Reviderbarhed af NIS2-overholdelse i Danmark

(Auditability of NIS2-compliance in Denmark)

Uddannelse: Cand.merc.aud.

Studerende / gruppe: Lasse Hamann

Vejleder: Hans Henrik Berthing

Indhold

Abstract

This thesis treats Danish NIS2-compliance as an audit problem. Obligations have to be translated into auditable criteria, evidence, and test procedures that support a repeatable and comparable audit. The method is document-based and relies on a fixed source-hierarchy. The thesis maps EU-legislation and Danish implementation-law, to official Danish guidelines and portal-workflows. Audit standards are used to structure the suitability of the criteria, the quality of the evidence and the logic of the reporting and conclusion (Chapter 2).

The main contribution is a repeatable transformation-chain: (Criteria - > Control objectives - > Evidence -> Test procedures -> Deviation rules), which is used to implement the Danish NIS2-obligation into testable objectives and expectations of the documentation (Chapter 2 & 4). The thesis identifies the Danish obligations, that are most relevant for IT-audit, for both essential and important entities, and demonstrates how portal-workflows (registration, incident-reporting on Virk, and authentication with MitID) creates timestamped evidence that can be archived and used for recreating the sequence of events (Chapter 3). Based on that, a Danish model for IT-audit for first-cycle audits in compliance with NIS2 is proposed, structured around cybersecurity risk-management measures, incident-handling, stepwise reporting, governance, and registration / traceability, with a deviation-model that distinguishes between provable non-compliance and scope limitations when sufficient evidence cannot be obtained (Chapter 4 & 5).

Because official guidelines and portal-workflows may change over time, freezing criteria and documenting those criteria by the date they are established are also treated as a control, to keep conclusions interpretable and comparable (Chapter 2 & 4). Finally, a comparison of selected member states, to identify useful measures to improve auditability, which can be used in Denmark, without changing the Danish legal criteria (Chapter 6).

1. Introduktion

1.1 Hvad specialet leverer

Det praktiske mål med specialet, er at gøre overholdelse af NIS2 til noget der kan vurderes og rapporteres omkring. Kapitel 2 fastlægger forskningsdesignet, kildehierarkiet og den kortlægningsmetode som bruges i hele specialet. Hvor forpligtelser omdannes til kontrolmål, der kobles til beviser, som kan testes via definerede procedurer og afvigelsesregler (se 2.3). Denne tilgang kræver både dokumentation for beviser, men også dokumentation for kriterier. Dokumentation for kriterier vil være gældende lovgivning, officielle vejledninger og workflows pr. en given dato, da disse kan ændres over tid (se 2.2 og 2.4). Kapitel 3-5 anvender metoden på danske NIS2-forpligtelser, med fokus på omfang og klassificering, portalbaseret registrering og hændelsesunderretning, governance og beviser.

Struktur:

- Et kildehierarki til fastfrysning af kriterier for erklæringsopgaver underlagt NIS2 (ikke kun begrænset til relevans for NIS2), hvor de officielle retningslinjer og værktøjer kan ændre sig under og mellem revisioner (se 2.2 og 2.4).
- En kortlægning fra de juridiske forpligtelser til afvigelsesregler, der muliggør sporbarhed og gentagelse af revisionshandlinger (se 2.3).
- Et dansk fundament for revisionsbeviser fra indberetningsportalen, herunder kopier / kvitteringer med referencenummer og tidsstempler, samt interne revisionsbeviser der understøtter de eksterne beviser (se kapitel 3).
- En sikkerhedsorienteret bevisdisciplin og afvigelsesregler, der adskiller beviselig manglende overholdelse fra begrænsninger i omfanget, og deres potentielle betydning for konklusionen (se kapitel 4).
- En dansk revisionsmodel med eksempler på procedurer (herunder start-til-slut genudførelse af hændelsesrapportering) der kan indarbejdes i et revisionsprogram (se kapitel 5).
- En oversigt der samler de tiltag fra udvalgte sammenligningslandes implementering og om nogen af disse med fordel kan implementeres i Danmark (se kapitel 6).

1.2 Revisionslogik anvendt i specialet

Den danske revisionsmodel er baseret på

1. Omfang og klassificering.
2. Portalbaseret udførelse af registrering og hændelsesunderretning.
3. Ledelsens godkendelse og tilsyn.

Beviser prioriterer pålidelige, eksternt- eller systemgenererede beviser og afvigelsesregler til at adskille påvist manglende overholdelse fra begrænsninger i omfang af beviser. Dette er særligt vigtigt for de forpligtelser der er omfattet af tidsfrister for bevidsthed og klassificering.

1.3 Forkortelser og definitioner

Tabel 1.1

Forkortelse / begreb	**Udfoldelse**	**Revisionsrelevant definition i dette speciale**
NIS2	Direktiv (EU) 2022/2555	EU's basis-kriterier, som indgår i kildehierarkiet og kortlægningen (Kapitel 2.2).
NIS2-loven	Dansk NIS2-lov (Lov nr. 434)	Bindende nationalt kriterielag (Kapitel 2.2).
BEK 620	Bekendtgørelse om kompetente myndigheder og obligatorisk digital kommunikation	Operationelt lag, der styrer obligatoriske digitale indsendelser og videresendelse (Kapitel 3.1).
SAMSIK	Styrelsen for Samfundssikkerhed	Tværsektorielt vejledningslag; hoster/koordinerer nationale incident-response-funktioner, som refereres i den danske vejledningspakke (Kapitel 3.1).
CSIRT	Computer Security Incident Response Team	Hændelseshåndteringsrolle; relevant for at bevare opfølgende korrespondance og beviser for teknisk koordinering (Kapitel 3.1).
Virk	Dansk selvbetjeningsportal	Obligatorisk indsendelseskanal til registrering og hændelsesindberetning; kvitteringer/kopier og tidsstempler understøtter revisionsbevis (Kapitel 3 og 5).
MitID	Dansk digital identifikation	Autentifikation i portal-workflows; understøtter bevis for autorisation ved indsendelser (Kapitel 3).
Digital Post	Dansk digital postkasse	Kvitteringskanal til at bekræfte portalindsendelser; understøtter test af rettidighed og sporbarhed (Kapitel 3).
ISAE 3000	Standard for erklæringsopgaver	Strukturerer kriterie-egnethed, vurdering af bevis og konklusionslogik (Kapitel 2 og 4).
ISA 500	Standard om revisionsbevis	Disciplin for tilstrækkeligt/egnet bevis og

		pålidelighed, brugt til at prioritere beviser (Kapitel 2 og 4).
ISAE 3402	Rapport om kontroller hos serviceorganisation	Leverandørbevis-input; kræver test af supplerende kontroller hos den regulerede enhed (Kapitel 4 og 5).
ISO 27001	Standard for informationssikkerhedsledelsessystem	Kontrolsprog, der mappes tilbage til juridiske kriterier; ikke en erstatning for juridiske kriterier (Kapitel 4).
COBIT	Framework for IT-governance	Struktursprog for governance og kontrolmål (Kapitel 4).
COSO	Framework for intern kontrol	Struktursprog for intern kontrol og rapporteringslogik (Kapitel 4).
Kildehierarki	Specialets begreb	Versioneret sæt af kilder, der definerer kriterier for en periode (Kapitel 2.2).
Kriteriefrysning	Specialets begreb	Fastlåsning af kriteriestakken pr. en dato og bevaring af snapshots for fortolkelighed over tid (Kapitel 2.4 og 4.6).
Kontrolmål	Specialets begreb	Revisionsneutral formulering afledt af et krav (Kapitel 2.3).
Afvigelsesregel	Specialets begreb	Regel for klassifikation af afvigelser og konsekvens for konklusion (Kapitel 2.3 og 4.7).
Manglende overholdelse	Specialets begreb	Krav/kontrolmål er ikke opfyldt mod de fastfrosne kriterier (Kapitel 4.7).
Omfangsbegrænsning	Specialets begreb	Utilstrækkeligt egnet bevis efter alternative handlinger (Kapitel 4.7).
Kompetent myndighed	Sektor-tilsynsmyndighed	Myndighed der modtager routede indsendelser og fører tilsyn; relevant for evidens-routing og bevaret korrespondance (Kapitel 3).
Afvigelsesmodel	Specialets begreb	Klassifikation, der omdanner afvigelser og omfangsbegrænsninger til konklusionspåvirkning (Kapitel 4.7).
Væsentlighed	Specialets begreb	Vurdering af om afvigelser/begrænsninger kan påvirke de tiltænkte brugere;

		styrer konklusionsvalg (Kapitel 4.5).
Trinvis rapportering	Specialets begreb	Hændelsesrapportering testet mod kendskabstidspunkt og indsendelsesbeviser (Kapitel 3 og 5).
SIEM	Security Information and Event Management	Systemkilde til alarmer og bevis for tidspunkt for bevidsthed, brugt i start-til-slut hændelsestest (Kapitel 5).
Kriterieregister	Specialets begreb	Versioneret liste over kriterier, kontrolmål, beviser og test, der bruges i en opgave (Kapitel 5).

1.4 Baggrund og motivation

NIS2 indfører cybersikkerhedsforpligtelser på EU-niveau, for virksomheder der vurderes som væsentlige eller vigtige. I Danmark skal disse forpligtelser dokumenteres og evalueres over tid. Ud fra et revisionsmæssigt perspektiv er den primære udfordring ikke kun om der findes foranstaltninger, men også om de vurderes at være tilstrækkelige til at overholde de juridiske forpligtelser ud fra et givent sæt kriterier, kan dokumenteres og om revisionstest er gentagelige.

Forpligtelser omfattet af tidsfrister (trinvis underretning / rapportering om hændelser), gør dokumentation af alt lige fra beslutningsgrundlag for registrering (klassificering og omfang), til bevidsthed om hændelser, hændelsesforløbet og afhjælpende foranstaltninger til centrale revisionsbeviser.

I de første revisioner vil driftshistorikken være begrænset. Mulighederne for revision kan dog stadig forbedres, ved at udforme rutiner for indsamling og opbevaring af bevismateriale, dokumentation for beslutningsgrundlag, fastlæggelse af kriterier for hver revision (og specificer ændringer fra version til version).

1.5 Problemformulering

Hvordan kan de NIS2-forpligtelser som dikteres på EU-niveau, i Danmark omdannes til faste, reviderbare kriterier / kontrolmål, beviser og afvigelsesregler, så revision kan gennemføres konsistent og gentageligt, på tværs af de omfattede virksomheder og revisioner, når de officielle vejledninger og portal-workflows ændres over tid?

1.6 Undersøgelsesspørgsmål

U1: Hvilke krav i NIS2 er mest relevante for IT-revisionen og hvordan kan IT-revisionen struktureres til at vurdere de krav til risikostyring, hændelseshåndtering, governance og rapportering, som NIS2 stiller?

U2: Hvordan kan internationale standarder og frameworks som ISA 500, ISAE 3000/3402, ISO 27001, COBIT og COSO, anvendes som revisionskriterier for NIS2-overholdelse, og hvilke udfordringer skaber forsinket national implementering for planlægning, væsentlighedsvurdering og bevisindsamling for IT-revisionen?

U3: Hvilke konkrete tiltag har Belgien, Tyskland, Rumænien, Slovakiet og Ungarn valgt i deres implementering af NIS2, som Danmark kan drage nytte af?

Målet er at udarbejde en revisionsmodel, der understøtter planlægning, indsamling af beviser og udarbejdelse af konklusioner. I kapitel 2-5 udvikles de danske kriterier, bevisgrundlag, samt revisionsmodellens struktur, herunder eksempler på procedurer der kan omdannes til dokumentation. Kapitel 6 sammenligner udvalgte landes tiltag ved implementeringen, for at udlede tiltag og forbedringer til den danske implementering.

1.7 Omfang og afgrænsninger

I specialet beskrives reviderbarhed som det omfang en forpligtelse kan omdannes til:

1. Et klart sæt kriterier eller kontrolmål.
2. Beviser der kan henføres til virksomheden og den relevante periode.
3. Afvigelsesregler der understøtter ensartet arbejdsgang for vurdering og rapportering, samt at kriterierne fastfryses pr. en given dato ved at dokumentere lovtekster, vejledninger og portal-workflows pr denne dato.

Specialet måler ikke egentlige resultater, da der grundet status på implementering af NIS2, ikke er tilstrækkeligt datagrundlag for dette. NIS2 er en bred lov, men fokuspunktet (dog ikke begrænset til) vil være lovens kapitel 4: ” CHAPTER IV, CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS”, og herunder Artikel 20 ”Governance”, Artikel 21 ”Cybersecurity risk-management measures”, Artikel 22 ”Union-level coordinated security risk assessments of critical supply chains”, og Artikel 23 “Reporting obligations” [1].

2. Metode

Dette kapitel definerer den anvendte metode til at fortolke NIS2 forpligtelser til reviderbare kriterier, revisionsmål og anvendelige IT-revisionsprocedurer [1].

Dette understøtter U1, ved at specificere sammenhængen mellem de lovmæssige krav, til de praktiske revisionsprocedurer, som kan anvendes på tværs af de forskellige revisioner.

U2 understøttes ved at forklare hvordan ISAE 3000 og ISA 500 strukturerer de kriterier for egnethed, bevisernes kvalitet og rapporteringslogikken i overensstemmelse med NIS2. [2] [3].

U3 understøttes ved at forklare en måde at bruge sammenligningslandenes implementeringsproces til at sammenligne revisionsmekanismer, uden at ændre på de danske kriterier. [1] [4].

2.1 Forskningsdesign

Forskningsdesign er primært baseret på sekundær empiri, fra juridiske dokumenter, artikler og øvrige ekspert-udtalelser.

Specialets problemstilling er ikke at måle selve resultaterne af IT-sikkerhed, men at gøre overholdelsen af NIS2 reviderbar. Kravene skal udtrykkes som kriterier der er forståelige nok til at kunne testes og rapporteres, og være præcist knyttet til de beviser (ud fra revisionsmål), der kan opbevares og gentages på tværs af revisioner [2] [3].

Den dokumentbaserede tilgang er passende, da de danske lag i implementeringen af NIS2 er offentligt tilgængelige lovtekster. NIS2 på EU-niveau [1], Danmarks gennemførselslov på Retsinformation.dk [4], og danske implementeringsvejledninger og workflows, som er offentliggjort af SAMSIK, Virk.dk, Digitaliseringsstyrelsen [5] [6] [7] [8] [9] [10] [11].

Kapitlets mål er derfor en gennemgang af strukturen med kriterier, beviser og revisionsmodel, der kan genbruges på tværs af revisionsopgaver og opdateret gennem en kontrolleret versionshistorik, i stedet for at blive fortolket ad-hoc [2].

Metoden er bundet i sikkerhedslogik. ISAE 3000 kræver passende kriterier (relevante, fuldstændige, pålidelige, neutrale og forståelige), samt tilstrækkelige passende beviser, til at underbygge konklusionen, hvilket gør definitionen af kriterierne og planlægningen af beviserne sammenhængende med forskningsdesignet [2].

