisor ikke offentliggøre eksplicit hvilke dokumenter der har ligget til grundlag for revisionen. EY vil derfor kraftigt anbefale at dette krav fjernes fra NSIS vejledningen. I samme afsnit er også til føjet at "der skal gives en eksplicit konklusion for hvert enkelt NSIS krav" I erklæringer af denne type giver revisor konklusion for hvert krav (eks. 3.1) i form af at der beskrives resultatet af de udførte test handlinger, typisk i 1 af 3 udgaver. 1. Ingen afvigelser konstateret. Dette betyder at revisor ikke har identificeret tilfælde hvor kontrollen eller kravet ikke er designet, implementeret (og for type 2 erklæringer operationelt effektiv. 2. Ingen yderligere afvigelser konstateret. Dette betyder at der lige inden denne tekst er anført en beskrivelse af hvorledes kontrollen eller kravet ikke er fuldt ud opfyldt, dvs. her vil være der situationer

	hvor kontrollen / kravet enten ikke er designet, implementeret eller operationelt effektivt. Af resultat af test vil der altid fremgå hvad der ikke er designet, implementeret eller operationelt effektivt og omfanget her af (eks. 2 of af 25 stikprøver). 3. At det ikke har været muligt at teste kontrollens effektivitet, da der ikke har været nogle tilfælde hvor kontrollen har været udført i perioden. Af resultat af test vil det fremgå hvad det er det ikke har været muligt at teste pga. at kontrollen ikke har skulle udføres. Dette er så eksplicit revisor kan rapportere i en ISAE 3000 erklæring, dette ligeledes pga. fortrolighed. Sidst i afsnit 3 er der indsat et afsnit om at Hvis der er foretaget ændringer i forhold til den oprindelige anmeldelse skal anmelder ved indsendelse af en type 2 erklæring yderligere fremsende en opdateret anmeldelse, hvor ændringerne fremgå tydeligt - eksempelvis markeret med fed tekst. Endvidere skal der indsendes en fornyet ledelseserklæring, der er dateret og underskrevet af ledelsen. Her til det være godt hvis det kunne præciseres at tilføjelser eller fjernelse af CVR nr. der er omfattet af den lokale IdP tjeneste ikke anses som ændringer til IdP tjenesten, og derved ikke kræver opdatering af erklæringen. Det er ganske omfattende at opdatere en erklæring hvis der blot er etableret et nyt datterselskab der er koblet på den eksisterende id-tjeneste, da det principielt er en ny erklæring der skal udarbejdes grundet revisionsmæssige krav til planlægning, risikovurdering, rapportering mv. i revisorlovgivningen. Afsnit 3.2 Behandling af anmeldelse og revisionserklæring. Afsnittet med tidsperioden som NSIS tilsynet har til gennemgang af modtagne anmeldelser og erklæringer er fjernet. Hvorfor? Som anmelder er det vigtigt at vide hvornår man kan forvente et svar fra NSIS tilsynet, særligt i forbindelse med

	første gangs anmeldelser, da den lokale IdP tjeneste ikke må tages i brug inden den er godkendt, men der kan være andre aftaler der er opsagt, hvorfor anmelder skal have mulighed for at estimere hvornår svar fra NSIS tilsyn kan forventes modtaget, således at den samlede tidsplan for anmeldelsen kan estimeres / fastlægges. Ligeledes i afsnit 3.2 er der tilføjet at "Hvis anmelders revisorerklæring indeholder samme revisionsbemærkninger i to på hinanden følgende årlige erklæringer, grundet manglende udbedring af forholdene, skal anmelder senest 6 måneder efter NSIS Tilsynets behandling sende NSIS Tilsynet dokumentation for udbedring af forholdet. Overholdes dette ikke, vil det som udgangspunkt medføre afnotering" Hvad menes med "samme revisionsbemærkninger". Er det hvis det er præcis den samme revisionsbemærkning (præcis samme formulering), eller menes blot hvis der stadig er en afvigelse fsva. den specifikke kontrol / krav. I visse situationer kan afvigelsen være delvist udbedret, men ikke fuldt udbedret, hvorfor der stadig kan være en afvigelse, men med en lidt anderledes formulering. Vil det også medføre afnotering hvis forholdet er forbedret, men ikke fuldt afhjulpet? Hvis det også vil medføre afnotering hvis blot der fortsat er en afvigelse bør dette præciseres. Afsnit 3.4.2 Revision efter partiel metoden I afsnittet er der tilføjet et punkt #5 med "Anmelders revisor skal eksplicit erklære sig om, hvorvidt revisor er enig i, at der er overensstemmelse mellem kravene, herunder at relevante krav i NSIS for underleverandøren vurderes som værende opfyldt." Som anført ovenfor så rapporterer revisor på en af 3 måneder: 1. Ingen afvigelser konstateret. Dette betyder at er enig i at der er overensstemmelse mellem krevene

