Digitaliserings-
styrelsen

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

Version 1.1.0

Dato: 28.06.2024

1 Indledning

Dette dokument indeholder en beskrivelse af anmeldelse- og revisionsprocessen for den til enhver tid gældende version af National Standard for Identiteters Sikringsniveauer (NSIS).

Dokumentet er målrettet offentlige og private organisationer, der ønsker at anmelde deres løsninger til Digitaliseringsstyrelsens NSIS Tilsyn som Elektronisk Identifikationsordning og/eller Identitetsbroker, samt de revisorer, der skal foretage revision af ID-tjenesterne.

Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsens NSIS Tilsyn, skal der på Sikringsniveau Betydelig og Høj vedlægges en revisionserklæring fra en godkendt revisor eller et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 3, stk. 1, nr. 18). Se venligst kapitel 3 *Anmeldelser på niveau Betydelig og Høj* for yderligere information om dette.

På sikringsniveau Lav er det tilstrækkeligt at indsende dokumentation for gennemført *intern* revision. Anmelderen skal på sikringsniveau Lav endvidere årligt indsende en ledelseserklæring på, at anmeldelsen fortsat er retvisende og løsningen er aktiv – eller alternativt opdatere sin anmeldelse eller bede om afnotering fra listen over anmeldte løsninger. Se venligst kapitel 4 *Anmeldelser på niveau Lav* for yderligere information om dette.

Læsere af dette dokument forventes at have orienteret sig i NSIS, den tilhørende vejledning samt øvrige relevante dokumenter.

1.1 Ændringshistorik

Dato	Version	Ændringer
03.05.2024	1.0.0	Dette er et nyt dokument, baseret på dokumentet "Revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS) - Version 2.0.7" • Dokumenttitel ændret fra "Revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)" til "Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)" for at tydeliggøre, at dokumentet ikke kun er rettet mod revisorer men også mod anmeldere. • Struktur: Opdeling af kapitler. • Eksemplet på udfyldelse af kontrolskema er uddybet og præciseret (2.1.1) • Afsnit 1.3 Krav til revisionserklæringer er ændret til kapitel 3: Anmeldelser på niveau Betydelig og Høj. • Præcisering af krav til dokumentation for tilsyn med underleverandører (3.4). • Udvidelse af frist for indsendelse af Type 2-erklæringer fra 60 kalenderdage til 90 kalenderdage fra den dag, hvor 12-måneders perioden udløber (3.1). • Nyt kapitel indført om anmeldelser på niveau Lav (kapitel 4). • Nyt kapitel indført om anmeldelse af flere organisatoriske enheder (CVR-numre) (kapitel 5). • Nyt kapitel indført om forhold der kan medføre afnotering (kapitel 6). • Nyt kapitel indført om revision ved ophør af ID-tjeneste (kapitel 7).

Dato	Version	Ændringer
28.06.2024	1.1.0	Tilrettet version af 1.0.0 på baggrund af høringssvar. • Kapitel 2 er præciseret så det fremgår, at det ikke er nødvendigt at vedlægge et kontrolskema i Excel-format, hvis det vedlægges i et andet format, og at Digitaliseringsstyrelsen vil udarbejde en skabelon for kontrolskemaet i Word. • Afsnit 2.1.1 er præciseret så det fremgår, hvilke revisionshandlinger revisor forventes at foretage. • Kapitel 3 er ændret, således at krav om eksplicit henvisning til dokumentation og eksplicit konklusion for hvert enkelt NSIS-krav udgår. • I afsnit 3.2 er den forventede behandlingstid i NSIS Tilsynet ændret fra 30 til 60 kalenderdage • Afsnit 3.3 er udbygget med yderligere eksempler på signifikante ændringer. • Afsnit 3.4.2 er præciseret i forhold til revisionshandlinger. • Krav om redegørelse og handlingsplan for mindre væsentlige forhold, der er afdækket af revisionen, udgår af afsnit 3.2 og kapitel 4. • Kapitel 4 er præciseret i forhold til intern revision. • Det er beskrevet i Kapitel 5, hvorledes ændringer i CVR-numre håndteres. • Kapitel 6 er præciseret omkring proces ved overskridelse af tidsfrister.