ISA 500 definerer regler for evaluering af om beviser er tilstrækkelige og pålidelige, som anvendes til at prioritere de objektive og systemgenererede beviser [3].

2.2 Kildehierarki

Specialet anvender et fast hierarki, for at undgå afvigelser fra de fastlagte kriterier, samt sikre at kriterierne kan forsvares i sikkerhedsrapporteringen [2].

1. EU's gældende lovgivning. Udgangspunktet er direktiv (EU) 2022/2555 (NIS2), som er offentliggjort på EUR-Lex [1].

2. Gældende Dansk lov. Den Danske lov er Lov nr. 434 af 06/05-2025 (NIS2-loven), som er offentliggjort på Retsinformation.dk [4]
3. Officiel Danske vejledninger og portaler. SAMSIK-vejledningen anvendes fortolkningsforslag på tværs af de forskellige brancher. Virk- og Digitaliseringsstyrelsens vejledninger og arbejdsgange, anvendes til at definere: datafelter, indsendelse og de minimumskrav der er til bevis for indsendelse. Gennemgange som kan bruges som revisionsbevis [5] [6] [7] [8] [9] [10] [11].
4. Internationale standarder (sikkerhed og bevisindsamling). ISAE 3000 og ISA 500, anvendes til at strukturere kriterier, vurdering af beviser og rapporteringen. De anvendes ikke til at vurdere selve compliance-kriterier, da det er defineret af selve NIS2 [2] [3].
5. Sammenligningslandenes primære kilder. Disse er begrænset til oversættelser af officielle lovtekster og portaler/vejledninger, til at identificere tiltag, som Danmark kan lære af.

Integrationsstrategi:

Kildesættet er bevidst snævert. En kilde er inkluderet, når den er 1) er standardiseret for forpligtelsen (loven), 2) er den officielle danske anvendelse af hvordan en forpligtelse er udført eller dokumenteret (vejledning / portal), eller 3) definerer krav til sikkerhed og bevisdokumentation, som kan konkludere præcist hvordan begrænsninger skal rapporteres [1] [4] + [5] [6] [7] [8] [9] [10] [11] [2] [3].

Ikke-autoriseret materiale (artikler af konsulenter, blog-indlæg og øvrige ikke-officielle kilder) er udelukket fra at blive anvendt i kriterierne, og skal hvis anvendt, udelukkende anvendes som hjælp til at navigere i søgningen i materialet fra kilderne i de 5 ovennævnte hierarkier [1] [4] [2].

Konfliktregel:

Hvis kilder vurderes at være i konflikt med hinanden, vil der altid søges opad i hierarkiet. Altså en bindende lov vil derfor altid tilsidesætte en vejledning [1] [4] [5]. Indenfor den danske lovgivning vil den tilsidesætte arbejdsgangespecifikke instruktioner, når de definerer dataindsamling, bevismaterialer, eller bevisgennemgang, der er krævet for at gennemføre registrering eller hændelsesrapportering (f.eks. Virk.dk vejledningerne til indberetning.) [7] [8] [11].

Sikkerhedsstandarder tilsidesætter ikke love. De anvendes til at implementere praktisk-anvendelige metoder til hvordan man vurderer og rapporterer (kriteriernes egnethed, tilstrækkelighed) [2] [3].

2.3 Metode for kortlægning

Den centrale metode er en transformationskæde som er gentagelig: Kriterier -> Kontrolmål -> Beviser -> Testprocedurer -> Afvigelsesregler [2] [3].

Krav: Kortlægningen er et krav som er bundet i én præcis placering i én kilde: et afsnit i NIS2-lovgivningen (EU) [1], en bestemmelse i den danske lov [4], eller en officiel instruktion af arbejdsgange som definerer obligatoriske datafelter og forventninger til bevisindsendelse [7] [8] [11].

Kontrolmål: Hvert krav omformuleres til et revisionsneutralt mål (hvad der skal være sandt), som kan evalueres, uden behov for at indbygge en specifik teknisk løsning i forklaringen [2].

Bevismateriale: Bevismateriale defineres som konkrete gennemgange, der kan opbevares og undersøges gentagende gange. Metoden prioriterer 1) eksternt-generede outputs, som f.eks. kopier af indsendte formularer og kvitteringer, som det anbefales i Virk-vejledningerne [7] [8] og 2) systemgenererede daterede (dato og klokkeslæt) registreringer, som kan anvendes til at understøtte det der er blevet indsendt [3].

Testprocedurer: For hvert revisionsmål skal der formuleres standardrevisionsprocedurer (forespørgsel, undersøgelser, observation og gentagelse) som er tilpasset formålet med revisionsopgaven (intern revision eller uafhængig gennemgang fra ekstern part) [2] [3].

Afvigelsesregel: Hver post skal indeholde en særlig regel for hvad der definerer en afvigelse, herunder hvornår manglende beviser resulterer i en begrænsning af revisionsomfanget (utilstrækkelige relevante beviser), fremfor en revisionskonklusion i overensstemmelse / compliance [2] [3].

Nedenstående tabel 2.1 viser de mindstekrav, der er registeret under hver kortlægningspost. Disse felter er udformet til at understøtte: sporbarhed, konsistente bevisanmodninger og genudførelse iht. Til de fastsatte kriterier [2].

Tabel 2.1

Post	**Mindstekrav**
Kilde	Dokument + afsnit + version/dato
Anvendelighed	Klassifikation og omfang, hvorvidt arbejdsgangen er relevant.
Beskrivelse af krav	Objektiv beskrivelse af hvad der kræves.
Kontrolmål	Hvad der skal være sandt, for at opfylde kravet.
Bevismaterialer	Primære outputs fra systemer, herunder foretrukket filformat, metadata.
Testprocedurer	Forespørgsel, gennemgang, observation, genudførelse. Herunder tilgang til udtagning af stikprøver.
Afvigelsesregel	Hvad der udgør en manglende overholdelse vs. begrænsning af omfanget, samt eskaleringsstrategi (f.eks. udtagelse af yderligere stikprøver).
Indeksering af arbejdspapir	Hvor revisionsbeviserne opbevares, indekseres og adgang-/skrivekontrol for revisionsnoter.

Praktisk anvendelse: Kortlægningen er det redskab der bruges til at strukturere arbejdsgange, for at kunne udarbejde 1) et kontrollerbart sæt kriterier, 2) et beviskatalog/database og 3) et genanvendeligt revisionsprogram.

I Danmark vil der blive skælnet mellem de juridiske krav (NIS2-loven på EU og Dansk niveau), og de officielle retningslinjer og arbejdsgange fra vejledninger.

2.4 Kriterier og versionskontrol

Fordi de danske retningslinjer og vejledninger kan ændres over tid, anvender specialet et princip om kriteriefrysning. Alle anvendte kilder er derfor dateret pr. 21. december 2025 eller tidligere.

Der er gennem skrivningen både gået tilbage til eksisterende kilder, for at finde ændringer. Hvilket har resulteret i løbende ændring af tilgangen til specialet, men det har ikke været muligt at finde specifikke ændringslogge for at de udvalgte kilder.

ENISA-udgivelser er anvendt til at fremlægge konkrete eksempler på implementering og bevistyper, men ligesom øvrige vejledninger og portaler, så opfylder de i sig selv ikke det juridiske kriterie, og der skal derfor altid henvises til gældende lovgivning (EU og Danmark) [1] [4] [12].

2.5 Kvalitative overvejelser og begrænsninger

Sporbarhed: Metoden prioriterer sporbarhed fra ethvert testresultat tilbage til en specifik kilde og frem til defineret mål og/eller afvigelsesregel [1] [4] [2] [3].

Gentagelighed; Kortlægningen, indekseringen af beviser og tidsstemplingen har til formål at gøre gentagelse af revisionen mulig, for at en anden revisor skal kunne anvende de samme revisionskriterier, på den samme data og nå frem til den samme konklusion [2] [3].

Beviskvalitet: Revisionsbeviser skal følge ISA 500. Bevisets pålidelighed skal underbygges af at være system- eller eksternt genereret, da man derfor opnår højere objektivitet, frem for individuelle subjektive fortolkninger [3].

Begrænsninger: Bevisgrundlaget er udelukkende dokumentbaseret. Dette kan fastlægge hvad der kræves og hvilke beviser der bør indsamles, men det kan ikke anvendes til at fastlægge hvordan de danske myndigheder vil håndhæve kravene i fremtiden.

Internet-kilder ændres over tid. Lovtekster vil for det meste være dateret og specificeret med version, mens portaler og interaktive vejledninger ændres løbende, oftest uden mulighed for at gå tilbage til tidligere versioner, hvorfor disse er revurderet løbende.

3. Danske NIS2-krav

Kapitlets formål og sammenhæng med U1. Dette kapitel fortolker den danske NIS2-implementering ift. revisionsmæssige krav, bevismateriale og overvejelser om gentagelighed af tests.

Det understøtter U1, ved at præcisere kravene i testbare omfang (Indsamling, registrering, governance, målinger og rapportering af hændelser) og ved at foreslå et minimumssæt af revisionsbeviser til den første revision under NIS2-overholdelse.

U2 understøttes ved at kortlægge hvilke forventninger der følger direkte af EU-lovgivningen i forhold til den Danske lov.

3.1 Dansk metode for implementering

En IT-revision af NIS2-overholdelse bør tilgås i lag, jf. det i kapitel 2 specificerede kildehierarki.

Først kommer EU-loven, derefter den danske gennemførelse, og til sidst de praktiske krav som er udformet af de officielle vejledninger [1] [4] [13] [5] [6] [14].

EU's grundlag er direktiv (EU) 2022/2555 (NIS2), der fastlægger minimumskrav til governance, IT-sikkerhedsforanstaltninger og forpligtelser til indberetning af hændelser for væsentlige og vigtige virksomheder [1].

Danmark overholder disse forpligtelser, gennem den danske NIS2-lov, der fastlægger danske definitioner, regler, minimumskrav, registreringsforpligtelser og krav til indberetning af væsentlige hændelser [4].

Bekendtgørelse BEK nr. 620 af 2. juni 2025 fordeler ansvaret og fastlægger hvordan tilsyn mellem de kompetente myndigheder og hvordan enhederne skal kommunikere med de pågældende myndigheder [13].

Bekendtgørelsen udpeger de kompetente myndigheder efter sektor (herunder Digitaliseringsstyrelsen, for flere kategorier af digital infrastruktur og udbydere af digitale produkter/services). Her kræves at registreringer og hændelsesindberetninger i henhold til loven, skal indsendes digitalt via den på virk.dk tilgængelige selvbetjeningsløsning, som der er adgang til med MitID [13].

Portalworkflows som virk.dk er derfor en vigtig del af det reviderbare kontrolmiljø. De indberetninger der bliver foretaget, på baggrund af de vejledninger der er tilgængelige, sammen med tidsstempler og referencenummer, vil være tilgængelige for download [7] [11]. Digitaliseringsstyrelsens vejledning præciserer yderligere at den indberettende enhed, vil modtage en kvittering på skærmen og via Digital Post, som vi kender det fra så mange andre handlinger på virk.dk [9].

BEK nr. 620 definerer det juridiske modtagelsestidspunkt som det tidspunkt hvor det er tilgængeligt for modtageren, ift. tidsstempel og test af overholdelse af tidsfrister [13].

Dokumenthåndtering / bevisføring er en integreret del af disse workflows. Virk vejledninger forklarer at indberetningerne sendes til Erhvervsstyrelsen og automatisk videresendes til relevante myndigheder på baggrund af den angivne sektor [7] [8]. Jf Digitaliseringsstyrelsens vejledning forklares det at hændelsesindberetninger indsendt via Virk, bliver videresendt til relevante sektormyndigheder [10].

SAMSIK's NIS2 side/portal linker hændelsesrapportering til Virk, samt at indberetninger håndteres af den nationale CSIRT-funktion [5]. Ud fra et revisionsmæssigt synspunkt, betyder det at planlægningen skal tage højde for korrekt bevisindsamling, både for de indledningsvise indberetninger og efterfølgende korrespondance mellem de ovennævnte kompetente myndigheder (sektor-specifikt), da denne korrespondance kan indeholde vigtig information ift. klarlægning af hændelsen [5] [10].

3.2 Omfang og klassificering, som den første kontrol

Omfang og klassificering er den første reviderbare kontrol, da alle efterfølgende krav afhænger af hvorvidt en virksomhed er omfattet af lovgivningen og hvilken del af loven, ud fra den sektor-opdelte klassificering [1] [4]. Den danske lov definerer væsentlige enheder hovedsageligt som dem der hører under bilag 1 og enten har 250 ansatte eller omsætning over 50m EUR og en balance på over 43m EUR, dog med særlige regler for offentlige enheder og dem som menes at være væsentlige uanset størrelse (herunder nogle udbydere af cybersikkerhed) [4]. Efter væsentlige, kommer vigtige enheder og de defineres som 50 ansatte eller omsætning og balance over 10m EUR, hvor der så er yderligere betingelserne for at blive omfattet af loven [4].

Klassificeringen af virksomheden skal være dokumenteret, da den danske registreringsworkflow kræver en særlig erklæring om væsentlig/vigtig-status, sammen med de regnskabsmæssige størrelsesgrænser og oplysninger om hvor vidt de er overskredet [7]. Virk's registreringsvejledning angiver også at den valgte sektor kan ændres, på baggrund af både virksomhedens aktiviteter og en eventuel ændring af lovgivningen. Dette indebærer at virksomhederne har løbende krav om at holde deres klassificering og sektorvalg ajourført [7].

Ift. revisionsplanlægningen er klassificeringen vigtig, da NIS2 har forskellige krav til tilsyn, på baggrund heraf. Væsentlige enheder er underlagt en mere systematisk tilsynsmetode, hvorimod vigtige enheder generelt kun bliver underlagt tilsyn reaktivt (efter en hændelse, eller på baggrund af øvrige beviser/indikationer) [1]. Det betyder at en fejlklassificering udgør en reel risiko for både overholdelse af loven og den eventuelle bevisbyrde. De underlagte virksomheder skal derfor kunne påvise hvordan de er kommet frem til deres regnskabstal ift. størrelsesgrænserne samt hvordan valgte sektor er ajourført i forbindelse med løbende organisationsmæssige ændringer [1] [4].

En oversigt, klargjort til revision bør indeholde følgende: kortlægning af de udbudte tjenester i forhold til bilagene, beregningsgrundlaget for overskredne / ikke-overskredne regnskabsmæssige størrelsesgrænser, samt underbygning af det/de foretagne sektorvalg ved registreringen (særligt vigtigt for virksomheder der opererer på tværs af flere sektorer, både væsentlige og uvæsentlige, da der skal koordineres med flere kompetente myndigheder) [4] [13] [7].