	i NSIS og de 'genbrugte' erklæring fra en underleverandør 2. Ingen yderligere afvigelser konstateret. Dette betyder at hele eller dele af kontrollen / kravet ikke er opfyldt. Der vil i resultat af test være anført hvilke dele der ikke anses opfyldt. 3. At det ikke har været muligt at teste kontrollens effektivitet (bør ikke være relevant i denne situation). Dvs. revisor skriver ikke positivt at revisor er enig. Dette kan udledes af, at der anføres at der er 'ingen afvigelser konstateret'. Revisor anfører i øvrigt også i "Revisionshandlinger ved udført revision", at de eksempelvis har inspiceret underleverandørens erklæring, som også er en klar indikation på, at revisoren har taget stilling til de relevante krav i NSIS efterleves ved gennemgang af underleverandørens erklæring. Herudover ved anvendelse af partiel metoden, så har revisor ikke haft mulighed for hverken at påvirke revisionen af underleverandøren, eller mulighed for at gennemgå arbejdspapirer mv. hos underleverandørens revisor. Revisor kan derfor ikke eksplicit (positivt) udtale sig om hvorvidt der er (100%) overensstemmelse mellem NSIS kravet og de relaterede kontroller. Revisor kan vurdere om der efter hans professionelle vurdering er overensstemmelse, og dette rapporteres gennem formuleringen 'ingen afvigelser konstateret', men revisor kan ikke positivt udtale sig om at der er overensstemmelse, da revisor ikke har den viden om underleverandøren til at kunne gøre dette. EY vil derfor kraft fraråde at der er krav om at revisor 'eksplicit skal erklære sig enig i, at der er overensstemmelse mellem kravene…" Der kan i stedet formuleres at virksomhedens ledelse skal indhente erklæring fra underleverandører og vurdere om erklæringen fra underleverandøren, og vurdere "at der er overensstemmelse mellem kravene…" Revisor skal herefter gennemgå ledelsens vurdering, og sikre at denne er foretaget og på en hensigtsmæssig måde.

	Kravet omkring vurdering af underleverandørens erklæring skal være et krav til virksomhedens ledelse, ikke til revisor. **Afsnit 4 Anmeldelser på niveau Lav** I det nye afsnit står der i første tekstafsnit " Den interne revision skal foretages af en organisatorisk enhed i den anmeldende organisation, som ikke er involveret i driften af ID-tjenesten – ideelt set en organisatorisk enhed som refererer til en anden del af organisationens ledelseschef-hierarki end den del af organisationen, som har ansvaret for ID-tjenesten." Traditionelt set, så er intern revision i Danmark organisatorisk placeret lige under bestyrelsen eller kommunalbestyrelsen. Bestyrelsen vil altid have det ultimativt sidste ledelsesansvar. En anden formulering der kan overvejes, er at "…ideelt set en organisatorisk enhed der er uafhængig af den øvrige organisation". Afsnit 4 omtaler alene intern revision, men der er vel ikke forbud mod at gennemgangen til brug for niveau lav udføres af en ekstern revisor. Det anbefales derfor at der sidst i afsnit 4 tilføjes en linje om at "Intern revisions opgaver i forbindelse med anmeldelse på niveau lav, kan også udføres af en ekstern revisor". **Afsnit 6 Forhold, der kan medføre afnotering.** For afsnit 6.1 og 6.2 lyder det som om at dagen efter tidsfristen er overskrevet, så bliver ID tjenesten afnoteret. Bør der ikke indføjes at ved overskridelse af tidsfristen sender NSIS tilsynet en rykker, og overskrides denne rykker, vil der ske afmeldelse. Således at en kortere forsinkelse pga. sygdom el.lign. ikke går hen og medfører afnotering.