2 Skema til anmeldelse

Der er udarbejdet et kontrolskema i både Excel- og Word-format, som 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. Såfremt indholdet fra kontrolskemaet er bevaret i et andet format, er det ikke nødvendigt at vedlægge det originale kontrolskema. Skemaet indeholder NSIS-kravene og tilhørende felter, som skal udfyldes af henholdsvis anmelder af løsningen og revisor. Derudover findes der en anmeldelsesskabelon med stamoplysninger om den anmeldte løsning samt ledelseserklæring.

De første kolonner i kontrolskemaet indeholder samtlige krav i NSIS opsat på struktureret form og udgør den primære dokumentation for efterlevelsen af kravene. For hvert enkelt krav er det angivet, om kravet er relevant for hhv. Elektroniske Identifikationsordninger, for Identitetsbrokere eller begge typer løsninger. Kun krav, der er relevante for anmeldelse af den pågældende type løsning, skal udfyldes.

I tilknytning til de respektive NSIS-krav indeholder skemaet to kolonner, som skal udfyldes af anmelderen af en løsning, og to kolonner, som efterfølgende skal udfyldes af anmelders revisor:

Anmelders beskrivelse af opfyldelse (Praksis)	Anmelders beskrivelse af kontrolmål (SMART)	Revisionshandlinger ved udført revision	Resultat af udført revision
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*Udfyldes af revisor*	*Udfyldes af revisor*
Udfyldes af NSIS anmelder *Udfyldes af NSIS anmelder*	*Udfyldes af NSIS anmelder* *Udfyldes af NSIS anmelder*	*Udfyldes af revisor* *Udfyldes af revisor*	*Udfyldes af revisor* *Udfyldes af revisor*

Hensigten med de enkelte kolonner gennemgås nedenfor:

- **Anmelders beskrivelse af opfyldelse (praksis)**
  Her beskriver anmelder, hvorledes de tilhørende NSIS-krav på det relevante sikringsniveau er opfyldt. Redegørelsen indeholder en beskrivelse af implementerede tekniske-, processuelle- eller organisatoriske- tiltag. Den kan med fordel udarbejdes i form af en 'praksis' som fx kendes fra dokumentation af overholdelse af certifikatpolitikker (via CPS – Certification Practice Statement).
- **Anmelders beskrivelse af kontrolmål**
  Her beskriver anmelder i form af kontrolmål, hvordan man konkret kan kontrollere, om den beskrevne praksis er opfyldt/implementeret. Punktet bør formuleres som en kontrol, hvortil der etableret passende procedurer
- **Revisionshandlinger ved udført revision**
  Her angiver revisor (intern eller ekstern), hvilke revisionshandlinger og observationer, der er foretaget ved vurdering af det konkrete krav.
- **Resultat af udført revision**
  Her udtrykker revisor en konklusion vedr. den udførte revision for det pågældende krav.

I udvælgelsesprocessen af revionshandlingerne ved vurderingen, anbefales det at anvende følgende principper:

Princip	Beskrivelse
Forespørgsel	Interview, møde, forespørgsel med ansvarligt personel hos leverandøren
Observation	Observation af gennemførelsen af kontrol
Inspektion	Gennemgang og evaluering af politikker, procedurer og dokumentation vedrørende kontrollens resultater. Dette omfatter gennemlæsning og evaluering af rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet og implementeret. Desuden vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførsel af kontrol	Gentagelse af de relevante kontrolelementer for at verificere udførslen af kontrolfunktionerne.

Bemærk, at anmelderens udfyldelse af kontrolskemaet bør være dækkende og selvindeholdt. Det er dog tilladt at referere til vedlagte dokumenter i kontrolskemaet for yderligere detaljer (fx teknisk dokumentation, certifikater inden for IT-sikkerhed og/eller beskyttelse af persondata - f.eks. ISO 2700x certifikat, diverse ISAE-erklæringer). Vær dog opmærksom på, at beskrivelsen i skemaet bør være tilstrækkelig dækkende til, at den i sig selv giver en sammenhængende redegørelse for, hvordan kravet er opfyldt.

2.1.1 Eksempel på udfyldelse af skema

I det følgende gennemgås kort et eksempel på udfyldelse af skemaet. Fokus er på at illustreret logikken i skemaet og ikke at give et udtømmende eksempel.

Der tages udgangspunkt i flg. krav til verifikation af identitet for fysiske personer på Sikringsniveau Lav, afsnit 3.1.2:

NSIS-krav afsnit 3.12

1) Der skal gennemføres verifikation, og der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund. 2) Ansøgeren (Entiteten) skal med overvejende sandsynlighed vurderes at være i besiddelse af almindeligt anerkendt dokumentation for sin Identitet. Dette kan fx være sygesikringskort, pas, kørekort, dåbsattest eller forskudsopgørelse. 3) Dokumentationen kan antages at være ægte og gyldig.