3.3 Registreringsforpligtelser og bevismateriale

Registreringen er både en juridisk forpligtelse og et centralt bevismateriale ifm. revisionen, fordi Danmark implementerer NIS2-registreringsforpligelsen, som er lovbestemt, via online-portalen på virk.dk [1] [4] [13] [6] [9]. På EU-niveau kræves det at medlemsstaterne udformer en liste over væsentlige og vigtige enheder, samt fastsætter hvilke specifikke oplysninger de skal indsende og ajourføre, for at denne liste overordnet set kan være korrekt (med de underlagte virksomheder) [1]. Den danske lov implementerer disse krav gennem

påkrævede datafelter ved registreringen, således at registreringen ikke kan fuldføres, hvis disse felter er tomme. Ligeledes vil tidsfrister variere efter enhedstype og/eller sektor [4].

For visse kategorier af digitale ydelser, som opererer på tværs af landegrænser, kræver loven at registreringen foretages inden for 3 måneder, efter virksomheden er blevet omfattet, og efterfølgende ændringer skal ajourføres i registreringen inden for 3 måneder efter de er trådt i kraft jf § 9 [4]. De generelle regler specificerer dog at væsentlige/vigtige enheder kræver registrering allerede inden for 2 uger efter de er omfattet og også 2 ugers frist for ajourføring af relevante ændringer til registreringen jf. § 10 [4]. Vejledningsportalen på virk.dk angiver den indledningsvise tidsfrist som 1. oktober 2025 (§ 33 stk. 3), og så de ovennævnte 2 uger, for dem som først bliver omfattet efter 1. oktober 2025, samt at ændringer skal rapporteres inden for 3 måneder, ved at indsende en ny registreringsformular [6]. For revisionskriterier er de lovbestemte tidsfrister de bindende, så det kræver også at portalens indbyggede tidsfrister testes ift. virksomhedens faktiske tidsfrister jf. lovgivningen [4] [6].

Virk-registreringsvejledningen indeholder en liste over de oplysninger der som minimum indsamles (herunder CVR-nummer, virksomhedsidentifikation, kontaktoplysninger, IP-adresse sektorvalg og klassificering) samt en advarsel om ikke at angive fortrolige oplysninger. Det nævnes også her at Erhvervsstyrelsen vil videresende de indsendte registreringer (ligesom der gøres med indberetning af hændelser) til de relevante kompetente myndigheder, på baggrund af valget af sektor, samt anbefaler at der downloades en kvittering efter fuldført registrering, som desuden fremsendes til virksomhedens digital postkasse [7] [9].

Fra et revisionsperspektiv bør registreringen behandles som en kontrol, som skal fungere uafbrudt, ikke som engangskontrol. Det kræves derfor at der udarbejdes et system der kan opdage når registreringsoplysningerne bliver forældede (både grundet virksomhedsspecifikke ændringer og lovgivningsmæssige ændringer eller fortolkninger), og dermed sikre rettidig ajourføring af registreringen [4] [7]. Revisionsbeviset for dette system vil typisk være: ændringslog, internt ejerskab for registreringen, samt bevis for at relevante opdateringer er indsendt (kvittering med referencenummer).

En praktisk metode til at revidere, kan være at behandle registreringen som en række påstande:

- Fuldstændighed (alle omfattede juridiske enheder er registreret).
- Nøjagtighed (korrekt kortlægning og aktiviteter til valg af sektor).
- Feltnøjagtighed (kontakt- og IP-oplysninger)
- Rettidighed (tidsfrist for registrering og ajourføring).
- Integritet / autorisation (autorisation med MitID og opbevaring af kvittering som bevis). [4] [13] [7].

Nedenstående tabel 3.1, viser de mindstekrav der er til revisionspåstande og bevismateriale ifm. registrering:

Tabel 3.1

Påstand	**Bevis**	**Revisionshandling**
Fuldstændighed	Omfangsmemo, liste over enheder, registreringer, kvitteringer	Gentag afgrænsning, afstem omfanget af enhederne med indsendelser
Nøjagtighed	Klassifikationsgrundlag, valg af sektor/enhedstype	Bekræft klassifikation ved at spore den valgte type til tjeneste indenfor de angivne kategorier i vejledningen
Feltnøjagtighed	Register over kontaktoplysninger og udbudte tjenester	Sammenhold de udfyldte felter med systemer og kontroller ændringsloggen.
Rettidighed	Tidsstempler på indsendelseskvitteringer	Sammenhold tidspunkter med de juridiske tidsfrister
Integritet	MitID ved login, referencenummer på kvittering, opbevaring af kopi	Bekræft at der faktisk er indberettet og at der opbevares en downloadet kvittering/kopi

Det juridiske grundlag for obligatoriske datafelter og tidsfrister er den danske lovgivning. De revisionsmæssige bevismaterialer er defineret af Virk og Digitaliseringsstyrelsen [4] [7] [9].

3.4 Governance og krav til involvering

NIS2 gør ledelsens involvering til reviderbare krav. Direktivet kræver at ledelsen godkender de foranstaltninger der er udarbejdet til styring af cybersikkerhedsrisici, overvåger implementering heraf og er korrekt uddannet (kurser mv.) til at varetage denne funktion, så der er mulighed for at placere et ansvar for eventuelle overtrædelser [1].

Den danske lov indeholder de samme forpligtelser og krav ift. at følge styringen og uddannelse, samt at ledelsen kan holdes ansvarlig i henhold til gældende dansk lovgivning [4].

Forventningerne til en revision bør derfor omfatte:

- Dokumentation for formel godkendelse af foranstaltninger og væsentlige ændringer.
- Dokumentation for aktivt tilsyn (beslutninger, rapportering, og opfølgning heraf).
- Dokumentation for at ledelsen og væsentlige nøglepersoner i virksomheden har gennemgået tilstrækkelig uddannelse for at varetage deres ansvar [1] [4].

SAMSIK-vejledningen præciserer at betragtningen af ledelsen kan variere alt efter lov og de forskellige offentlige myndigheder, hvorfor revisionsomfanget bør dokumentere hvem i virksomheden der er ansvarlig for hvad og hvorfor de skal betragtes som ledelsesorgan og dermed ansvarlig [15].

Typiske kontrolbeviser vil omfatte, men ikke være begrænset til:

- Ledelsesreferater og godkendelse af politikker.
- Beslutninger om risikoovertagelse, som forklarer hvorfor kontrollerne er hensigtsmæssige og tilstrækkelige.
- Periodiske rapporteringer om cybersikkerhed, samt dokumentation for gennemført uddannelse af relevante medarbejdere og ledelsen [1] [4].

En praktisk tilgang til revisionen, kan være at teste governance, både som design (er governance-modellen udarbejdet så den tildeler ansvar og eskaleringsforanstaltninger, krævet af loven) og operationelt (anvender ledelsen den udarbejdede model i deres daglige virke, f.eks. ved at gennemgå hændelser, godkende foranstaltninger og reagere på eventuelle fejl i kontrollen) [1] [4].

3.5 Cybersikkerhed: Risikostyring som revisionsområde

Både NIS2(EU) og den danske lov kræver at der er passende og proportionelle, tekniske, operationelle og organisatoriske foranstaltninger, til at kunne styre risici for netværks- og informationssystemer der anvendes til at levere serviceydelser [1] [4]. Direktivet og loven angiver de kategorier af minimumsforanstaltninger, der omfatter politikker og risikoanalyse, hændelseshåndtering, kontinuitet, sikring af forsyningskæden, sikker udvikling og håndtering af sårbarheder, effektivitetsvurdering, uddannelse, kryptering, adgangskontrol og sikker kommunikation [1] [4]. Den danske lov definerer disse kategorier som foranstaltninger til at forebygge potentielle hændelser og minimere deres indvirkning på virksomhedens drift [4].

SAMSIK's implementeringsvejledning opdeler den lovpligtige liste af minimumsforanstaltninger i praktiske emner og bevistyper, og fastslår at vurderingen om virksomheden agerer i overensstemmelse med de krav, vurderes af den relevante myndighed (sektorbestemt) [15].

For visse virksomheder som leverer digitale-ydelser, har EU-kommissionen tilføjet yderligere tekniske krav på EU-niveau (EU 2024/2690), som præciserer yderligere hvornår hvilke hændelser er væsentlige. Digitaliseringsstyrelsen påpeger i deres vejledning, at denne EU-forordning supplerer definitionen af væsentlige hændelser for den digitale sektor [10] [16].

For at gøre "passende og proportionelle" reviderbart, skal hvert kontrolområde have en dokumenteret begrundelse knyttet til kritiske tjenester, definerede bevismaterialer, og gentagelige tests med regler for eventuelle afvigelser [1] [4] [15]. Nedenstående kontrolområder er i overensstemmelse med de minimumsforanstaltninger i den danske lov og afspejler i al almindelighed en generel revisionsstruktur.

- **Identitets- og adgangskontrol (IAM).** Minimumsforanstaltninger omfatter adgangskontrols politikker (også HR-sikkerhed) og multifaktor-autentificering (MFA) [1] [4] [15].
    - Beviser:
        - Adgangskontrolpolitik og procedurer for tildeling/flytning/afmelding af adgange, styring af privilegeret adgang (udover det normale for den pågældende rolle) og gennemgang af beviser.
        - Bevis for MFA-opsætning for fjernadgang og administrator-rettigheder, herunder dokumenterede undtagelser.

        - Review af adgangslogge for kritiske systemer, herunder afhjælpning af fundne problemer.
    - Forslag til test:
        - Stikprøve af brugere og administrator og kontroller at tildeling/flytning/afmelding af adgange er sket rettidigt på tværs af væsentlige systemer.
        - Kontroller håndhævelse af MFA-politikker og validere undtagelser iht. risikobaserede godkendelser og overvågning.
        - Kontroller privilegerede adgange og opfølgning på om de bliver afmeldt korrekt og rettidigt.
- **Sårbarheds- og opdateringsstyring.** Minimumsforanstaltninger omfatter håndtering af sårbarheder og sikker vedligeholdelse/udvikling af systemer [1] [4] [15].
    - Beviser:
        - Procedure for sårbarhedsstyring og bevis for afhjælpning.
        - Opdaterings-/ændringsregister for kritiske systemer, og vurdering med opfølgende handlinger.
        - Definerede grundkonfigurationer for centrale systemer og bevis for afvigelsesdækning/korrektion, hvor det anvendes.
    - Forslag til test:
        - Stikprøvetest på kritiske fund og spore afhjælpningen heraf, eller dokumenteret begrundelse for ikke at afhjælpe.
        - Kontroller om afhjælpningen har været rettidig og eskaleret til de rette personer / instanser, for de systemer der påvirker leverancen af kritiske tjenester.
        - Vurder om sårbarhedsoplysninger fremgår af klassificering af hændelser, når der er mistanke om udnyttelse heraf.

- **Overvågnings- lognings- og opdagelsesevne.** De danske retningslinjer trækker tråde fra håndtering af hændelse til logning/overvågning og logbeskyttelse [15].
    - Beviser:
        - Lognings-/overvågningsprocedurer (dækning, opbevaring og dokumentintegritet) samt plan for håndtering af hændelser (SIEM).
        - Alarmudslag, der viser klassificering af hændelse og vurdering for om der skal eskaleres, samt efterfølgende overvågning.
        - Bevis for adgangsbegrænsning (ikke alle skal kunne se) og beskyttelse mod at ændre den (manipulation).
    - Forslag til test:
        - Gentag / rekonstruer udvalgte scenarier/ hændelser og vurder om de tilknyttede beviser understøtter at der er foretaget rettidige og korrekte beslutninger.
        - Kontroller at loggen er fuldstændig med tidsstempel og præcis beskrivelse af hændelser, til brug for en eventuel rekonstruktion af scenariet.
        - Udvælg stikprøver af hændelser og vurder om eskalering og afslutning var rettidig og veldokumenteret.

- **Fortsat drift (BC), beredskab (DR), krisehåndtering.** Minimumsforanstaltninger omfatter BC/DR, sikkerhedskopiering og gendannelse og krisehåndtering [1] [4] [15].
    - Beviser:

        - BC/DR-planer for væsentlige systemer og test af systemer for sikkerhedskopi og gendannelse.
        - Øvelse af hændelser, protokoller herfra og dokumenterede efterfølgende forbedringer.
        - Dokumenterede roller, eskaleringsplaner, beslutningsansvar tilknyttet rapportering af hændelser.
    - Forslag til test:
        - Kontroller kritiske tjenester og bekræft om den udarbejdede plan er fyldestgørende.
        - Gennemgå tidligere, dokumenterede øvelser og bekræft om forslag til forbedringer er implementeret.
        - Kontroller om kriseprocedurer understøtter de tilknyttede rapporteringstidsfrister (opdagelse, 24 timer, 72 timer).

- **Leverandørstyring (SCM), outsourcing og indkøbsprocesser.** Minimumsforanstaltninger omfatter sikkerhed i forsyningskæden og eventuelle kontraktmæssige sikkerheder [1] [4] [15].
    - Beviser:
        - Risikovurdering af kritiske leverandører og klausuler i kontrakten (krav til sikkerhed, revision mv.).
        - Dokumenterede gennemgange af leverandørovervågning og opfølgninger.
        - Dokumentation for at kritiske leverandørers forpligtelser, understøtter den indkøbende virksomheds egne.
    - Forslag til test:
        - Udtag stikprøver af kritiske leverandører og kontroller om kontraktuelle vilkår understøtter virksomhedens egne rapporteringsfrister og bevisbehov.
        - Vurder om overvågning af kritiske leverandører sker systematisk, risikobaseret og der er tilknyttet afhjælpende foranstaltninger i tilfælde af en hændelse.
        - Gennemgå en dokumenteret hændelse med en leverandør og vurder om den interne eskalering har fulgt planen.

- **Sikker udvikling, ændringsstyring og konfiguration.** Minimumsforanstaltninger omfatter sikkerhed i forbindelse med anskaffelse/udvikling/vedligeholdelse samt håndtering af sårbarheder [1] [4] [15].
    - Beviser:
        - Bevis for sikkerhedstest / SDLC af ændringer der påvirker kritiske tjenester, godkendelse af ændringer og kontroller ved nødændringer.
        - Bevis for håndteringer af sårbarheder til tilknyttede respons og opdatering/patch af fejlen.
        - Kontrol af funktionsadskillelse i udvikling og implementering.
    - Forslag til test:
        - Gennemgå tidligere opdateringer og om der er tilknyttet ændringslog, sikkerhedstest og godkendelser, forud for implementering.
        - Kontrollér hvordan sårbarheder er dokumenteret håndteret, fra opdagelse til afhjælpning.
        - Undersøg om eventuelle nødændringer og blevet korrekt dokumenteret, gennemgået og godkendt, efterfølgende.

Tværgående kontroller, som ofte er afgørende for revisionen er:

- Kryptering og sikker kommunikation (herunder nøglepersoner og krisekommunikation)
- Cybersikkerhed og uddannelse (særligt uddannelse af ledelsen).
- Vurdering af effektivitet (interne gennemgange og øvelser). [1] [4] [15].

Revisionsbeviset vil for disse områder typisk omfatte politikker og opsætninger af kryptering/nøgleadministration(adgange), dokumentation for gennemført uddannelse (kursusbevis) samt resultater af gennemgange af kontroleffektivitet og opfølgning heraf. I den digitale sektor hvor 2024/2690 forordningen bliver anvendt, bør revisionen omfatte de nødvendige yderligere tekniske krav og tærskler for hændelsernes betydning [10] [16].