	For afsnit 6.3 Gentagende revisionsbemærkninger, se kommentar ovenfor omkring afsnit 3.2 og 'samme revisionsbemærkninger" Det er uhensigtsmæssigt at der i afsnit 3.2 og 6.3 ikke anvendes samme begreber, henholdsvis 'samme revisionsbemærkninger (3.2) og "gentagende forhold" (6.3) om noget der antages at skulle dække samme situation.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad Afsnit 2.1.1: Teksten i afsnittet Kolonne K er ændret således, at revisionshandlingen angives som "inspektion" hhv. "genudførsel af kontrol". Teksten i afsnittet Kolonne I er ændret således, at de eventuelle afvigelser beskrives, eller det konstateres, at der ingen afvigelser er fundet. Ad Afsnit 3 Anmeldelser på niveau Betydelig og Høj: Digitaliseringsstyrelsen imødekommer forslaget om at fjerne kravet om direkte henvisning til dokumentation, idet vi forstår de fortrolighedshensyn, som revisor skal overholde. Ligeledes fjerner vi kravet om eksplicitte konklusioner for hvert enkelt NSIS-krav, da de eksisterende formuleringer i ISAE 3000-erklæringer allerede opfylder behovet inden for revisors tavshedspligt. Ad Sidst i afsnit 3 er der indsat et afsnit om at: NSIS Tilsynet ønsker ikke at bede om en ny fuld erklæring men en erklæring om, at hvad der er gældende i første erklæring også er gældende for datterselskabet. Til afsnit 5 er tilføjet en forklaring af, hvilke revisionshandlinger, der skal foretages ved tilføjelse til CVR til det eksisterende. Ad Afsnit 3.2 Behandling af anmeldelse og revisionserklæring: Digitaliseringsstyrelsen imødekommer forslag og sætter en forventet maksimal behandlingstid på 60 dage. Der tilføjes en bemærkning om, at behandlingstiden kan være længere i perioder, samt at behandlingen først anses for at være påbegyndt, når alle forhold er belyst og al nødvendig dokumentation er NSIS Tilsynet i hænde. Den angivne forventede behandlingstid er sat under hensyntagen til, at sagen skal behandles i NSIS Tilsynet, samt at der skal være tid til partshøring over afgørelser, som NSIS Tilsynet træffer. Der tilstræbes således at give anmeldere

	en mere præcis forventning om behandlingstid og dermed muliggøre bedre planlægning af den samlede tidsplan for anmeldelsen. Ad Ligeledes i afsnit 3.2 er der tilføjet at: Det er præciseret, at det omhandler forhold fra tidligere revisionserklæringer, som ikke er blevet udbedret (Gentagne forhold). Ad Afsnit 3.4.2 Revision efter partielmetoden: Punkt 5 er ændret til, at revisor foretager en inspektion af anmelders redegørelse for sammenhængen mellem NSIS-krav og kontrollerne i den genbrugte erklæring samt af relevante kontroller i den genbrugte erklæring. Ad Afsnit 4 Anmeldelser på niveau Lav: Digitaliseringsstyrelsen imødekommer forslaget og har præciseret vejledningen. Formuleringen er ændret til: "...ideelt set en organisatorisk enhed, der er uafhængig af den øvrige organisation." Desuden tilføjes en linje om, at "intern revisions opgaver i forbindelse med anmeldelse på niveau Lav kan også udføres af en ekstern revisor." Ad Afsnit 6 Forhold, der kan medføre afnotering: Digitaliseringsstyrelsen imødekommer forslaget og har ændret vejledningen, så det fremgår, at ved overskridelse af tidsfristen sender NSIS Tilsynet en rykker. Hvis denne rykker også overskrides, vil der ske afnotering. Dette vil forhindre, at en kortere forsinkelse, eksempelvis på grund af sygdom, medfører afnotering. Derudover er begreberne harmoniseret i afsnit 3.2 og 6.3, så begge steder anvender udtrykket "gentagne forhold" for at undgå forvirring og sikre konsistens.

Ikast-Brande Kommune

Bemærkninger	<u>Punkt 2:</u> *"Der er udarbejdet et Excel-skema ('kontrolskemaet'), der skal udfyldes og vedlægges anmeldelsen og indgå som en del af anmeldelsen. Kontrolskemaet må ikke modificeres ved eksempelvis at fjerne felter eller foretage ændringer i tekst. Anmelder og revisor skal anvende den nyeste version af kontrolskemaet. Det er tilladt at overføre*