Kolonne i - Anmelders beskrivelse af opfyldelse (praksis)

1. Ansøgningen gennemføres via en online formular. Her skal alle ansøgere uploade en kopi af dansk pas eller kørekort, som registreres på ansøgningen, samt angive CPR nummer. Det kontrolleres at

pas/kørekort ikke er udløbet, og ved opslag i pas- og kørekortregister sikres, at det pågældende dokument ikke er spærret. Ved opslag i CPR-registret sikres, at den pågældende person findes og ikke er død eller meldt savnet. Endelig kontrollerer en sagsbehandler manuelt, at identiteten i CPR-registret stemmer overens til identiteten i pas/kørekort ved at sammenligne for- og efternavne. Sagsbehandler vurderer endvidere den uploadede dokumentations ægthed.

2. Såfremt opslag i pas- og kørekortregister viser at det relevante dokument ikke er spærret, opslaget i CPR-registret viser, at den pågældende person findes og ikke er død eller meldt savnet og CPR-nummeret matcher for- og efternavn på den uploadede dokumentation vurderes identiteten at være korrekt.
3. Såfremt dokumentationen af sagsbehandler vurderes at være ægte og gyldig godtages denne.

Kolonne j - Anmelders beskrivelse af kontrolmål (SMART)

For hver ansøgning etableres et kontrolspor i form af en logning af, hvor flg. oplysninger fremgår:

1. Oplyst CPR nummer
   Uploadet billede af pas/kørekort
2. Resultat af opslag i CPR-registret inkl. navn, adresse og status i CPR
   Resultat af opslag i pas/kørekortregister
   Sagsbehandlers godkendelse af billede inkl. entydig identifikation af sagsbehandler
   Status på sagsbehandlers godkendelse af overensstemmelse mellem identitet i CPR og pas/kørekort
3. Sagsbehandlers vurdering af ægtheden af dokumentationen

Ud fra dette kontrolspor, vil det være muligt at kontrollere, om praksis er efterlevet.

Kolonne k - Revisionshandlinger ved udført revision

Der er udtaget en population på 50 tilfældige ansøgninger og det er inspiceret, om der foreligger en logning for hver ansøgning med alle ovennævnte oplysninger. Det er inspiceret, om der for alle godkendte ansøgninger er overensstemmelse mellem identitet i CPR og pas/kørekort, herunder om sagsbehandleren har foretaget en korrekt sammenligning. Det er endvidere inspiceret, om der er ansøgninger, hvor opslag på pas/kørekort/CPR viser ugyldig status, som er blevet godkendt.

Der er foretaget genudførsel af kontrol af, om ansøgning med spærret pas og kørekort medfører, at disse afvises af systemet med korrekt fejlkode i loggen.

Endelig er der foretaget genudførsel af kontrol af, om indtastning med CPR-nummer for død person eller med et ugyldigt CPR-nummer medfører, at disse afvises med korrekt fejlkode i loggen.

Kolonne l – Resultat af udført revision

Ingen afvigelser konstateret.

3 Anmeldelser på niveau Betydelig og Høj

Revisor skal ud over udfyldelse af ovennævnte skema udarbejde en specifik erklæring om den anmeldte løsning. Revisionserklæringen kan være en ISAE 3000-erklæring eller tilsvarende, og der skal opnås en høj grad af sikkerhed efter denne standard. Revisionserklæringer suppleres altid med en ledelseserklæring.

Revisionserklæringen har formål at konkludere (på baggrund af indholdet i kontrolskemaet for de enkelte krav), hvorvidt anmelder samlet set har etableret alle relevante procedurer og udformet funktionaliteten af kontroller, der knytter sig til procedurer, som beskrevet i NSIS på det ønskede sikringsniveau. Samtlige krav på et bestemt sikringsniveau og på alle lavere sikringsniveauer skal således være opfyldt for den relevante type løsning, før løsningen kan siges at leve op til det pågældende sikringsniveau.