3.6 Hændelseshåndtering og rapportering

NIS2 kræver gradvis underretning til kompetente myndigheder om væsentlige hændelser. Første underretning skal ske inden for 24 timer efter at man er blevet opmærksom på hændelsen, derefter 72 timer efter man er blevet opmærksom på hændelsen og til sidst en endelig rapport en måned efter 72-timers underretning, med status på opfølgninger og afhjælpning af problemet [1].

EU-direktivet angiver også de minimumsforventninger der er til indholdet i underretningen, herunder en indledende vurdering af om hændelsen vurderes at være følge af et ondsindet angreb og om den kan have påvirket driften i andre lande (hvis virksomheden drives på tværs af landegrænser) [1].

Den danske lov afspejler de tidsfrister fra EU-direktivet og definerer hvornår en hændelse vurderes at være væsentlig, via konsekvenskriterier (alvorlig driftsforstyrrelse og økonomiske/samfundsmæssige konsekvenser). Det kræves også at CSIRT, hvis det er relevant, giver indledende tilbagemelding inden for 24 timer efter modtagelse af den tidligere varsling, og tilbyder vejledning og teknisk hjælp [4].

Danmark varetager rapportering gennem obligatorisk indsendelse via den portal der stilles til rådighed. BEK nr. 620 kræver at underretningen indsendes digitalt via Virk-selvbetjeningsløsningen med MitID, i henhold til lovens §§ 12-14. Dog med forbehold for en alternativ kanal, hvis portal-løsningen ikke er tilgængelig. Virk-vejledningen til indberetning af hændelser, angiver hvilke oplysninger der er påkrævet for henholdsvis 24-timers, 72-timers og endelig underretning, beskrivelse af hændelse (og tidslinje), omfang /berørte systemer, indikationer på kompromittering, udnyttede sårbarheder, involvering af tredjepart (ikke alle virksomheder har råd til at have kompetente nøglepersoner til hændelseshåndtering som fuldtidsansatte, og vil i disse tilfælde have kontrakt med konsulenter), samt beskrivelse af handlinger for at afhjælpe at hændelsen kan gentages. Der angives desuden også at flere rapporteringstyper og sektorer kan vælges, så underretningen bliver videresendt til de relevante kompetente myndigheder, afhængigt af valg [8].

Virk-vejledningen anbefaler anmelderen at downloade en kopi/kvittering af den indsendte formular, som bevis, og beskriver desuden også at Erhvervsstyrelsen videresender til de relevante kompetente myndigheder, på baggrund af sektorvalg [8]. Digitaliseringsstyrelsens vejledning specificerer også at de indberetninger der er sendt til via Virk-portalen, videresendes til sektormyndigheder og CSIRT [10]. Det betyder at som revisionsbevis skal hændelsesdokumentation indeholde både de indsendte formularer (med tidsstempel og referencenummer) og eventuel efterfølgende kommunikation med myndigheder.

For virksomheder i den digitale sektor, der er underlagt forordning 2024/2690, skal en hændelses betydning vurderes både i forhold til dansk lov og EU-direktivets detaljerede tærskler og de anvendte kriterier skal dokumenteres, således beslutningsforløbet kan gentages under en revision. [4] [10] [16].

Det minimale revisionsspor for hændelser (gentagelighed):

- Bevis for opdagelse af hændelsen: Logfiler/advarsler, systematisk oprettelse af tickets, tidsstempler og identifikation af påvirkede tjenester.
- Klassificering og beslutningsgrundlag herfor (EU-tærskler, hvis relevant), inklusiv tidsstempler.
- Dokumentation for portalindberetning (24-timers, 72-timers og endelig), med downloadede kopier (med referencenumre og tidsstempler).
- Gemte beviser (digital post og øvrig ekstern korrespondance) og interne kontroller.
- Dokumentation for udførte afhjælpende foranstaltninger, gennemgang efter hændelsen og opdatering af kontroller (så der ikke sker gentagelse) og kommunikation til de modtagere af tjenesten som potentielt kunne være påvirket [4].

Afvigelsesregler bør være i overensstemmelse med lovbestemte tidsfrister og krav om sporbarhed. Ved en væsentlig hændelse, bør manglende bevis for tidspunktet for kendskab til hændelsen, eller tilsvarende manglende bevis for underretningen, behandles som manglende overensstemmelse, medmindre det kan bevises at den pågældende hændelse ikke var væsentlig i henhold til de lovbestemte kriterier [1] [4] [13] [8] [10] [16].

3.7 Opsummering af minimumsforanstaltninger

En førstegangsrevision bør prioritere dokumentation der påviser korrekt afgrænsning/klassificering, udførelse af obligatoriske handlinger/underretninger i indberetningsportalen, kortlægning af ledelsesansvar og praktisk kapacitet til at opdage og reagere på væsentlige hændelser.

Omfang og registrering:

- Vurdering af omfang (kortlægning af tjenester) og dokumenteret anvendelse af regler, vurdering i henhold til størrelsesgrænser og dokumenterede overvejelse i forhold til påvirkning på tværs af sektorer.
- Registreringsbevis: downloadet kopi af den indsendte formular, med referencenummer, tidsstempel og eventuel kvittering for modtagelse fra Digital Post.
- Opdateringsregler: ændringslog, beviser for genindsendelse (ajourføring) af registrering, hvis der er sket væsentlige ændringer i virksomheden.

Foranstaltninger:

- Policies & procedures, der dækker de områder der som minimum kræves af loven, knyttet til kritiske tjenester, og en dokumenteret risikovurdering.
- Løbende dokumenterede stikprøver, baseret på område (adgangskontrol, sårbarhed, overvågning, gendannelse, leverandørvurderinger. Opdatering).
- Vurdering af effektivitet og sporing af afhjælpende foranstaltninger, med de ansvarlige personer / ledelsen, dokumentation for opfølgningen og gentagende gennemgang.

Hændelser og sporbarhed af rapportering:

- Register/arkiv med beslutninger om klassificering og tidspunkt for opdagelse.
- Dokumentation for underretning via Virk-portalen (24-, 72-timers og endelig), samt eventuelle statusrapporter.
- Efterfølgende gennemgang af hændelsesforløb, og konklusion på erfaringer og opdatering af kontrolforanstaltninger der bør implementeres, korrespondance med myndigheder, hvis relevant.
- Bevis for at der er sket kommunikation med påvirkede / potentielt påvirkede tjenestemodtagere, og at denne er i overensstemmelse med hændelsesklassificeringen [4].

Ovenstående minimumsforanstaltninger er jf. den danske lovs forpligtelser vedrørende klassificering, registrering, styring, kontrol, og trinvise underretning, samt at anvende Virk-portalen og identifikation med MitID, og de yderligere specificerede krav på EU-niveau i 2024/2690 [1] [4] [13] [5] [6] [7] [9] [8] [10] [15] [16].

4. Revisionskriterier og -metode

Dette kapitel forklarer hvordan NIS2-forpligtelser kan omdannes til reviderbare mål, samt blive vurderet gennem gentagende test. Det primære fokus er U1 og U2, ved at vurdere NIS2- forpligtelserne vedrørende: governance, risikostyring og hændelsesrapportering, til praktiske kontrolmål, dokumentationskrav og afvigelsesregler.

4.1 Hvad gør NIS2 reviderbart

I revisionsøjemed er en forpligtelse reviderbar, når: 1) den kan måles eller evalueres i henhold til fastlagte kriterier, 2) der kan indhentes beviser som kan henføres til forpligtelsen, 3) afvigelser kan defineres og rapporteret i ensartet format. ISAE 3000 definerer en erklæringsopgave som at opnå tilstrækkelige og passende revisionsbeviser, til at udarbejde en konklusion der øger brugerens tillid til de oplysninger der er evalueret i henhold til de fastlagte kriterier. Den specificerer også at passende kriterier er: relevante, fuldstændige, pålidelige, neutrale og forståelige, og upræcise/vage formuleret forventninger ikke kan bruges som revisionskriterier [2].

For NIS2 er det juridiske grundlag, EU-direktiv 2022/2555 (NIS2), som er gennemført via den danske lov [1].

NIS2 anvender en del upræcist formulerede begreber som ”passende” og ”forholdsmæssige” foranstaltninger, hvilket kræver en overordnet proportionalitetsvurdering, for at tage højde for ting som: risiko, virksomhedens størrelse, sandsynligheden / alvoren af hændelsen, økonomiske / samfundsmæssige konsekvenser. Reviderbarhed kræver derfor en praktisk tilgang. Lovkrav skal omdannes til kontrolmål, beviser og afvigelsesregler, som definerer hvad der kan betragtes som overholdelse og mangel på overholdelse [1] [2].

NIS2 gør det også muligt at placere ansvar. Ledelsen skal godkende de foranstaltninger der er implementeret til at styre cybersikkerhedsrisiko, og bliver holdt personligt ansvarlig hvis kravene om risikostyring ikke er overholdt. Dette kræver som tidligere nævnt at ledelsen og nøglepersoner er tilstrækkeligt uddannet til at varetage det ansvar der er forbundet med at kunne foretage risikostyring for levering af de tjenester der er omfattet af NIS2 [1] [2].

Implementeringen kan udføres ved at forholde sig til de krav IAASB / IFAC stiller for erklæringsopgaver: et trepartsforhold (revisor, virksomheden der bliver revideret og slutbrugeren), et passende emne og tilpassede kriterier, passende beviser / dokumentation og en skriftlig beretning fra revisor [2]. For NIS2 kan slutbrugeren være både kompetente myndigheder (som har den underlagte virksomhed som et af deres ansvarsområder), andre interessenter samt kunder, som er nødt til at kunne stole på virksomhedens evne til at styre deres cybersikkerhedsrisiko og rapporteringsforpligtelser i tilfælde af væsentlige hændelser. Revisionsmodellen skal derfor gøre de upræcist formulerede juridiske kriterier udtrykkelige for både revisor, virksomheden og slutbruger, så alle kan forstå hvordan overholdelsen blev vurderet [1] [2].

I praksis betyder det at omdannelse af lovteksten til specifikke kontrolmål, der beskriver sikkerhedsniveauet, og en rapporteringskapacitet som er passende i forhold til de risici der er tilknyttet. Dette er i overensstemmelse med NIS2’s krav om at proportionalitet afhænger af både virksomhedens risikoeksponering og hændelses alvor. Dog med forbehold for at EU-kommissionen senere kan præcisere

yderligere krav, som kan ændre hvordan specifikke sektorer er defineret og skal dokumenteres og testes [1] [16].

4.2 Erklæringstyper og hvad de indebærer

ISAE 3000 omhandler erklæringsopgaver. Konsulent-/ rådgivningsopgaver er ikke erklæringsopgaver, og ikke omfattet af ISAE 3000, så af hensyn til revisionsplanlægning, skelner dette kapitel mellem 3 typer af opgaver: 1) forbedrende arbejde, 2) intern revision og 3) uafhængig revision.

Forberedende gennemgang vurderer om beredskabs- og handlingsplaner er tilstrækkelige, uden at afgive en erklæring med sikkerhed. Dette gør det muligt at udføre en gap-analyse (afdækning af huller i planen) og komme med anbefalinger til udførelse og / eller forbedring af kontroller [2]. Intern revision foregår som af navnet internt i virksomheden og defineres i ISAE 3000 som udførelse af revisionsopgaver, til at evaluere og forbedre governance, risikostyring og intern kontrol, en slags forberedelse til at blive revideret eksternt med erklæring [2].

Erklæring med sikkerhed kræver i henhold til ISAE 3000, at erklæringsgiver(revisor) overholder de etiske krav og uafhængighed [2] [17], samt at revisor overholder IESBA (eller tilsvarende), og kun accepterer/fortsætter opgaven, når der ikke er mistanke om at etiske krav / uafhængighed ikke bliver overholdt [2]. IESBA kræver uafhængighed for at udføre revision, gennemgang og andre erklæringsopgaver, og har et framework til at opdage, evaluere og håndtere trusler med uafhængighed. I henhold til NIS2, betyder det at revisor ikke bør være ansvarlig for udarbejdelse og / eller indførelse af de kontroller den skal revidere, da dette så vil være selvkontrol [17].

Grænser for uafhængighed kan udtrykkes som simple regler i NIS2-revisionsplanlægningen. Revisor kan vurdere og teste om der findes kontroller og hvorvidt de bør forbedres på nogen punkter, men bør afholde sig fra at udforme selve kontrollerne, samt uddelegere ansvar eller endnu værre, selv påtage sig ansvaret for klassificering af hændelser [17]. Hvis den uafhængige revisor tidligere har ydet assistance, kræver IESBA at der foretages en evaluering af trusler og implementering af foranstaltninger (det kan være at et andet team hos revisor foretager revisionen) for at reducere truslen mod uafhængighed til et acceptabelt niveau [17]. Der er også regler mod honoraraftaler vedrørende revision. Honoraret må ikke være betinget af resultatet af revisionen. Disse begrænsninger er vigtige for NIS2-implementering, da mange revisorer i al almindelighed også agerer konsulenter for deres kunder.

Erklæringsniveauet har også betydning for hvad der kan konkluderes på. ISAE 3000 definerer rimelige og begrænsede erklæringsopgaver, og forklarer at begrænsede erklæringsopgaver er mindre omfattende end dem der gælder for erklæring med rimelig sikkerhed [2]. Dette understøtter NIS2 i den indledningsvise fase, hvor der lægges vægt på design og implementering, mens der i de efterfølgende faser vil blive fokuseret på praktisk effektivitet [2].

4.3 Kriterier

Kriterierne for at kunne revidere NIS2 bør kunne adskille det juridiske sprog (forpligtelser) fra revisionssprog (kontroller) for at kunne implementeres.

NIS2 fastsætter governance-forpligtelser (artikel 20), et minimumssæt af foranstaltninger (artikel 21), og forpligtelser til gradvis (24 timer / 72 timer / endelig) anmeldelse af hændelser (artikel 23) [1].

Artikel 21 kræver passende og forholdsmæssige foranstaltninger, som beskrevet i afsnit 4.1. Artikel 23 definerer hvornår en hændelse er væsentlig og kræver indberetning ud fra de nævnte tidsfrister. Samt de yderligere krav for virksomheder der er indenfor den digitale sektor jf. EU 2024/2690 [1] [16].

ISO 27001 definerer krav til informationssikkerhedsstyringssystem (ISMS) og giver en vejledning til etablering og forbedring af ISMS [18]. Overensstemmelse med ISO 27001 indikerer at et ISMS er implementeret, men er ikke i sig selv et tilstrækkeligt bevis på overholdelse af forpligtelserne i NIS2, da det juridiske anvendelsesområde, rapporteringsforpligtelser og sektorspecifikke regler, kan variere [1] [18]. COBIT (udarbejdet af ISACA) er et rammeværktøj til at optimere en virksomheds governance i henhold til IT, og til at integrere standarder og regler til Best Practice, til en samlet governance-løsning. COBIT 2019 indeholder en basismodel med 40 governance-mål [19].