	kontrolskemaet til andre dokumenttyper, hvis dette vurderes mere praktisk, så længe indholdet bevares for de krav, der besvares. Skemaet indeholder NSIS kravene og tilhørende felter, som skal udfyldes af henholdsvis anmelder af løsningen og revisor." I dokumentet Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS) krav 4.1.7 står der dette: *4.1.7 Anmeldelse og revision* *Elektroniske Identifikationsordninger og Identitetsbrokere skal underlægges periodevis intern eller ekstern revision. Ved anmeldelse af løsninger på Sikringsniveau Betydelig og Høj, skal der indgå en revisonserklæring udarbejdet efter vejledningen til anmeldelses- og revisionsprocessen [REV], som Digitaliseringsstyrelsen har udgivet til formålet. Desuden er der udarbejdet et kontrolskema (Excel og Word), som kan anvendes til at dokumentere kravopfyldelse, revisionshandlinger og konklusion. Ved udfyldelse af skemaet skal der krav-for-krav redegøres for, hvordan kravet er opfyldt, hvordan revisionen er foretaget, og hvilken konklusion revisor er kommet frem til.* Der bør rettes i punkt 2.1 så der står det samme begge steder så der ikke er nogen tvivl om, at vi kan anvende Word kontrolskemaet. <u>Punkt 3.3 Opdateringer efter anmeldelse</u> *" Eksempler på sådanne signifikante ændringer kunne være, at løsningen opdateres fra at være på sikringsniveau Betydelig til Høj, at der indføres helt nye typer af identifikationsmidler eller helt nye processer for identitetssikring etc. Ændringer til løsningen, der ikke vurderes som signifikante, medfører ikke krav om ny anmeldelse, og vil blive håndteret af den næste, årlige revision."* Kan det uddybes, hvad "helt nye processer for identitetssikring" indebærer? Er det f.eks. indførsel af et IdM system eller skift af en autoritativ datakilde? <u>Generel kommentar omkring anmærkninger og revision</u> En opfordring til mere smidighed omkring revision / anmærkninger – en opdeling i graverende fejl (som skal udløse en anmærkning), vurdering som enkeltstående fejl

	(hvis der er 1 ud af 20 stikprøver – skal det så udløse en anmærkning) Det må være meningen med revisionen at klarlægge, om de beskrevne kontroller fungerer som de skal overordnet set. Ikke at der bliver fundet en enkelt "smutter". Dette vil ligeledes betyde en mere smidig sagsbehandling hos NSIS tilsynet som vil få anmeldelser med færre anmærkninger som skal håndteres med kommunerne.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad Punkt 2: Der er udarbejdet et kontrolskema i Word-format. Ad Punkt 3.3 Opdateringer efter anmeldelse: Digitaliseringsstyrelsen imødekommer forslaget og tilføjer eksempler for at tydeliggøre, hvad "helt nye processer for identitetssikring" indebærer. Ad Generel kommentar omkring anmærkninger og revision: Digitaliseringsstyrelsen imødekommer forslaget om mere smidighed i håndteringen af revision og anmærkninger. Da en sådan ændring skal koordineres med revisorerne, vil Digitaliseringsstyrelsen arbejde på at implementere dette i en fremtidig version af vejledningen. Digitaliseringsstyrelsen forstår vigtigheden af at skelne mellem graverende fejl og enkeltstående fejl for at sikre en mere effektiv og retfærdig revisionsproces.

Lakeside A/S

Bemærkninger	1. Lidt formuleringer: side 5, 7 2. I afsnit 6.1 mangler vejledning ift. Niveau Høj. 3. Figur 1 grafik mangler opdatering i forhold til ændringer.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og har tilrettet vejledningen som foreslået.

Region Syddanmark

Bemærkninger	**Side:** 4 **Bullet punkt:** "Anmelders beskrivelse af kontrolmål". **Bemærkning:** Det bemærkes at der ved denne ændring fra SMART mål til passende procedurer kan åbnes op for fortolkning og evt. diskrepans ift. forståelse for hvad passende procedurer er. Det kunne derfor være hensigtsmæssigt at der blev formuleret nogle konkrete eksempler ift. hvad passende procedurer kan være, samt til hvilke krav man har ønsket at imødekomme udfordringerne med SMART-mål? **Side:** 10 **Krav 3.4.2:** "Revision efter partielmetoden" pkt. 5 **Bemærkning:** Vi er usikre på, om der ved denne præcisering kan opstå uoverensstemmelser imellem anmelders revisor og underleverandørens revisor, fx at anmelders revisor er uenig i underleverandørens revisor, og hvilke udfordringer det kan give for anmelder.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad **Bullet punkt:** "Anmelders beskrivelse af kontrolmål".: Afsnit 2.1.1 indeholder et eksempel på udfyldelse af skema, herunder et forslag til, hvordan et kontrolmål kan beskrives. Ud fra dette skal der etableres en passende procedure. I den sidste ende vil det være en eksterne revisor, som vurderer om proceduren er passende. Ad **Krav 3.4.2:** "Revision efter partielmetoden" pkt. 5: Det er i alle tilfælde anmelders revisors vurdering, der er den gældende. Formuleringen er ændret, så dette tydeligere fremgår.