Det er anmelderens ansvar at udforme alle relevante procedurer og kontroller til sikring af, at kravene i NSIS overholdes. Det er revisors ansvar at udtrykke en konklusion om, hvorvidt de af ledelsen etablerede procedurer og kontroller var hensigtsmæssigt udformet og implementeret på anmeldelsestidspunktet, og hvorvidt disse fungerede hensigtsmæssigt i hele erklæringsperioden (se afsnit 3.1 nedenfor). Det skal tydeligt fremgå, hvilke revisionshandlinger revisor har udført.

I kontrolskemaet er angivet kontrolmål, som skal være omfattet af revisionserklæringen, samt dokumentation af de konkrete revisionshandlinger, der er udført. Revisionen skal omfatte procedurer og kontroller for alle relevante kontrolmål. Det er revisors ansvar at tilpasse revisionshandlingerne til de konkrete procedurer og kontroller, der er etableret hos anmelderen.

3.1 Typer, frister og perioder for erklæringer

Hvis der er tale om en ny løsning under udvikling, kan der anvendes en ISAE 3000-erklæring gående på løsningens design til den første anmeldelse.

Der kan anvendes en ISAE 3000 type 1-erklæring (design og implementering) til den første anmeldelse for løsninger, som er færdigimplementeret.

Endelig kan der ved anmeldelse af en kørende løsning benyttes en ISAE 3000 type 2-erklæring (design, implementering og operationel effektivitet) for en bagudrettet periode.

Erklæringstidspunktet[1] for den første erklæring må under alle omstændigheder højst være 90 dage før anmeldelsen foretages, så det sikres, at erklæringen afspejler det faktiske system.

Anvendes en ISAE 3000-erklæring alene på design som første erklæring, skal anmelder senest 4 måneder efter idriftsættelsen af løsningen (go-live) levere en type 1-erklæring (design og implementering) for at demonstrere, at implementeringen efterlever designet.

[1] Ved 'erklæringstidspunktet' forstås her den specifikke dato (design eller type 1), som revisionen udtaler sig om - ofte benævnt 'per-datoen', skæringsdatoen eller 'as-of' datoen. I tilfældet med en type 2-erklæring forstås den sidste dato i erklæringsperioden. Erklæringstidspunktet er således afkoblet fra, hvornår erklæringen underskrives.

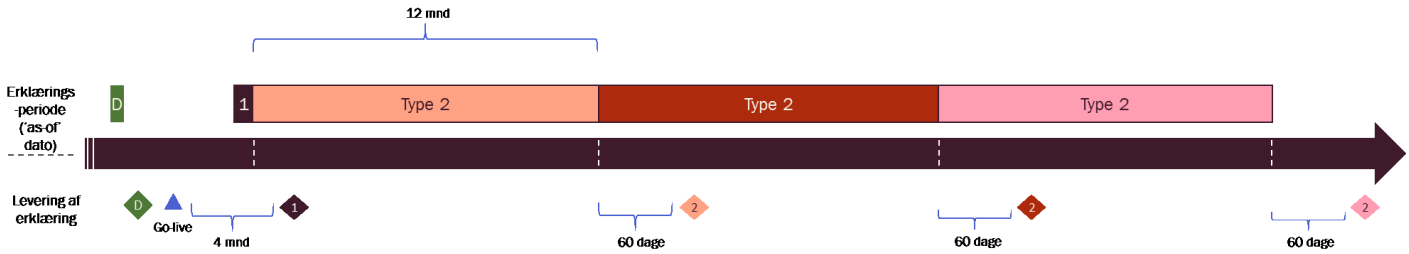
Efter indsendelse af en type 1- eller type 2-erklæring, skal anmelder én gang årligt indsende en ISAE 3000 type 2-erklæring for en 12 måneders periode, hvor erklæringsperioden ligger i umiddelbar forlængelse af perioden for seneste erklæring. Erklæringen skal være Digitaliseringsstyrelsens NSIS Tilsyn i hænde senest 90 kalenderdage regnet fra den dag, hvor 12-måneders perioden udløber. Det er tilladt at benytte en kortere periode end 12 måneder for en type 2-erklæring, hvis særlige hensyn taler herfor - eksempelvis et ønske om at harmonisere erklæringsperioder for flere systemer med hinanden. For at opnå en tilstrækkelig høj sikkerhed i revisors udtalelse, skal erklæringsperioden dog være på mindst 6 måneder.