COSO's "Internal Control – Integrated Framework" definerer interne kontroller som en proces der er designet til at give rimeligsikkerhed for opretholdelse af virksomhedens drift, rapporterings- og compliance-mål. Den indeholder 5 komponenter, som understøttes af 17 principper [20]. Dette rammeværktøj kan bruges til at designe kontrollen, men skal ikke ses en egentlig løsning til de juridiske forpligtelser som NIS2 stiller [2] [18] [19] [20].

Brugen af rammeværktøjer som kontrolsprog er i forening med ISAE 3000's kriteriemodel. Her udtrykkes der at kriterier kan fastsættes i love / forskrifter, eller de kan udstedes af autoriserede / anerkendte ekspertorganisationer, efter at have gennemgået en gennemsigtig implementeringsproces, samt at de fastsatte kriterier er egnede og relevante for slutbrugerens behov [2]. For NIS2's vedkommende er EU-direktivet og de landespecifikke gennemførelseslove, de fastlagte juridiske kriterier / forpligtelser, mens ISO 27001, COBIT og COSO hjælper med at omdanne dem til strukturerede begreber (risikostyring, governance, intern kontrol, måling og overvågning), som kan understøtte en ensartet udførelser på tværs af de forskellige underlagte virksomheder [1] [16] [18] + [19] [20].

Det er dog vigtigt at bemærke at ISO selv advarer mod at en certificering (f.eks. ISO) ikke skal behandles som en erstatning for en kontekst-specifik evaluering (konteksten her er NIS2), da loven allerhøjest trække tråde til de ovennævnte standarder, men aldrig kan ses som 1:1 erstatning. I sig selv vil det bare dokumentere at der er implementeret et ISMS, men ikke om eller hvordan det opfylder de sektorspecifikke krav som NIS2 stiller [18]. Ligeledes er COBIT et værktøj til at integrere standarder og regler i henhold til udarbejdelse af en governance-løsning, men ikke lig med compliance til at tilsidesætte reglerne [19]. Hvorfor de udarbejdede kriterier altid bør indeholde henvisninger til de relevante NIS2-artikler og gældende nationale gennemførelsesbestemmelser.

ISAE 3000 kræver at de udvalgte kriterier skal være egnede og tilgængelige for de tilsigtede slutbrugere, og at vagt formulerede forventninger, ikke er egnet som kriterie [2]. En NIS2-revision bør derfor altid specificere de lovtekster og vejledningsdokumenter der udgør kriterierne pr. en given dato og sammenhængen til de implementerede kontrolmål der anvendes til at imødekomme disse kriterier [1] [2].

NIS2 kræver sikkerhed i forsyningskæden, og kræver at underlagte virksomheder tager højde for deres leverandørers cybersikkerhedspraksis og sårbarhed, herunder sikre udviklingsprocedurer (patch) [1], da virksomhedens leverandørers sårbarheder vægter på samme niveau, da ingen kæde(forsyning) er stærkere end det svageste led.

ISAE3402 er en erklæring med sikkerhed om kontroller hos virksomheder der leverer tjenesteydelser, som med høj sandsynlighed er relevante for virksomhedens interne kontrol, da det vedrører finansiel rapportering [21]. En ISAE 3402 erklæring kan derfor være relevant dokumentation for visse specifikke

tredjepartskontroller som overlapper nogen af kravene i NIS2 (f.eks. adgangsstyring og ændringskontroller), men revisorer skal vurdere omfanget og relevansen ud fra den enkelte virksomhed og sektorvalg, i henhold til vurdering om virksomheden er i overensstemmelse med NIS2 [1] [21].

4.4 Dokumentationsspor og kvalitetssikring af revisionsbevis

Revisionsbevis er broen mellem revisionskriterier og konklusionen. ISA 500 definerer tilstrækkelighed som mængden af beviser, og hensigtsmæssighed som kvaliteten af disse beviser (relevans og pålidelighed), og kræver at revisorer planlægger og udfører revisionen efter at opnå tilstrækkeligt og hensigtsmæssigt revisionsbevis [3]. Tilsvarende kræver ISAE 3000 samme mængde og kvalitet af bevis, for at underbygge erklæring med sikkerhed [2].

For at gøre NIS2 reviderbart, skal beviser håndteres som en kæde: Kriterier -> Kontrolmål -> Beviser -> Testprocedurer -> Afvigelsesregler [2] [3]. Beviser skal kunne stå på egen hånd og eksistere udenfor revisionen (godkendte politikker, standardopsætninger, overvågningsresultater, hændelsesregistreringer tidsstemplede underretninger), og skal opbevares i et format der understøtter de lovpligtige tidsfrister og krav om sporbarhed [1] [3].

ISA 500 giver praktisk vejledning om pålidelighed. Beviser fra uafhængige kilder er generelt mest pålidelige. Internt generede beviser kan være pålidelige, når kontrollen med deres udarbejdelse og vedligeholdelse er effektiv. Arkiveret dokumentationsbevis er altid mere pålideligt end mundtlige udtalelser. Originale dokumenter er mere pålidelige end kopier, hvis kontrollen med kopierne er usikker. ISA 500 kræver også at der tages hensyn til relevansen og pålideligheden af eksterne informationskilder, herunder deres autoritet og troværdighed, og forekomsten af eventuelle ansvarsfraskrivelser. Disse principper understøtter en disciplineret brug af tredjepartsattester, portal-modtagelser og kommunikation fra tilsynsmyndigheder, samt logfiler, som bevis i NIS2-compliance [1] [3].

Valget af procedurer skal sikre sporbarhed helt tilbage til bevismålene. ISAE 3000 beskriver generelle sikkerhedsprocedurer som: forespørgsel, inspektion, genberegning, genudførsel, observation, bekræftelse og analytiske procedurer. ISA 500's principper om pålidelighed vejleder derefter om hvilke procedurer der er mest overbevisende i henhold til NIS2. For eksempel vil kontrol af originale hændelsesindberetninger med tidsstempel og direkte observation/genudførelse af hændelsesrapporteringsworkflowet, generelt udgøre et bedre bevis. Dette er især relevant for de fastsatte tidsfrister i NIS2 artikel 23, hvor der skelnes mellem dokumenteret og påviselig gennemførsel inden for tidsfristerne [1] [3].

Bevismateriale skal ikke kun vurderes i forhold til deres eksistens, men også med hensyn til integritet og sammenhæng. NIS2 kræver at der rapporteres trinvist, ud fra hvornår virksomheden er blevet opmærksomme på den væsentlig hændelse [1]. En reviderbar kæde af beviser vil derfor kræve tidsstempler for at underbygge forløbet. 1) tidspunktet for opdagelse af hændelsen, 2) tidspunktet for beslutningen på at gøre opmærksom på hændelsen, 3) tidspunktet for beslutningen om at klassificere hændelsen som væsentlig / ikke-væsentlig, 4) tidspunktet for indsendelse af underretningen inden for tidsfristerne. I henhold til ISA 500 er sådanne tidsstemplede dokumenter generelt mere pålidelige end mundtlige udtalelser og beviser som er indhentet selv af revisoren er mere pålidelige end beviser som er indhentet indirekte (gennem forespørgsler) [3].

Når beviser ikke er konsistente eller fuldstændige, vil det være nødvendigt at iværksætte yderligere procedurer, eller indhente yderligere tilstrækkelige beviser. Ellers vil der være en begrænsning i omfanget af revisionen, som vil påvirke den endelige konklusion [2] [3].

4.5 Væsentlighed og betydning i overholdelse af NIS2

Væsentlighed i forbindelse med sikkerhed er knyttet til brugerens behov for informationen. ISAE 3000 påpeger at fejlinformationer (herunder udeladelser af væsentlig information) er væsentlige, hvis de med rimelighed kan forventes at påvirke brugerens relevante beslutninger, samt at væsentlighed er den samme for rimelig- og begrænset sikkerhed, da den er baseret på den tilsigtede brugers behov. Væsentlig tager hensyn til kvalitative faktorer og hvor det er relevant, kvantitative [2].

For NIS2 kan en konsekvensbaseret væsentlighedsmodel tilpasses direktivets egen ramme. Artikel 21 kræver at der er et sikkerhedsniveau i forhold til de risici der er forbundet med virksomhedens drift, og knytter proportionalitet til eksponering, størrelse, sandsynlighed og alvor, samfundsmæssige- og økonomiske konsekvenser. Artikel 23 definerer en væsentlig hændelse som en alvorlig driftsforstyrrelse / økonomisk tab, eller betydelig skade på andre og fastsætter strenge rapporteringsfrister, baseret på hvornår virksomheden er blevet opmærksom på den væsentlige hændelse [1].

Tre praktiske vinkler til væsentlighed:

- Kritisk indvirkning på tjeneste: I hvilket omfang en mangel / fejl øger sandsynligheden for eller indvirkningen af en væsentlig hændelse, der påvirker tjenesterne.
- Indvirkning på rapporteringskapaciteten: Om mangler underminerer, opdagelse, klassificering og rapportering, inden for de lovbestemte tidsfrister, eller evnen til at udarbejde en endelig opfølgningsrapportering.
- Indvirkning på afhængighed: Hvor vidt mangler / fejl vedrører leverandører / tjenesteudbydere på en måde, der væsentligt øger eksponeringen, i betragtning af de krav NIS2 stiller til forsyningskæden og leverandørrisiko (Artikel 22) [1].

Svagheder i ledelsen kan være kvalitativt væsentlige, selv uden at der er sket en væsentlig hændelse. NIS2 tilknytter ledelsens godkendelse, tilsyn og ansvar direkte til kravet om risikostyringsforanstaltninger, hvilket gør dokumentation til ledelsen, til en central del af konklusionen om overholdelse [1] [2].

Bevidst er også et revisionskritisk kontrolpunkt. Artikel 23 i NIS2-direktivet knytter rapporteringsfrister til bevidstheden om hændelsen og ikke dens faktiske forekomsttidspunkt [1]. Dette gør virksomhedens interne beslutningsregler for bevidsthed og væsentlighed til en del af det revisionspligtige system. Revisorer skal teste om virksomhedens procedurer for håndtering af hændelser, fører til rettidige beslutninger om bevidsthed, der er underbygget af dokumenterbare beviser og om disse beslutninger pålideligt fører til konkrete handlinger [1] [2]. Med hensyn til væsentlighed kan mangler / fejl, der forsinker bevidstheden (f.eks. utilstrækkelig overvågning / logning eller uklar eskaleringsplan), behandles som væsentlige, da de truer virksomhedens evne til at overholde de lovmæssigt fastsatte tidsfrister på 24 og 72 timer [1].

4.6 Forsinket / igangværende national implementering og konsekvenser for revisionen

NIS2 krævede at medlemslandene vedtog og offentliggjorde gennemførelsesforanstaltninger inden den 17. oktober 2024, og anvendte dem fra 18. oktober 2024 [1]. NIS2 indeholder også bestemmelser om yderligere præciseringer, gennem gennemførelsesakter og der er udstedt sektorspecifikke krav, ud fra de tjenester som de underlagte virksomheder yder. For Danmark (og andre medlemslande) kan den nationale

implementering udvikle sig gennem bekendtgørelser og officielle retningslinjer, hvilket skaber risiko for ændringer til kriterierne i de første revisioner.

Dette skaber øget risiko for ustabil planlægning af revisionen, hvis kriterierne indledningsvist både er upræcist formuleret (til fortolkning) og kan ændres løbende. ISAE 3000 kræver at revisionskriterier er egnede og tilgængelige for de tilsigtede brugere. Hvis kriterierne ændrer sig, skal revisionsopgaven begrænses til at være relevant t.o.m. en given dato og der skal vedlægges de pr. den dato gældende love og retningslinjer, hvilket dermed skaber en fastfrysning af kriterierne og gør konklusionen fortolkelig [1] [2].

Førstegangsrevision og øvrige tidlige revisioner efter implementering af ny lov, lægger stor vægt på design og implementering. Det kan være at sikkerhedsprocedurer designes til opfylde NIS2-forpligtelser, inden de implementeres operationelt, for at have NIS2 som fundamentet i processerne [1] [2].

Kriterieændringer er ikke begrænset til de nationale retningslinjer. NIS2 indeholder som tidligere nævnt udtrykkelige bestemmelser om gennemførelsesakter, der yderligere kan specificere oplysninger, format og procedurer for anmeldelse, og kræver gennemførelsesakter for visse sektorers risikostyringsforanstaltninger. Disse ændringer på EU-niveau, kan finde sted uafhængigt af de nationale tidsfrister, og kan ændre revisionskriterier og forventninger til dokumentation for virksomheder der er underlagt NIS2 [16]. En fastfrysning af kriterierne under en igangværende revision, skal derfor omfatte både de nationale- og EU-retningslinjer, og dokumenteres med version og tidsstempel [1] [2].

ISAE 3000 tillader at konklusionen rapporteres i lang form, med resultater og anbefalinger (og ikke bare det vi kalder en ”blank påtegning”), hvis disse er tydeligt adskilt og ikke forringer konklusionen, for at en konklusion med fastfrosne kriterier stadig kan fortolkes. Dette format kan dokumentere de fastfrosne kriterier og forklare hvordan senere ændringer i lovgivningen skal vurderes efterfølgende [2].

ENISA-udgivelser kan anvendes som hjælp i processen til at designe revisionsprocedurerne. Implementeringsvejledning til NIS2 præsenteres som en teknisk vejledning til EU 2024/2690 og indeholder praktiske eksempler og kortlægninger, men at følge denne er i sig selv ikke ens betydende med overholdelse af NIS2-kravene [1] [16] [2].

4.7 Afvigelsesmodel

En afvigelsesmodel omdanner testresultater til en forsvarlig konklusion. ISA 500 forklarer at test af kontroller involverer opdagelse af kontrolegenskaber, der indikerer at kontrollen er udført, samt afvigelsesbetingelser, der viser når den udførte kontrol afviger fra det der anses for at være tilstrækkeligt [3]. ISAE 3000 tilknytter derefter afvigelserne til ændring af konklusionen, når der opstår en begrænsning i omfanget og effekten deraf vurderes at være væsentlig, skal revisor udtrykke en betinget konklusion eller helt afvise, på erklæringen. Det forklares også at en betinget konklusion, anvendes når konstaterede eller mulige indvirkninger af et forhold ikke er så væsentlige og gennemgribende, at der ikke kan afgives erklæring [2].

For NIS2 skal afvigelsesmodellen skelne mellem:

- Manglende overholdelse (kriterier er ikke opfyldt) og
- Begrænsning af omfang (der kan ikke opnås tilstrækkeligt dokumentation / bevis) [3] [18].

Denne adskillelse er for at gøre revisionskonklusionen forståelig for tilsynsmyndigheder og ledelsen, ved at skelne mellem om kontrollen ikke er på plads og om den ikke kunne dokumenteres [2].

