DIGITALISERINGSSTYRELSEN

Revisionsvejledning
til
National Standard for
Identiteters Sikringsniveauer (NSIS)

Status: Version 2.0.7

Version: 08.11.2022

1 Indledning

Dette dokument udgør revisionsvejledningen til version 2.0.2 af National Standard for Identiteters Sikringsniveauer (NSIS).

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 statsautoriseret revisor eller et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 3, stk. 1, nr. 18). Dette dokument beskriver kravene til eksterne revisionserklæringer og giver vejledning og eksempler på udformning af disse.

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.

Dokumentet er målrettet organisationer, der ønsker at anmelde deres løsninger til Digitaliseringsstyrelsens NSIS Tilsyn som Elektronisk Identifikationsordning og/eller Identitetsbroker, samt de revisorer, der skal udarbejde tilhørende erklæringer.

Læsere af dette dokument forventes at have indsigt i NSIS.

1.1 Ændringshistorik

Dato	Version	Ændringer
08.11.2022	2.0.7	I afsnit 1.3 er det præciseret, at revisionserklæringer altid suppleres med en ledelseserklæring. I afsnit 1.3.2 er det præciseret, at man ved en delta-anmeldelse skal vedlægge opdaterede bilag, så det er tydeligt, hvad forskellen siden sidste anmeldelse består i. Afsnit 1.3.3 om håndtering af underleverandører er opdateret, herunder beskrivelsen af anvendelse af partielmetoden og helhedsmetoden. Disse to metoder er nu ligeværdige alternativer. Terminologien er ensrettet, så begrebet 'underleverandør' anvendes konsekvent.

1.2 Skema til anmeldelse

Som supplement til dette dokument er der udarbejdet et Excel-skema ('kontrolskemaet'), der udfyldes og vedlægges anmeldelsen. Det er tilladt at overføre indholdet af 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. Derudover findes der en anmeldelsesskabelon med stamoplysninger om den anmeldte løsning samt ledelseserklæring.

Der er ikke krav om, at kontrolskemaet anvendes ved intern revision, men det anbefales også at anvende under den interne revision.

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 revisor*	*Udfyldes af revisor*
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*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 (SMART)**
  Her beskriver anmelder i form af kontrolmål, hvordan man konkret kan kontrollere, om den beskrevne praksis er opfyldt / implementeret. Punktet bør formuleres som et SMART[1] krav, så det sikres, at det er entydigt og målbart.
- **Revisionshandlinger ved udført revision**
  Her angiver revisor, hvilke revisionshandlinger og observationer, som benyttes 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

[1] **S**pecific (Specifik), **M**easurable (Målbare), **A**chievable (Opnåelige), **R**elevant (Relevante) og **T**ime-bound (Tidsbestemte)

	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 bilag A for yderligere detaljer (fx teknisk dokumentation, certifikater indenfor 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.

1.2.1 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 og realistisk 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 en 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)

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.

Kolonne j - Anmelders beskrivelse af kontrolmål (SMART)

For hver ansøgning findes en logning af et kontrolspor, hvor flg. oplysninger fremgår:

- Oplyst CPR nummer
- Uploadet billede af pas/kørekort
- 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

Kolonne k - Revisionshandlinger ved udført revision

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

Der er endvidere forsøgt ansøgning med spærret pas og kørekort og konstateret, at disse afvises af systemet med korrekt fejlkode i loggen.

Endelig er der forsøgt ansøgning med CPR-nummer for død person samt ugyldigt CPR-nummer, og det er konstateret, at disse afvises med korrekt fejlkode i loggen.

Kolonne l – Resultat af udført revision

Revisionen har ikke givet anledning til bemærkninger, og det konkluderes, at de beskrevne procedurer og kontroller er implementeret og effektive.

1.3 Krav til revisionserklæring

Revisor skal udover udfyldelse af ovennævnte skema udarbejde en specifik erklæring om den anmeldte løsning. Revisionserklæringen udarbejdes efter ISAE 3000 standarden 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-standarden på det ønskede sikringsniveau. Samtlige krav på et bestemt sikringsniveau 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-standarden 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 1.3.1 nedenfor).

I bilag A er angivet kontrolmål, som skal være omfattet af revisionserklæringen, samt eksempler på konkrete revisionshandlinger, der kan udføres. Revisionen skal omfatte procedurer og kontroller inden for alle kontrolmålene. Det er revisors ansvar at tilpasse revisionshandlingerne til de konkrete procedurer og kontroller, der er etableret hos anmelderen.

1.3.1 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. Hvis løsningen er færdigimplementeret men ikke idriftsat, kan der anvendes en ISAE 3000 type 1 erklæring (design og implementering) til den første anmeldelse. 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[2] for den første erklæring må under alle omstændigheder højst være 90 dage før anmeldelsen foretages, så det sikres, at erklæringen afspejler det faktiske system.

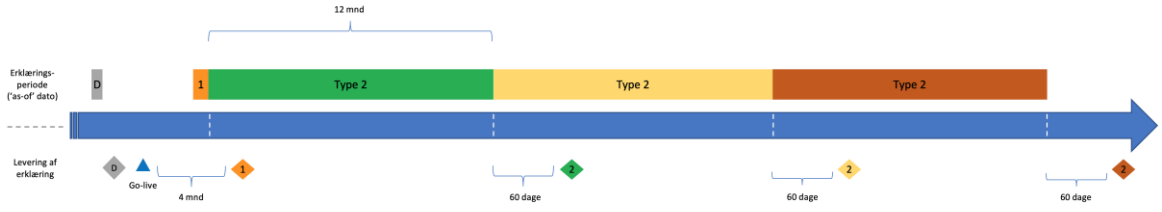
Anvendes en ISAE 3000 erklæring alene på design som første erklæring, skal anmelder senest 4 måneder efter idriftsættelsen af løsningen (go-live) levere en type 1 erklæring (design og implementering) for at demonstrere, at implementeringen efterlever designet.