Hvis der er foretaget ændringer i forhold til den oprindelige anmeldelse skal anmelder ved indsendelse af type 2-erklæringen yderligere fremsende en opdateret anmeldelse, hvor ændringerne fremgår tydeligt - eksempelvis markeret med fed tekst. Endvidere skal der indsendes en fornyet ledelseserklæring, der er dateret og underskrevet af ledelsen.

Brugen af de forskellige erklæringer er opsummeret i nedenstående skema:

Erklæring	Næste erklæring som skal leveres
Design	Type 1 senest 4 måneder efter idriftsættelsen af systemet
Design og implementering (type 1)	Type 2-erklæring senest 12 måneder + 90 dage efter erklæringstidspunkt for type 1 erklæringen.
Design, implementering og operationel effektivitet (type 2)	Type 2-erklæring senest 12 måneder + 90 dage efter erklæringstidspunkt for seneste type 2-erklæring.

Et eksempel på et erklæringsforløb er illustreret på nedenstående figur. Her indleveres først en designerklæring (grøn), dernæst en type 1-erklæring (mørk lilla) og herefter årlige type 2-erklæringer (laksefarvet, rød, lyserød).



Figur 1: Eksempel på erklæringsforløb

3.2 Behandling af anmeldelse og revisionserklæring

NSIS Tilsynet vil ved gennemgang af revisionserklæringer fra anmelder anvende kontrolskemaet til at vurdere, om revisors erklæring omfatter de nødvendige forhold. Hvis der er områder, som ikke er relevante, skal anmelders revisor begrunde, hvorfor forholdet ikke er relevant. Eksisterer der forhold, som er væsentlige, og som ikke er indeholdt i områderne nedenfor, skal disse områder medtages i den afgivne revisionserklæring.

Er NSIS Tilsynets gennemgang ikke afsluttet inden 60 kalenderdage efter anmeldelsen, underretter NSIS Tilsynet anmelderen herom, forklarer årsagerne til forsinkelsen samt oplyser, hvornår gennemgangen forventes at være afsluttet. Behandlingen anses først for at være påbegyndt, når alle forhold er belyst og al nødvendig dokumentation er NSIS Tilsynet i hænde.

I det tilfælde at en revisionserklæring afgives med forbehold, kan dette medføre afvisning eller afnotering som godkendt udbyder af en Elektronisk Identifikationsordning eller Identitetsbroker. I det tilfælde at der fremgår bemærkninger af erklæringen (af mindre væsentlig karakter), vil NSIS Tilsynet gøre anmelder opmærksom på, at de forhold, der har givet anledning til bemærkningerne i revisionserklæringen skal udbedres inden næste opfølgende revision.

Hvis anmelders revisionserklæring indeholder gentagne bemærkninger grundet manglende udbedring af forhold, som er bemærket i foregående revisionserklæring, skal anmelder senest 6 måneder efter NSIS Tilsynets behandling sende NSIS Tilsynet dokumentation for udbedring af disse. Overholdes dette ikke, vil det som udgangspunkt medføre afnotering.

3.3 Opdateringer efter anmeldelse

Hvis der foretages signifikante ændringer til den anmeldte løsning, skal der uden for den normale revisionscyklus beskrevet ovenfor indsendes en opdateret anmeldelse med en delta-anmeldelse inkl. revisionserklæring samt opdaterede bilag, som tydeligt beskriver de relevante ændringer, samt hvilke NSIS-krav, der påvirkes af ændringen. Det skal ligeledes fremgå af revisionserklæringen, hvilke NSIS-krav erklæringen omfatter, samt hvordan revisor har forholdt sig til disse krav. Om nødvendigt vil NSIS Tilsynets registrering af løsningen blive opdateret. Den opdaterede anmeldelse med tilhørende revisionserklæring indsendes til NSIS Tilsynet senest 90 dage efter, at ændringen er sat i drift.

Anmelder bærer ansvaret for, at løsningen lever op til NSIS-kravene fra idriftsættelsen af ændringen, herunder konsekvenser i form af tilbagerulning eller andet som følge af manglende opfyldelse. NSIS Tilsynet kan først forventes at opdatere registreringen på sin hjemmeside efter modtagelse og efterfølgende behandling af den opdaterede anmeldelse.

Eksempler på sådanne signifikante ændringer kan være, at løsningen opdateres fra at være på sikringsniveau Betydelig til Høj, at der indføres helt nye typer af identifikationsmidler, at en væsentlig underleverandør udskiftes, at der er væsentlige ændringer til processer, herunder identitetssikring (som f.eks. biometri eller multifaktor autentificering) eller organisatorisk ansvar - eller andre ændringer, som vil medføre behov for opdatering af anmelders risikovurderinger.