Nedenstående tabel 4.1 viser en praktisk måde at klassificere afvigelser på, så klassifikationen er jf. ISAE 3000:

Tabel 4.1

Kategori	**Typisk udløser**	**Afvigelsesregel**	**Typisk effekt på ISAE 3000-konklusion**
Kritisk	Fejl der underminerer centrale lovkrav (f.eks. ingen implementeret hændelsesrapporteringsproces, der kan sørge for rettidig underretning, eller ingen tilsyn fra ledelsen).	Én eller flere afvigelser vurderes som væsentlige og gennemgribende, i henhold til relevante kriterier.	Høj grad af sikkerhed: afkræftende konklusion. Begrænset sikkerhed: afkræftende konklusion.
Betydelig	Udarbejdelse / implementering opfylder ikke de juridiske krav, men konsekvensen heraf er begrænset (f.eks. mangler i krav til forsyningskæden/leverandører).	Afvigelser er væsentlige, men ikke gennemgribende.	Høj grad af sikkerhed: konklusion med forbehold. Begrænset sikkerhed: Konklusion med forbehold.
Forbedring	Forhold der ikke påvirker opfyldelsen af kriterier væsentligt (f.eks. manglende dokumentation, hvor drift kan dokumenteres, mindre forsinkelser, men stadig inden for lovens tidsfrister).	Afvigelser registreres som observation, ingen betydning, med mindre de samlet set er væsentlige.	Uændret konklusion, med observationer og anbefalinger, adskilt fra selve konklusionen.
Omfangs-begrænsning	Revisor kan ikke opnå tilstrækkeligt og egnet bevis for et væsentligt område (f.eks. logning, adgangsbegrænsninger, eller centrale registre ikke er tilgængelige).	Bevismangel forbliver efter forsøg på alternative revisionshandlinger, manglen skyldes bevisets manglende tilgængelighed, ikke nødvendigvis et svigt af kontroller.	Konklusion med forbehold eller ingen konklusion, afhængigt at væsentlighed og om det er gennemgribende.

Klassifikation anvendes på niveauet for et defineret kriterie / kontrolmål. Herefter vurderes der samlet set ud fra 1) hvor vigtigt det berørte kriterie er for NIS2's formål (ledelsesansvar, risikostyring og rapportering), 2) om afvigelserne er gennemgribende på tværs af alle kriterier. I praksis kan gennemgribende i henhold til NIS2 være indikeret ved gentagne svigt på tværs af de områder der er defineret i artikel 21, eller ved manglende evne til at opfylde de trinvise underretningsforpligtelser i artikel 23 [1] [2].

Klassifikation og sammenlægning af beviser, skal dokumenteres, så en uafhængig 3.part kan forstå grundlaget for konklusionen og sammenhængen mellem fund og konklusionen [2]. Når mangler / fejl vedrører flere områder efter artikel 21, eller undergraver rapporteringskapaciteten efter artikel 23, er det indikation på at de er gennemgribende og vil dermed påvirke konklusionen med mere end blot et forbehold [1] [2].

5. Forslag til dansk model for IT-revision efter NIS2

Kapitlet foreslår en dansk IT-revisionsmodel for NIS2, der omdanner de juridiske og vejledende forpligtelser til revisionskriterier, bevismateriale og testprocedurer. Modellen implementerer kravene til risikostyring, hændelseshåndtering, governance og rapportering, der er relevante for U1 og anvender sikkerhedskoncepter (egnede kriterier, beviskvalitet og afvigelsesregler) der er relevante for U2. Den er udarbejdet til første revision af danske virksomheder underlagt NIS2, mens de officielle vejledninger / portaler stadig er under udarbejdelse [1] [4] [2].

5.1 Principper for udarbejdelse af modellen

Modellen er bygget på 4 grundprincipper

- Bevisindsamling først
- Fastfrysning af kriterier (hvis loven eller retningslinjer ændres)
- Virkningsbaseret væsentlighed
- Trinvis sikkerhed

Disse principper er i overensstemmelse med de juridiske forpligtelser til kriterier og tilstrækkeligt bevis [2] [3].

Revisionsmodellen er udarbejdet omkring bevismateriale, der kan henføres til virksomheden og gentages af en anden revisor. ISA 500 fastlægger bevismaterialets kvalitet ud fra tilstrækkelighed og hensigtsmæssighed (relevans og pålidelighed), og ISAE 3000 kræver at revisionskonklusionen understøttes af tilstrækkeligt og hensigtsmæssigt bevismateriale [2] [3]. I Danmark er centrale arbejdsgange til at understøtte NIS2-forpligtelser beskrevet af Virk.dk, med fokus på registrering og hændelsesrapportering. Bekendtgørelsen fastslår at kommunikation i henhold til den danske NIS2-lov §§ 9-10 (registrering) og §§ 12-14(underretning) skal indsendes digitalt via den portal-løsning der stilles til rådighed og identifikation med MitID [13]. Dette gør dokumenter indsendt og modtaget via denne portal til primær-beviser [7] [8].

ISAE 3000 kræver at sikkerhedsrapporteringen identificerer de gældende kriterier, og at revisors konklusion udtrykkes i henhold til disse kriterier [2]. Da den danske implementering er baseret på EU-direktivet, dansk lov, bekendtgørelser, officielle retningslinjer og portal-vejledninger / workflows, skal revisionsopgaven definere og fastfryse(tidsstempel) det sæt kriterier som er gældende for revisionen [1] [4] [13] [9] [10] [6]. Fastfrysningen forhindrer at kriterierne ændres undervejs i revisionen og understøtter sammenlignelighed til efterfølgende revisioner, da der så kan tages højde for hvis kriterierne har ændret sig og hvilke der har [2].

ISAE 3000-konklusion udtrykkes i alle væsentlige henseender, hvilket indebærer at der fokuseres på forhold der med rimelighed kan påvirke den tilsigtede slutbrugers tillid til information om den underlagte virksomhed [2]. NIS2 og dansk lovgivning er begge fokuseret på effekt. Risikostyringsforanstaltninger skal være passende og proportionelle, i forhold til de risici der er forbundet med de leverede tjenester, og rapporteringsforpligtelsen udløses af væsentlige hændelser som er vurderet ud fra potentiel indvirkning / effekt [1] [4] [10]. Revisionsmodellen definerer derfor væsentligheden ud fra:

- Beskyttelse af kritiske tjenester.
- Virksomhedens evne til at opdage og rapportere væsentlige hændelser, inden for de lovbestemte tidsfrister.
- Afhængighed af leverandører, som kan have væsentlig indflydelse på tilgængelighed, fortrolighed / integritet, eller rapporteringsevne. [1] [4] [21].

De første revisionen underlagt NIS2, kan af åbenlyse årsager have begrænset dokumentation for driftshistorik (f.eks. nye procedurer, portal-workflows efterlovens ikrafttræden). [4] [13]. ISAE 3000 understøtter både revisionsopgaver med begrænset og rimelig sikkerhed, og tillader konklusioner der afspejles i den tilgængelige dokumentation for design, implementering og driftseffektivitet (hvis muligt). Modellen anvender derfor trinvis sikkerhed. De tidlige revisioner, prioriterer design og implementering, og udvider dens test af driftseffektiviteten, når de officielle kriterier (og heraf kontroller) stabiliseres [2] [3].

5.2 Modeloverblik: De 4 revisionsområder

Modellen opdeler revisionen i 4 kerneområder, der afspejler de vigtigste revisionsmæssige forpligtelser i NIS2.

- Risikostyringsforanstaltninger.
- Opdagelse og håndtering af hændelser.
- Governance.
- Registrering, rapportering og sporbarhed [1] [4] [13].

Hvert område definerer revisionsmål, primære bevismaterialer og en typisk testtilgang der kan omdannes til et revisions-workflow [2] [3].

5.2.1 Risikostyringsforanstaltninger:

Revisionsmål:

- Påvise at virksomheden har truffet passende og proportionelle tekniske, operationelle og organisatoriske foranstaltninger til at styre risici for netværks- og informationssystemer, der anvendes til drift eller levering af kritiske tjenester [1] [4].
- Påvise at de minimumsområder der er beskrevet i NIS2 artikel 21, stk. 2 og dansk lov § 6 (risikoanalyse og sikkerhedspolitikker, håndtering af hændelser, fortsat drift, sikkerhed i forsyningskæden, sikker udvikling, håndtering af sårbarheder, effektivitetstest, uddannelse, kryptografi, adgangskontrol og sikker kommunikation) er afdækket [1] [4].
- Påvise at de valgte foranstaltninger er begrundet og dokumenteret ud fra risiko for de definerede kritiske tjenester. Altså fokus på selve begrundelsen for foranstaltningen og ikke blot dens tilstedeværelse [1] [4] [15].

Primære beviser:

- Risikovurderingsmetode, risikoregister og dokumenterede beslutninger om risikoovertagelse / -overdragelse, der knytter risici til kritiske tjenester og trusler [4] [15].

- Dokumentation for kontrol af nøgleområder (IAM, sårbarheds-/patchstyring, logkontrol/overvågning, backup/gendannelse, leverandørstyring og sikker udvikling) [1] [4] [15].
- Implementerings- driftsregistreringer (konfigurationer for IAM, periodisk / systematisk kontrol, logning af backups, opdateringer og gendannelser, overvågningsregler og alarmer, sporing af hændelser og afhjælpning) [3].

Testtilgang:

- Designets tilstrækkelighed: Vurder om de dokumenterede kontrolmål og procedurer er i stand til at håndtere de definerede risici i det fastfrosne omfang af kriterier [2] [3].
- Implementering: Test udvalgte konfigurationskontroller (privilegeret adgang, MFA, indstillinger for log) og kontroller at disse kontroller er implementeret i de kritiske systemer [3].
- Driftseffektivitet: På de områder med tilstrækkelig historik, foretages der stikprøver over periode [3].

5.2.2 Hændelseshåndtering:

Revisionsmål:

- Bevise virksomhedens evne til at opdage, klassificere og reagere på hændelser, og efterfølgende underrette de om dem der er væsentlige, uden unødvendig forsinkelse gennem den trinvise rapporteringsproces (tidlig varsel, hændelsesunderretning, mellemliggende opdateringer, og hvis anmodes om, endelig rapport) [1] [4] [8].
- Påvise at virksomheden kan dokumentere tidspunktet for hvornår den er blevet opmærksom på hændelsen, som danner udgangspunktet for den lovpligtige rapporteringsfrist, og dermed underbygge de via Virk-portalen indsendte oplysninger [1] [4] [8] [3].

Primære beviser:

- Policies & procedures til håndtering af hændelser, definerede roller (ansvar), eskaleringsveje samt dokumenterede beslutninger (og grundlag) [1] [4].
- Hændelsesregistreringer (systemgenerede advarsler, undersøgelsesnoter, vurderinger, klassificeringsbeslutninger, og grundlag for beslutning om væsentlig eller ikke-væsentlig) [4] [10] [3].
- Bevis for indsendelse via Virk-portalen (downloadede kopier / kvitteringer for indberetningen med referencenummer og tidsstempel). Virk-vejledningen påpeger at man skal downloade kopier efter indsendelsen [7] [8].

Testtilgang:

- Gennemgang af hele hændelsesprocessen, fra opdagelse til rapportering, herunder rekonstruktion af tidlige advarsler, for at vurdere om bevidsthed om hændelsen er opstået tids nok, til at kunne reagere og at de lovpligtige frister jf. NIS2 artikel 23 og dansk lov § 13 [1] [4].
- Stikprøvevist gentag klassificeringsbeslutninger i forhold til danske lovmæssige (og fra vejledningen) definitioner af væsentlige hændelser og kontroller om portal-indberetningerne er i overensstemmelse med de registrerede hændelser [4] [10] [8].
- Kontroller om de interne registreringer og indberetningerne er fuldstændige og konsistente med beviserne og at beviserne svarer til den faktiske hændelse [3].

5.2.3 Governance og ansvar:

Revisionsmål:

- Påvise at ledelsen godkender og overvåger de implementerede foranstaltninger til styring af cybersikkerhedsrisici og kan dokumentere de tilsyn der kræves i henhold til NIS2-bestemmelserne om governance [1] [4].
- Påvise at ansvarsområderne, rapporteringsveje og uddannelsesforpligtelser er implementeret og overholdt, og ikke kun beskrevet i policies & procedures [1] [4].

Primære beviser:

- Ledelsesreferater og godkendelser, der viser både indledningsvis godkendelse af cybersikkerhedsforanstaltninger og løbende tilsyn fra den ansvarlige ledelse. NIS2 artikel 20 / dansk lov § 7, kræver godkendelse fra ledelsen og tilsyn under implementeringen [1] [4].
- Definerede roller, uddelegering af ansvar og rapporteringspakker (KPI for risiko og kontrolmål, hændelsesmålinger, sporing af afhjælpende foranstaltninger) [4] [3].
- Register for uddannelse af ledelsesmedlemmer om cybersikkerhedsstyring, og dokumentation for at uddannelses / kursus' relevans, det er altså ikke nok at have et kursusbevis, uden dokumentation for at kurset er relevant [1] [4].

Testtilgang:

- Kontroller ledelsens / bestyrelsens referater / materiale med henblik på godkendelse, tilsyn og løbende opfølgning. Spor udvalgte beslutninger omkring sikkerhed (risikoaccept, ressourceallokering, leverandørvalg) til ledelsens involvering [1] [4].
- Kontroller at governance-politikker rent faktisk dækker det nødvendige omfang (kritiske tjenester og -systemer) samt er i overensstemmelse med den indledningsvise risikobegrundelse [4] [15].

5.2.4 Registrering og rapportering:

Revisionsmål:

- Påvise at virksomheden har en gentagelig omfangsvurdering og opfylder de lovpligtige registreringsforpligtelser, med nøjagtige data og rettidige opdateringer / ajourføring [4] [9].
- Påvise at eksterne kommunikationskanaler er funktionsdygtige (hvem har ansvaret for at videregive relevant intern kommunikation), herunder indsendelse via Virk-portalen og adgangskontrol over hvem der kan indsende, samt opbevaring af dokumentation / beviser for indsendelsen [13] [7] [8].

Primære beviser:

- Beslutningsreferater om klassificeringsbegrundelse (sektor, væsentlig eller vigtig), identifikation af kritiske tjenester og dokumenterede grænseværdier) [4] [9].
- Registreringsbevis, kvittering / kopi af indsendelse af denne, både oprindelige og efterfølgende opdateringer. For virksomheder omfattet af §§ 9-10 skal oplysningerne indgives 1. oktober 2025 (§33 stk. 3.), eller hvis de først er omfattet efterfølgende, senest 3 måneder efter at virksomheden bliver omfattet af loven, og eventuelle senere ændringer skal ajourføres 3 måneder efter de er trådt

i kraft (§ 9). For væsentlige og vigtige enheder omfattet af § 10, er fristen 2 uger for både indledende registrering og ajourføring [4] [9].

- Ændringslog over opdateringer af registreringen, underliggende beslutningsgrundlag og godkendelse fra ledelsen. Dansk lov kræver ligesom den første registrering at væsentlige ændringer opdateres / ajourføres i registrering inden for 3 måneder (§ 9) eller 2 uger (§ 10) af at de er trådt i kraft [4].