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 60 kalenderdage regnet fra den dag, hvor 12-måneders perioden udløber. Det er dog 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.

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 + 60 dage efter erklæringstidspunkt for type 1 erklæringen.
Design, implementering og operationel effektivitet (type 2)	Type 2 erklæring senest 12 måneder + 60 dage efter erklæringstidspunkt for seneste type 2 erklæring.

Et eksempel på et erklæringsforløb er illustreret på nedenstående figur. Her indleveres først en designerklæring (grå), dernæst en type 1 erklæring (orange) og herefter årlige type 2 erklæringer (grøn, gul, orange).



Figur 1: Eksempel på erklæringsforløb

NSIS Tilsynet vil ved gennemgang af revisionserklæringer fra anmelder anvende kontrolskemaet til at vurdere, om revisors erklæring omfatter de nødvendige forhold. Hvis der er

[2] 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.

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 30 dage efter anmeldelsen, underretter NSIS Tilsynet anmelderen herom, forklarer årsagerne til forsinkelsen samt oplyser, hvornår gennemgangen forventes at være afsluttet.

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 (ofte af mindre væsentlig karakter), skal NSIS Tilsynet senest 60 kalenderdage efter NSIS Tilsynets behandling af erklæringen modtage en skriftlig redegørelse fra anmelder indeholdende en beskrivelse af forholdene og en detaljeret handlings- og tidsplan for udbedring af forholdet. Overholdes dette ikke, kan dette ligeledes medføre afnotering.

1.3.2 Opdateringer efter anmeldelse

Hvis der foretages signifikante ændringer til den anmeldte løsning, kan 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, hvorefter NSIS Tilsynets registrering af løsningen kan blive opdateret. Den opdaterede anmeldelse med tilhørende revisionserklæring indsendes til NSIS Tilsynet senest 60 dage efter, at ændringen er sat i drift. Såfremt der er væsentlige revisionsbemærkninger til den idriftsatte løsning, skal disse udbedres senest 60 dage efter erklæringstidspunktet, hvorefter der sendes dokumentation for udbedring af forholdene til NSIS Tilsynet.

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, og efter eventuelle væsentlige revisionsbemærkninger er håndteret og dokumenteret over for Tilsynet.

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.

1.3.3 Håndtering af underleverandører

Det er meget udbredt, at organisationer anvender underleverandører til at håndtere systemer eller processer, der er underlagt krav i NSIS. I den forbindelse er det vigtigt i anmeldelsen klart at redegøre for, hvilke parter, der håndterer hvilke krav – samt sikre at alle dele er underlagt revision. Hvis underleverandørens 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 underleverandøren.

1.3.3.1 Revision efter helhedsmetoden

Hvis anmelder anvender underleverandører, kan anmelders erklæring udformes efter 'helhedsmetoden', hvor alle leverandører i kæden er omfattet af samme erklæring. Helhedsmetoden er en metode til håndtering af de ydelser, en underleverandør leverer, hvor underleverandørens beskrivelse af sit system omfatter arten af de ydelser, en underleverandør leverer, og hvor underleverandørens relevante kontrolmål og tilknyttede kontroller indgår i anmelderens beskrivelse af sit system og i omfanget af anmelders revisors opgave.

1.3.3.2 Revision efter partielmetoden

En anmelder kan alternativt beslutte at anvende partielmetoden for revision, hvor underleverandørens ydelser ikke direkte er omfattet af revisionen. Et eksempel på, hvor denne metode kan være hensigtsmæssig, er når underleverandøren fx er en driftsleverandør (fx en international cloudleverandør), der ikke kan levere en NSIS-specifik erklæring eller underlægges anmelderens (kundens) revisor - men i stedet kan levere en alternativ, erklæring for tilsvarende sikkerhedskrav udformet af egen revisor.

Det er således tilladt at henvise til (og hermed genanvende) en revisionserklæring fra en underleverandør med henblik på at dokumentere underleverandørens opfyldelse af krav i NSIS. Forudsætningen for genbrug af en eksisterende erklæring fra en underleverandør er, at der er tale om en ISAE 3000 revisionserklæring med høj grad af sikkerhed, hvor krav og kontrolmål er tilsvarende de specifikke krav i NSIS, som er relevante for underleverandørens ydelser (eksempelvis en driftsydelse). Dette kan være en generel eller løsningsspecifik erklæring, så længe kravene modsvarer NSIS[3]. Anmelderen skal ved genbrug af underleverandørerklæring eksplicit redegøre for, hvorledes opfyldelsen af hvert enkelt NSIS krav kan ses dokumenteret i den genbrugte erklæring. Anmelderens egenkontrol af underleverandørens erklæring skal derudover indgå i revisionen udført af den statsautoriserede revisor, og anmelders revisor skal i den forbindelse 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.

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 1.3.1 gælder således ikke for underleverandørers erklæringer.

[3] 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 statsautoriserede revisor.