Ændringer til løsningen, der ikke vurderes som signifikante, medfører ikke krav om ny anmeldelse, og vil blive håndteret af den næste, årlige revision.

3.4 Håndtering af leverandører

Det er meget udbredt, at organisationer anvender leverandører og eventuelt underleverandører til at håndtere systemer eller processer, der er underlagt kravene i NSIS. I den forbindelse er det vigtigt, at der i anmeldelsen og/eller revisionserklæringen eksplicit er redegjort for, hvilke parter, der håndterer hvilke krav, samt at alle relevante parter er underlagt revision. Bemærk at visse tværgående og organisatoriske krav kan være relevante for alle parter. Hvis leverandørens system eller ydelse

er NSIS-anmeldt selvstændigt og dermed optræder på positivlisten, er det tilstrækkeligt at henvise til dette, og der er i dette tilfælde ikke behov for at indsende revisionserklæring for leverandøren.

3.4.1 Revision efter helhedsmetoden

Hvis anmelder anvender leverandører og/eller underleverandører, kan anmelders erklæring udformes efter 'helhedsmetoden', hvor alle leverandører i kæden er omfattet af samme erklæring. Det vil sige både leverandører og eventulle underleverandører. Helhedsmetoden er en metode til håndtering af de ydelser, en leverandør leverer, hvor leverandørens beskrivelse af sit system omfatter arten af de ydelser, en leverandør leverer, og hvor leverandørens og eventuelle underleverandørers relevante kontrolmål og tilknyttede kontroller indgår i anmelderens beskrivelse af sit system og i omfanget af anmelders revisors opgave.

3.4.2 Revision efter partielmetoden

En anmelder kan alternativt beslutte at anvende partielmetoden for revision, hvor leverandørers og eventuelle underleverandørers ydelser ikke direkte er omfattet af revisionen.

Det er således tilladt at genanvende en revisionserklæring fra en leverandør med henblik på at dokumentere leverandørens opfyldelse af krav i NSIS. Anvendes partielmetoden skal leverandørers relevante revisionserklæringer også medsendes NSIS-anmeldelsen.

Forudsætningen for genbrug af eksisterende erklæringer fra en leverandører er følgende:

1. At der er tale om en ISAE 3000-revisionserklæring eller tilsvarende med høj grad af sikkerhed, hvor krav og kontrolmål er tilsvarende de specifikke krav i NSIS, som er relevante for leverandørens ydelser (eksempelvis en driftsydelse).
2. Erklæringen kan være en generel eller løsningsspecifik erklæring, så længe kravene modsvarer NSIS[2].
3. Anmelder skal eksplicit angive, hvilket krav der varetages af henholdsvis anmelder og leverandør, eller eventuelt af begge.
4. Anmelderen skal ved genbrug af leverandørerklæringer eksplicit redegøre for, hvorledes opfyldelsen af hvert enkelt NSIS-krav kan ses dokumenteret i den genbrugte erklæring. Hvert enkelt relevant NSIS-krav skal således mappes til et navngivet kontrolmål i den genbrugte erklæring. Denne mapning skal inkluderes i anmelders kontrolskema.
5. Anmelders revisor skal inspicere, om der er overensstemmelse mellem relevante NSIS-krav og de respektive kontrolmål i den genbrugte erklæring, samt om kontrolmålene er efterlevet.
6. Anmelderens egenkontrol af leverandørens erklæring skal derudover indgå i revisionen udført af den godkendte revisor

Et eksempel på, hvor denne metode kan være hensigtsmæssig, er når underleverandøren fx er en driftsleverandør (fx en international cloudleverandør), der ikke kan

[2] Generelle erklæringer kan eksempelvis lægges til grund for de dele, som ikke er løsningsspecifikke, f.eks. fysisk sikkerhed i et datacenter, mens den konkrete og løsningsspecifikke opsætning af miljøer skal gennemgås af den godkendte revisor.

underlægges anmelderens (kundens) revisor - men i stedet kan levere en alternativ, erklæring for tilsvarende sikkerhedskrav udformet af egen revisor.

Erklæringsperioden for underleverandører kan afvige fra anmelders egen erklæringsperiode. En underliggende Type 1- eller 2-erklæring må være op til et år gammel, når den indgår i en anmeldelse, og 90-dages reglen omtalt i afsnit 3.1 gælder således ikke for underleverandørers erklæringer.