Testtilgang:

- Gentag omfangsvurderingen og afstem datafelter i registreringen med intern dokumentation [4] [7] [3].
- Kontroller opdateringskontroller og stikprøvevist kontroller opdateringer (nøjagtighed, rettidighed og dokumentation heraf) [4] [3].

5.3 Indgåelse af kundeforhold og fastfrysning af kriterier

Planlægningen og opbygningen af revisionen omdanner de lovbestemte kriterier til kontrolmål. Et fastlagt sæt kriterier (fastfrosne ud fra tidsstemplet lovgrundlag), afgrænsning af bevismaterialet og en tilstrækkelig påviselig grad af uafhængighed. ISAE 3000 kræver at de gældende kriterier identificeres i rapporteringen og ISA 500 kræver at der udarbejdes procedurer for indhentning af tilstrækkeligt og passende bevismateriale [2] [3].

Trin 1:

Definér emnet, omfanget og de tilsigtede slutbrugere. Definér om det er beredskabsopgave, intern revision eller uafhængig erklæring med sikkerhed (se kapitel 4), og dokumenter hvad rapporten / erklæringen skal bruges til (f.eks. bestyrelsens tilsyn, tilsynsmyndigheder, leverandører) [4] [2]. Fastlæg det organisatoriske og tekniske omfang som et kontrolmål, kortlæg kritiske tjenester, involverede systemer og vigtige leverandører, der er væsentlige for at fortsætte driften af disse tjenester [1] [4] [15].

Trin 2:

Opbyg et kriterieregister / -ramme. Registrer kriterier i et struktureret register, kortlagt ud fra juridiske krav og omdannet til praktiske og implementerbare krav. Minimumskravene i NIS2 er:

- Governance-forpligtelser jf. direktivets artikel 20 og den danske lovs §7, foranstaltninger jf. artikel 21 og den danske lovs § 6 og rapportering jf. artikel 23 og den danske lovs §§ 12-14.
- Krav i bekendtgørelsen om digital indsendelse via Virk-portalen og identifikation med MitID.
- Officielle retningslinjer, vejledninger og portal-workflows, der definerer krævede datafelter og bevistyper [1] [4] [13] [7] [8].

Når en EU-gennemførelsesforordning finder anvendelse i en bestemt kategori af virksomheder (sektorvalg) (f.eks. EU 2024/2690), vil den blive registreret som et yderligere juridisk grundlag for virksomhedens forpligtelser [10] [15] [16].

Trin 3:

Fastfrysning af kriterier pr. dags dato og dokumenter kriteriegrundlag (download lovtekster, vejledninger, skærmdumps fra portal-workflows) og eventuelle efterfølgende ændringer hertil [3]. Før en ændringslog der registrerer: hvad der er ændret (kilden), ændringens ark (præcisering ift. væsentlighed), ændringens virkning på revisionstest og bevismateriale og om revisionsopgavens omfang og kriterier er blevet opdateret som følge af denne ændring [2].

Trin 4:

Definer en afgræsning af revisionsbeviserne og eventuelle ændringer undervejs. Det gælder både beviser for test af driftssikkerhed og for eventuelle indsendelser via Virk-portalen. Det kan være at en revisionsperiode er t.o.m. 31. december, så der skal defineres om der undersøges hændelser der er sket eller opdaget i perioden, da hændelser der er sket før skæringsdatoen først kan være opdaget efter skæringsdatoen. Hvis portal-workflow ændres under revisionen, skal det præciseres hvis forventningerne til revisionsbeviser ligeledes ændres. Enten skal de fastfrosne kriterier beholdes og ændringen skal noteres som en efterfølgende begivenhed, eller også skal de ellers fastfrosne kriterier opdateres og indvirkningen på testprocedurer og konklusioner dokumenteres [2] [3].

Trin 5:

Hvis revisor også yder konsulentydelser i form at hjælp til implementering og senere revision af selvsamme, er der betydelig risiko for at det ender med at være selvrevision, som er en trussel for uafhængigheden. ISAE 3000 lægger stor vægt på overholdelse af etiske principper, herunder uafhængighed, og det er vigtigt at erklæringen udviser dette [2]. Revisionsmodellen kræver derfor at der er i disse tilfælde er separate teams for konsulentopgaven og revisionsopgaven, eller som minimum er skiftende underskrivende revisor / partner. Derudover skal der for konsulentydelsen være defineret klare grænser for hvad der assisteres med (anbefalinger vs. reelt design) og hvem der bærer ansvaret for dette [2].

5.4 Planlægning af revisionen og udarbejdelse af arbejdsprogram

Arbejdsprogrammet i planlægning er forbindelsen mellem de juridiske forpligtelser og hvilke grænser der er for hvad der kan testes, samt afvigelsesregler. Det er en række revisionsmål, der kan gentages på tværs af virksomheder og cyklusser (førstegangsrevision og tilbagevendende) [2] [3].

1. Omfangsmemo, der fastslår omfanget af revisionen, ud fra virksomhedens sektor, klassificering som væsentlig / ikke-væsentlig, kortlægning af kritiske tjenester, der ligger til grund for proportionalitetsvurderingen [1] [4] [9]. Indbyg tidsfrister for registrering og ajourføring, da en

manglende eller ukorrekt registrering ikke bare en ekstern manglende overholdelse, men danner fundament for strukturering af selve revisionen [4].

2. Kriterieregister med liste over beviskrav: Omfangsmemoet skal være kort og præcist, for at kunne kvantificeres til en liste over beviskrav, der er knyttet til 4 revisionsområder i 5.2. Listen over beviskrav skal omfatte dokumenter (med referencenummer og tidsstempel) indsendt og modtaget gennem Virk-portalen [13] [7] [8].

3. For hver kritisk tjeneste / system skal der identificeres: nøgleprogrammer, infrastruktur, netværk, identiteter, logning og overvågning, sikkerhedskopi- og gendannelseskapaciteter) [4] [15]. Afgræsningen af systemerne kontrolleres til troværdige kilder (inventarliste over hardware, hvem der er ansvarlige og identitetsregistre) og bruges til at fastlægge hvad der er indenfor omfanget for hvad der kan testes [3].

4. Identificer væsentlige leverandører til kritiske tjenester eller hændelsesrespons (hvis funktionen er udliciteret til konsulent) og udarbejd en bevisstrategi for hver leverandør: ISAE 3402-rapporter, direkte revisionstest hos virksomheden eller målrettet gennemgang af kontraktens indhold (sikkerheder, klausuler og ansvarsfraskrivelser) og hvordan virksomheden er stillet i tilfælde af en væsentlige hændelse hos leverandøren [1] [4] [3] [21].

5. Udarbejd en konsekvensbaseret risikovurdering, der forbinder trusselsniveauet for kritiske tjenester, kontrolmiljøets niveau og dækning, og spredningsrisiko (kan hændelsen påvirke flere kritiske systemer og tjenester) [1] [4] [15]. Udarbejd test der kan opnå tilstrækkelig og passende dokumentation for højrisikokriterier (f.eks. rettidig opdagelse og rapportering af hændelser, privilegeret adgangskontrol, sikkerhedskopiering og gendannelse) [2] [3].

6. Der skal indarbejdes en alvorlighedslogik ud fra om der er tale om: manglende overholdelse af lovgivningen, indvirkning på kritiske tjenester, tab af ekstern sporbarhed. For eksempel er manglende dokumentation for tidspunktet for opdagelse af hændelsen, som danner juridisk grundlag for underretningstidsfristerne (NIS2 artikel 23 og dansk lov § 13) lige så alvorlig som hvis opdagelsestidspunktet er dokumenteret og fristerne ikke er overholdt [1] [4]. Manglende dokumentation for godkendelse og tilsyn fra ledelsen vil normalt være væsentligt, da dette er governance-forpligtelser i NIS2 artikel 20 og dansk lovgivning § 7 [1] [4]. Forslag til forbedringer er kontrolsvagheder, der ikke udgør nogen øjeblikkelig manglende overholdelse, men øger risikoen for væsentlige hændelser. [1] [4] [15]. Omfangsbegrænsninger registreres når der ikke kan indhentes revisionsbevis og afhængigt af væsentligheden medføre en konklusion med forbehold, eller hvis begrænsningen er gennemgribende at der ikke kan udtrykkes konklusion efter ISAE 3000 [2].

5.5 Struktur for revisionsprogram

For at gøre revisionen struktureret og gentagelig, bruger modellen et kriterieregister / kontrolkatalog, som omdanner de juridiske forpligtelser til kontrolmål (herunder primære beviser, test og afvigelsesregler) ISAE 3000 kræver at revisionspåtegningen identificerer de gældende kriterier og ISA 500 kræver at revisionsprocedurer er designet til at indhente tilstrækkeligt og passende bevis, samt overveje relevansen og pålideligheden af disse beviser [2] [3].

Kriterieregisteret er versionskontrolleret og knyttet til de i planlægningen fastfrosne kriterier pr. dags dato, ud fra gældende lovgivning. Dette er ikke kun brugbart under igangværende revision, men vil også gøre revisionen sammenlignelig fra år til år, da det ellers vil anses som mangelfuldt, vil kunne forklares af daværende kriterier ud fra gældende lovgivning / officiel vejledning [10].

5.6 Bevisstrategi for leverandører

Sikkerhed i forsyningskæden er en stor del af NIS2-risikostyringsforanstaltninger, herunder sikkerhedsrelaterede forhold i forbindelse med direkte underleverandører og tjenesteudbydere [1] [4]. Leverandørbeviser betragtes derfor som kernebevis for de første 2 revisionsområder i 5.2 (risikostyringsforanstaltninger og hændelseshåndtering) og ikke bare som et supplerende bilag [1] [4] [15].

ISAE 3402 leverer en erklæring om kontroller hos en serviceleverandør, der med høj grad af sandsynlighed er relevante for den modtagne kundes bevismateriale vedrørende intern kontrol og forsyningskæden [21]. For revisioner der er underlagt NIS2, kan en ISAE 3402-erklæring anvendes som revisionsbevis for outsourcede IT-tjenester (f.eks. netværk, cloud, systemer, driftsansvar, sikkerhed), hvis de i erklæringen omfattede kontroller, overlapper de revisionsområder der er kræves afdækket i NIS2 (f.eks. tilgængelighed, adgangskontrol, ændringsstyring og overvågning) [1] [21]. ISA 500 tillader nemlig at revisor anvender information fra flere kilder, men kræver at der foretages en samlet vurdering af relevans og pålidelighed, herunder om beviset er internt eller eksternt genereret, og om der er uoverensstemmelser mellem de forskellige kilder [3].

ISAE 3402-erklæringer er dog afgrænset til bestemte kontrolmål, for en bestemt periode, og vil ofte være afhængige af supplerende kontroller, for at kunne opfylde kontrolmålene tilstrækkeligt. ISAE 3402 definerer supplerende kontroller som kontroller der forudsættes at er implementeret i brugerens (køber) [21]. Overholdelse af NIS2 kræver dog at specifikke pligter (ledelsens involvering og godkendelse, rettidig rapportering om hændelser og risikobaseret begrundelse), som ikke nødvendigvis vil være afdækket af en leverandørs ISAE 3402-erklæring [1] [4]. Revisionen kan derfor ikke anvendes en ISAE 3402-erklæring som erstatning for kontrol test hos leverandøren, men den kan underbygge de test der foretages [3] [21].

Procedurer for kobling mellem leverandørbeviser og NIS2-kriterier:

- Kortlæg hver kritisk leverandør til NIS2-relevante kontrolmål og identificer hvilke forpligtelser der fortsat er virksomhedens eget ansvar (f.eks. beslutninger om rapporteringspligt og indsendelse via Virk-portalen) [1] [4] [13].
- Indhent leverandørens seneste ISAE 3402 rapport og vurder omfang, periode og eventuelle undtagelser, fastlæg om den er lavet som type 1 (pr. statusdato) som fokuserer på hvad der er implementeret, eller type 2 (over en periode) som også dokumenterer den operationelle indvirkning [3] [21].
- Vurder leverandørens egne kontroller (adgangskontrol, overvågning, beredskabsplaner / eskaleringsveje) [3] [21].
- Udfør supplerende revisionshandlinger, hvis den eksisterende ISAE 3402-erklæring ikke dækker hele revisionsperioden og/eller hvis omfanget af kontrolmål ikke er tilstrækkeligt [3].
- Gennemgå kontrakter / SLA for klausuler der er relevante for NIS2 (sikkerhedsansvar, sårbarheder/patch, hændelsesunderretning, indsigt i den lovpligtige revision som den er underlagt) [1] [4].

- Hvis leverandørens revisionsbevis primært er baseret på certificeringer eller at være i overensstemmelse med rammeværktøjer (f.eks. ISO 27001), så brug det som understøttelse til beviser, men ikke i sig selv som bevis for overholdelse af NIS2; der skal stadig testes kontroller specifikt med henblik på NIS2 [1] [3] [18].

5.7 Praktisk eksempel: Start-til-slut-test af hændelsesunderretning

Dette eksempel viser en testprocedure, med dokumentationsspor for en væsentlig hændelse, fra opdagelsen til bevis for indsendelse til Virk-portalen. Testen er med fokus på NIS2 artikel 23 / dansk lovs §§ 12-13 (underretning af myndigheder), som specificerer de trinvise pligter og tidsfrister for underretning om væsentlige hændelser, fra det tidspunkt den underlagte virksomhed bliver opmærksom på hændelsen [1] [4].