Signaturgruppen A/S

Bemærkninger	Kapitel 2: Man har foreslået at fjerne SMART fra beskrivelsen i forbindelse med kontrolmål, men det fremgår fortsat af figuren i afsnit samt i teksten i afsnit 2.1.1. Kapitel 3, afsnit 4: Man har foreslået en ændring, hvoraf det fremgår at "revisor skal eksplicit henvise til den dokumentation, som ligger til grund for revisionen". Revisor vil

	som en del af sin revisionsopgave have adgang til den nødvendige dokumentation for at kunne udarbejde sin erklæring, hvorfor vi ser det som en unødvendig tilføjelse, da en kildehenvisning i sig selv ikke tilfører nogen værdi til opgaven, heller ikke for Tilsynet i forbindelse med deres vurdering af den indsendte erklæring. Vi anmoder derfor om at denne tilføjelse fjernes. Kapitel 3.2: Vi finder det uhensigtsmæssigt at man fra Tilsynets side ikke vil beskrive hvilke forventninger markedet kan have til Tilsynets gennemgang af indsendte erklæringer, herunder en forventet maksimal behandlingstid. I forbindelse med nye produkter i markedet er det essentielt at kunne styre kundernes forventninger til ibrugtagning af nye produkter, hvorfor Tilsynets behandling af indsendte erklæringer er et vigtigt element heri. Kapitel 3.2: Nyt krav om yderligere revision forholder sig ikke til usikkerheden i den gennemførte revision. Fastholdes ekstra revisionskravet i høringsforslaget uændret kan det betyde, at en NSIS anmelder er forpligtet til at prioritere evt. gengangere for at kunne opfylde ekstra revisionskravet, uagtet at der på andre områder slet ikke har kunnet gennemføres revision. Kravet bør justeres ud fra en væsentlighedsbetragtning og afgrænses fx til de meget usikre situationer, hvor revisor gentagne gange tager et revisionsforbehold på hele, eller dele af, NSIS-området, hvorved revisor ikke har kunnet foretage NSIS revision, med den fornødne sikkerhed. Det behøver ikke være samme område, det er gentagelsen af væsentlige problemer med revisionsgennemførelsen, som bør være den afgørende faktor for yderligere revision. At en observation gentages, kan være udtryk for at NSIS-anmelder og revisor ikke er enige, hvilket typisk også vil kunne fremgå al ledelsens handlingsplan for den konkrete observation. I en sådan situation vil yderligere revision ikke gøre nogen forskel.
Svar fra DIGST	Digitaliseringsstyrelsen takker for jeres feedback og imødekommer forslagene med følgende rettelser: Ad Kapitel 2: Dette er rettet. Ad Kapitel 3, afsnit 4: Digitaliseringsstyrelsen imødekommer dette forslag og har fjernet tilføjelsen.

	Ad Kapitel 3.2 (om forventet maksimal behandlingstid): Digitaliseringsstyrelsen imødekommer forslag og sætter en forventet maksimal behandlingstid på 60 dage. Der tilføjes en bemærkning om, at behandlingstiden kan være længere i perioder, samt at behandlingen først anses for at være påbegyndt, når alle forhold er belyst og al nødvendig dokumentation er NSIS Tilsynet i hænde. Den angivne forventede behandlingstid er sat under hensyntagen til, at sagen skal behandles i NSIS Tilsynet samt at der skal være tid til partshøring over afgørelser, som NSIS Tilsynet træffer. Der tilstræbes således at give anmeldere en mere præcis forventning om behandlingstid og dermed muliggøre bedre planlægning af den samlede tidsplan for anmeldelsen. Ad Kapitel 3.2 (om revision ved gentagne forhold): Ved uenighed mellem anmelder og revisor om efterlevelse af et relevant NSIS-krav opfordrer Digitaliseringsstyrelsen til, at parterne gennem dialog når frem til enighed om, hvorledes anmelder kan udbedre manglende efterlevelse af NSIS-kravet, således at forholdet ikke gentages i efterfølgende revisionserklæringer.