4 Anmeldelser på niveau Lav

På sikringsniveau Lav, skal der udføres intern revision i forbindelse med anmeldelse af ID-tjenester og hvert derpå følgende år. 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 der er uafhængig af den øvrige organisation. Alternativt kan den interne revision udføres af en ekstern revisor.

Den interne revision skal gentages hvert år og anmelder skal årligt indsende en ledelseserklæring hvoraf det fremgår, at ID-tjenestens samlede data-, system- og driftssikkerhed fortsat er betryggede og efterlever den gældende Nationale Standard for Identiteters Sikringsniveauer på sikringsniveau Lav, og at der er gennemført intern revision af ID-tjenesten, som dokumenterer dette.

Den interne revision har til formål at vurdere (på baggrund af indholdet i kontrolskemaet for de enkelte krav), hvorvidt anmelder samlet set har etableret alle relevante revisionsprocedurer og udformet funktionaliteten af kontroller, der knytter sig til procedurer, som beskrevet i NSIS sikringsniveau Lav.

Det er anmelderens ansvar at udforme alle relevante procedurer og kontroller til sikring af, at kravene i NSIS overholdes. Det er den interne revisors ansvar at udtrykke en konklusion om, hvorvidt de af ledelsen etablerede procedurer og kontroller var hensigtsmæssigt udformet og implementeret på anmeldelsestidspunktet, og hvorvidt disse fungerede hensigtsmæssigt, og den interne revisor skal attestere denne konklusion med sin underskrift.

I kontrolskemaet er angivet kontrolmål, som skal være omfattet af den interne revision, samt konkrete revisionshandlinger, der er udført. Den interne revision skal omfatte procedurer og kontroller for alle kontrolmålene. Det er den interne revisors ansvar at tilpasse revisionshandlingerne til de konkrete procedurer og kontroller, der er etableret hos anmelderen.

I det tilfælde at den interne revisionserklæring afgives med forbehold, kan dette medføre afvisning af anmeldelsen af ID-tjenesten. I det tilfælde at der fremgår bemærkninger af erklæringen (af mindre væsentlig karakter), vil NSIS Tilsynet gøre anmelder opmærksom på, at de forhold, der har givet anledning til bemærkningerne i revisionserklæringen skal udbedres inden næste opfølgende revision. Ved den efterfølgende årlige interne revision skal anmelder indsende en intern revisionserklæring, der dokumenterer, at der er rettet op på forholdene, der gav anledning til revisionsbemærkningerne. Hvis anmelders opfølgende interne revision derimod ikke dokumenterer, at forholdene er udbedret, skal anmelder til NSIS Tilsynet senest 6 måneder efter NSIS Tilsynets afgørelse fremsende dokumentation for udbedring af forholdene. Overholdes dette ikke, vil dette som udgangspunkt medføre afnotering.

4.1 Opdatering efter anmeldelse

Hvis der foretages signifikante ændringer til den anmeldte løsning, skal der uden for den normale revisionscyklus indsendes en delta-anmeldelse som beskrevet i punkt 3.3 *Opdateringer efter anmeldelse* ovenfor.

4.2 Håndtering af leverandører

Hvis der i forbindelse med levering af ID-tjenesten anvendes leverandører, skal den interne revision dokumentere dette jævnfør retningslinjerne i afsnit 3.4 *Håndtering af leverandører ovenfor*.

5 Anmeldelse af flere organisatoriske enheder

Der kan foretages en 'fælles' NSIS-anmeldelse for flere virksomheder, f.eks. i en koncern. Dette forudsætter dog, at både anmeldelsen (forsiden) og revisionserklæringen (omfangsbeskrivelsen) indeholder beskrivelser af det samlede system (inkl. de pågældende CVR-numre). Der må således ikke forekomme lokale varianter i processer eller systemer, som ikke er dækket af anmeldelsen og den tilhørende revisionserklæring.

Ved 'fællesanmeldelser' skal én af organisationerne fremgå som kontaktperson for den samlede anmeldelse.

5.1 Ændringer i CVR-numre

Såfremt der er ændringer i, hvilke CVR-numre, der er omfattet af NSIS-anmeldelse og revisionserklæring, skal NSIS Tilsynet orienteres om dette, og hvis der tilføjes nye organisatoriske enheder, skal der vedlægges en revisionserklæring, som udtaler sig om, hvorvidt NSIS-kravene håndteres som i den oprindelige anmeldelse.

Såfremt NSIS-kravene ikke håndteres på samme måde for de nye organisatoriske enheder, skal der gennemføres revision af disse jævnfør afsnit 3.3 *Opdateringer efter anmeldelse*.

6 Forhold, der kan medføre afnotering

Nedenstående forhold kan medføre, at en ID-tjeneste bliver afnoteret fra NSIS-positivlisten. Genoptagelse på NSIS-positivlisten vil kræve en ny anmeldelse af ID-tjenesten.

6.1 Manglende årlig revisions- eller ledelseserklæring

Anmeldere på niveau lav skal årligt indsende en ledelseserklæring.

Modtager NSIS Tilsynet ikke denne erklæring inden for fristen, vil der blive sendt en påmindelse. Hvis anmelder ikke reagerer på denne påmindelse, vil dette som udgangspunkt medføre afnotering fra NSIS-positivlisten.

Anmeldere på niveau betydelig skal årligt indsende en revisionserklæring (Type 2).

Modtager NSIS Tilsynet ikke denne erklæring inden for fristen, vil der blive sendt en påmindelse. Hvis anmelder ikke reagerer på denne påmindelse, vil dette som udgangspunkt medføre afnotering fra NSIS-positivlisten.

6.2 Gentagne revisionsbemærkninger

Indeholder ID-tjenestens årlige, opfølgende revionserklæring bemærkninger, som omhandler forhold, der også blev bemærket i den foregående revisionserklæring grundet manglende udbedring af forholdene, giver NSIS Tilsynet udbyderen af ID-tjenesten en frist på 6 måneder til at indsende dokumentation for udbedring af forholdene samt en fornyet revisionserklæring, som bekræfter dette.

Modtager NSIS Tilsynet ikke denne erklæring inden for fristen, vil der blive sendt en påmindelse. Hvis udbyderen ikke reagerer på denne påmindelse, vil dette som udgangspunkt medføre afnotering fra NSIS-positivlisten.

7 Revision ved ophør af ID-tjeneste

Ønsker en udbyder at ophøre med at udbyde en ID-tjeneste samt at blive afnoteret fra NSIS-positivlisten, skal udbyderen af ID-tjenesten hurtigst muligt og senest på datoen for ophøret med udbydelsen af ID-tjenesten orientere NSIS Tilsynet om denne beslutning.

Som anført i NSIS punkt 4.1.7 *Anmeldelse og revision* er anmelder ansvarlig for, at den udbudte ID-tjeneste til stadighed efterlever relevante NSIS-krav, og der skal gennemføres intern eller ekstern revision, som vurderer om dette er tilfældet.

Dette gælder således også i perioden fra seneste revision og indtil ophørstidspunktet for ID-tjenesten.

Som anført under punkt 3.1 ovenfor, vurderes det, at en revisionsperiode på mindst 6 måneder er nødvendig for, at der kan opnås en tilstrækkelig høj grad af sikkerhed i revisors udtalelse om efterlevelsen af relevante NSIS-krav.

Kravet om revision vil derfor bortfalde, såfremt perioden fra seneste revision til ophørstidspunktet er mindre end 6 måneder. I disse tilfælde vil det være tilstrækkeligt, at udbyder senest 30 dage efter ID-tjenestens ophør til NSIS Tilsynet indsender en ledelseserklæring, som redegør for, at ID-tjenesten i ophørsperioden har efterlevet alle relevante NSIS-krav.

Såfremt perioden fra seneste revision til ophørstidspunktet er 6 måneder eller derover, vil der skulle foretages intern eller ekstern revision på samme måde som i forbindelse med den årlige opfølgning.

På NSIS-sikringsniveau Lav, skal udbyder således indsende en ledelseserklæring hvoraf det fremgår, at alle relevante NSIS-krav på sikringsniveau Lav er efterlevet i perioden fra seneste revision til ophørstidspunktet, og at der er gennemført intern revision af ID-tjenesten, som dokumenterer dette.

På sikringsniveau Betydelig eller Høj skal udbyder seneste 90 dage efter ID-tjenestens ophør indsende en type 2-revisionserklæring, som dokumenterer, at alle relevante NSIS-krav på sikringsniveau Betydelig eller Høj er efterlevet i perioden fra seneste revision til ophørstidspunktet.