1. Udvælg en registreret hændelse og definer revisionsperioden (opdagelses- og hændelsestidspunktet kan ligge i forskellige perioder). Fastlæg om revisionen omfatter hændelser hvor hændelsestidspunkt og opdagelses- og / eller underretningstidspunktet overlapper revisionens skæringsdato og dokumentér afgrænsningsreglen for skæringsdato [2] [3]. Stikprøven skal med rimelighed opfylde på danske lovs definition på en væsentlig hændelse (alvorlig driftsforstyrrelse, økonomisk tab og / eller væsentlig skade for andre personer) [4].
2. Fastlæg tidspunktet for bevidsthed om hændelsen (SIEM-alarm, SOC-sagsnummer, driftsovervågning) og identificer det første dokumenteret tidspunkt for hvornår virksomheden blev opmærksom på at hændelsen var indtruffet og hvor vidt den var væsentlig (eller muligvis væsentlig) [1] [4] [3]. Bevidsthedstidspunktet skal være veldokumenteret, da det definerer de lovpligtige trinvise tidsfrister (24 timer, 72 timer, endelig) [1] [4].
3. Gentag vurdering af klassifikation ud fra virksomhedens dokumenterede beviser, i henhold til dansk lov § 12, ved at spore konsekvensanalysen tilbage til de 2 betingelser i § 12 stk. 2 (alvorlig driftsforstyrrelse / økonomisk tab og / eller betydelig skade for andre personer). Hvis virksomheden har klassificeret hændelsen som ikke-væsentlig, men beviser tyder på at den burde være klassificeret som væsentlig, eller der er mangler / huller i dokumentationssporet, skal dette registreres som en afvigelse i klassifikationskontrollen, og vurdere om det skyldes underliggende svagheder i governance eller risikostyring [1] [4].
4. Gennemgå indsendte underretninger og deres tidsstempel. Kontroller at den tidlige advarsel blev indsendt inden for de lovpligtige 24 timer efter opdagelsen, at hændelsesunderretningen blev indsendt inden for 72 timer, og kontroller om der er afgivet statusrapporter (hvis der er anmodet om det fra myndighederne), samt om den endelige rapport er indsendt inden for en måned [1] [4]. Hvis hændelsen stadig var igangværende (ikke fuldstændigt afhjulpet) på tidspunktet for den endelige rapport (1 måned), skal der kontrolleres at det i stedet blev indsendt som statusrapport og at den endelige rapport er indsendt efterfølgende [1] [4].
5. Afstem portal-indberetninger med de interne beviser, herunder kvitteringer og kopier af de indsendte underretninger. Afstem dem med det internt dokumenterede hændelsesforløb (tidslinje for hændelsen, berørte tjenester, alvorlighed, indikationer på kompromittering og afhjælpende foranstaltninger) [8] [3]. Virk-vejledningen instruerer om at downloade kvitteringer/kopier for portal-indsendelser og mangel derpå vil være bevismangel [8].
6. Vurder dokumentationens pålidelighed og afklar eventuelle uoverensstemmelser. Anvend ISA 500's krav til dokumentationspålidelighed (internt genereret, understøttet af uafhængige kilder og

undersøg om der er overensstemmelse mellem dokumentation fra forskellige kilder, f.eks. tidsmæssige afvigelser). Foretag supplerende revisionshandlinger, indtil huller / uoverensstemmelser i tidslinjen kan afdækkes, ellers skal det registreres som en begrænsning i revisionens omfang [2] [3].

7. Vurder afvigelsens alvor og indvirkning på konklusionen. Manglende overholdelse af lovbestemte tidsfrister eller manglende dokumentation på underretninger vil typisk være en kritisk afvigelse, da det er en direkte mangel på overholdelse af juridiske forpligtelser, som underminerer ekstern sporbarhed [1] [4]. Hvis der er væsentlige dele af hændelsesforløbet som der ikke kan indhentes dokumentation for, skal det betragtes som en begrænsning af omfanget og der skal overvejes hvor vidt der afgives konklusion med forbehold eller ingen konklusion, i henhold til ISAE 3000's vurdering af væsentlighed [2].

5.8 Rapportering og opfølgning

Modellens rapporterings- og opfølgningsdel er designet til at understøtte både beredskabsforbedringer og senere uafhængig revision, samtidig med at revisionen er sammenlignelig fra år til år, gennem fastfrysning af kriterier og kortlægning til kontrolmål [2].

Hver observation rapporteres ud fra: kriterie-ID (kriterieregister) og juridisk grundlag, betingelse (hvad der blev observeret), kriterie (hvad der kræves), effekt (risiko for væsentlig indvirkning på kritiske tjenester), bevismateriale (dokumentation for fundet) og hjælpende foranstaltninger (med ansvarlig person, tidsstempler og tidsfrister) [2] [3]. For portalbaserede forpligtelser (registrering og ajourføring af denne, samt underretning om hændelser), angiver rapporteringen de beviser der er anvendt (med referencenumre og tidsstempler), så bevisrækkefølgen kan gentages [13] [7] [8].

Ifølge ISAE 3000 afgiver revisor en konklusion i forhold til de anvendte kriterier og en konklusion med forbehold, hvis der er væsentlig manglende overholdelse af forpligtelser og / eller fejl, eller hvis en omfangsbegrænsning gør at der ikke kan hentes tilstrækkeligt og egnet bevis [2]. Modellen rangerer observationer efter alvorlighed (se 5.4). Kritiske afvigelser (lovbestemte tidsfrister og -pligter), behandles som mulig væsentlig manglende overholdelse. Væsentlige afvigelser (f.eks. manglende dokumentation for ledelsesgodkendelse, mangler i risikostyringsforanstaltninger) kan også være væsentlige, afhængigt af deres indvirkning. Forbedringsforslag præsenteres særskilt for konklusion, så de ikke blandes sammen [1] [4] [2].

Til de efterfølgende revisioner skal tidligere revisioners (oftest nok med den seneste) fastfrosne kriterieregister videreføres, så de kan sammenlignes med de aktuelle kriterier og en ændringslog, så revisor kan identificere hvilke kriterier der er ændret og på hvilket juridisk grundlag [2]. Gentest af tidligere revisioners kritiske / væsentlige mangler, ændringer i virksomhedens omfang (nye kritiske tjenester og ændringer på leverandørsiden) og eventuelle ændringer i de officielle vejledninger eller portal-workflows, der påvirker bevisindsendelse og formatet dokumentationen derfra udlæses [4] [13] [9] [8]. For at sikre at konklusionerne på tværs af revisioner, forbliver fortolkelige og sammenlignelige over tid, skelner rapport mellem, 1) præsentation i forhold til de aktuelle fastfrosne kriterier, 2) ændringer i kriterierne siden den forrige revision, der har ændret forventningerne (f.eks. nye datafelter i indberetningsportalen, eller nye supplerende EU-krav for virksomheder i den digitale sektor [10] [16] [2].

6. Sammenligning med andre lande

Dette kapitel besvarer U3, ved at sammenligne Belgien, Tyskland, Rumænien, Slovakiet og Ungarn ud fra et revisionsperspektiv. Landene er udvalgt på baggrund af at de på visse områder har været længere fremme end Danmark i implementeringen af NIS2, samt at de differentierer sig geografisk og kulturelt. Med længere fremme, menes der at der er implementeret operationelle mekanismer der omdanner de juridiske NIS2-forpligtelser til præcise revisionskriterier og beviser (f.eks. officielle vejledninger, indberetningsportaler og de beviser der dannes derfra). Formålet er at identificere mekanismer som Danmark kan anvende for bl.a. at forbedre bevisføring, gentagelighed og sammenlignelighed i revisioner fra år til år.

6.1 Hvorfor sammenligning på tværs af landegrænser er vigtig for revisionen

NIS2 er på EU-niveau baseret på principper inden for centrale områder (krav om foranstaltninger der er passende og proportionelle i forhold til risici), så den nationale implementering afgør hvordan forpligtelserne skal kontrolleres, hvilken myndighed der tilser hvilke sektorer, hvilke oplysninger der er krævet som minimum i indberetningerne og hvilken dokumentation der kan udlæses herfra og anvendes som eksternt revisionsbevis [1].

Sammenligningen er ud fra de forskellige landes implementerede mekanismer, og ikke egentlige resultater (ny lov, begrænset datagrundlag), hvorfor der heller ikke kan rangeres mellem landene. Der undersøges hvorvidt implementeringerne skaber gentagelige revisionsprocedurer og klare beviskæder.

Sammenligningskriterier:

- **Tidspunkt og stabilitet.** Om gældende regler / retningslinjer (herunder officielle vejledninger) er trådt i kraft, herunder om ændringer hertil offentliggøres med tydeligt versionsbeskrivelse / tidsstempel (for at kunne fastfryse kriterier) og eventuel ændringslog.
- **Ansvarsfordeling (myndigheder).** Er kompetente myndigheder (ud fra sektor), CSIRT, og kontaktpunkter er tydelige anviste (dokumentation og placering af ansvar).
- **Omfangsværktøjer.** Om staten stiller tilstrækkelige rammeværktøjer til rådighed, eller juridiske afgørelser til at sætte præcedens (understøtter gentagelig revision, omfang og klassificering).
- **Portal- og workflowværktøjer.** Om registrering (klassificering) og indberetning af hændelser, er portalbaseret, med klart strukturerede datafelter, tidsstempler og bekræftelser / kvitteringer (beviser).
- **Vejledningsniveau.** Om de officielle vejledninger er i overensstemmelse med de inputfelter der i portalerne, og der beskrives minimumsoplysninger for registrering og underretning om hændelser (reducerer fejlfortolkninger).
- **Revisionsmiljø og håndhævelsesforanstaltninger.** Om staten fastlægger eksterne rapporteringskrav (f.eks. rapporteringsformater og registre over revisorer / MNE-numre) og signalerer tilsynsforventninger (understøtter sammenlignelighed og pålidelighed).

I nedenstående tabel 6.1 ses kontrolområde, tilhørende mekanismer og typisk dokumentation:

Tabel 6.1

Kontrolområde	Mekanismer	Revisionsbeviser
Kriteriestabilitet	Versionsnummer på loven / vejledning, samt dato for vedtagelse og ikrafttrædelse.	Kopi af lovtekst / vejledning pr. given dato, med versionsnummer og datering, til fastfrysning af kriterier.
Afgrænsning af omfang	Officielle værktøjer / workflows eller afgørelser.	Gemte inputs og outputs for værktøjer, samt notater heromkring, gør revision genudførlig og mulig at efterprøve.
Registrering	Struktureret og forståelig portal for korrekt registrering og ajourføring, med obligatoriske felter.	Kopi / kvittering for registrering, med referencenummer og tidsstempel.
Hændelsesrapportering	Indberetningsportal der understøtter de trinvise deadlines og obligatoriske felter for hvert trin.	Kopi / kvittering for indsendelser, med referencenummer og tidsstempel.
Mapning til myndigheder	Kortlægning af de kompetente myndigheder for de forskellige sektorer og CSIRT.	Regler for videregivelse af informationer (hvem får hvad). Eventuel efterfølgende korrespondance.
Revisionssystem	Eksterne revisionsspor (registre, standardformater, indberetningsportaler)	Sammenlignelig rapportering, dokumentation overfor tilsynsmyndigheden og at revisor har den rette faglige kompetence.

6.2 Belgien

Belgien indførte NIS2 på nationalt plan gennem loven af 26. april 2024 om etablering af en cybersikkerhedsramme for netværks- og informationssystemer af almen interesse for den offentlige sikkerhed [22] [23] [24].

Den belgiske implementering er gennem en kombination af national NIS2-lov, et kongeligt dekret, portalworkflows, officielle vejledninger af Centre for Cybersecurity Belgium (CCB) og Safeonweb [25] [24].

Safeonweb-siden beskriver den nationale lovs ikrafttrædelsesdato, 18. oktober 2024 og definerer at det er loven der implementerer de vigtigste bestemmelser (herunder at CCB er den overordnede nationale myndighed for cybersikkerhed) [24].

Ud fra et revisionsmæssigt synspunkt har Belgien formået at omdanne de centrale forpligtelser i NIS2 til praktisk anvendelige portal-workflows og vejledninger, som klart og præcist definerer minimumsdata og tidsfrister [26] [27] [28].

Overordnede mekanismer og deres indvirkning på revisionen:

- Registreringsfrister og kobling mellem, om man er omfattet, og portalen. Safeonweb@Work's guide, angiver frister for registrering af virksomheder der er underlagt NIS2 (herunder præcisering af de forskellige sektorer), samt henviser til deres portalbaserede registreringsworkflow [27]. Dette gør at registreringen kan bruges som revisionsbevis, da indsendelser og kvitteringer fra portalen kan bruges til at kontrollere om de er indsendt rettidigt og korrekt udfyldt [27].
- Den officielle vejledning (Safeonweb), forklarer forventninger til input i, ned til de enkelte datafelter, hvilket giver en forståelig definition af minimumsdata ved registreringen, hvilket revisor kan bruge til at vurdere fuldstændighed, præcision, rettidighed [26]. Typisk revisionsdokumentation omfatter en kopi af de indsendte oplysninger (og eventuel kvittering for modtagelse af denne), hvis tilgængeligt, skærmbilleder fra portalen med angivet status, dokumentation for at indberetter er bemyndiget / har fuldmagt til at foretage denne på vegne af virksomheden [26].
- Den samme portal som anvendes til registrering, er også der hvor hændelsesunderretninger skal indberettes (notif.safeonweb.be) [29]. Typisk revisionsdokumentation vil som ved registrering være kopier, kvitteringer for modtagelse samt efterfølgende korrespondance med tilsynsmyndighederne [29].
- Eksternt generede beviser for korrespondance med myndigheder. CCB beskriver at korrespondance efter underretning om hændelser, foregår via e-mail, med tilknyttet referencenummer (fungerer som bevis for dokumentation og til klar kommunikation mellem myndigheder og virksomheder) [30].
- Officiel vejledning om underretningsforløb. CCB har en praktisk vejledning om NIS2 underretninger, som beskriver de trinvise indberetninger og forventninger til tidsfrister, hvilket understøtter kriterier for revisionstest, hvor man genskaber hændelsesforløbet, dets beslutninger og beslutningsgrundlag [28].

Samlet set har Belgien skabt en klar proces, fra de juridiske forpligtelser, til arbejdsgange og bevismateriale. Loven og det kongelige dekret fastlægger kravene, mens Safeonweb- og CCB-vejledninger gør dem lette at forstå og indsende via online-portalen, der genererer dokumentation.

6.3 Tyskland

Tyskland indførte NIS2 på nationalt plan via Bundesgesetzblatt I nr. 301 af 5. december 2025 [31].

Bundesamt für Sicherheit in der Informationstechnik (BSI) beskriver at gennemførselsloven træder i kraft d. 6. december 2025 [32] [33]. Der er annonceret en BSI-portal, som vil blive åbnet d. 6. januar 2026, og fungere som det officielle værktøj til at indberette væsentlige hændelser jf. NIS2 [32].

For at understøtte en gentagelig afgrænsning, tilbyder BSI et portal-værktøj. I portalen stilles der spørgsmål til brugeren, som trækker tråde til lovgivningen, og dermed kan hjælpe virksomhederne med at vurdere om de er omfattet af NIS2 eller ej [34].

BSI stiller desuden et vejledningsdokument med et beslutningstræ til rådighed, som yderligere hjælpemiddel, der også kan arkiveres som en del af revisionsbeviset [35].

Overordnede mekanismer og deres indvirkning på revisionen:

- Der er fastlagt juridisk grundlag via offentliggørelsen i Bundesgesetzblatt, hvilket giver klare kriterier for revisionen og gør det muligt at fastfryse dem når revisionen er påbegyndt [31].

- BSI portalværktøjet og vejledningen med beslutningstræet gør det muligt at gentage vurderingen om hvorvidt virksomheden er underlagt NIS2, teste om ledelsen har vurderet korrekt (sektor, størrelse, aktiviteter) [34] [35].
- BSI forklarer at registreringen under NIS2 ikke er tilgængelig endnu, men at den vil blive sat i drift primo januar 2026 [33]. De første revisioner underlagt NIS2, kan derfor kræve som alternativt bevis til en af gode grunde ikke-eksisterende registrering, at virksomheden kan bevise at de er klar til at blive registreret (beslutninger ud fra de officielle vejledninger samt underliggende dokumentation), indtil portalen åbner og muliggør registrering [33].
- Når portalen er åbnet, vil den være i stand til at danne eksterne beviser i form af kopier / kvitteringer for registrering / indberetninger, samt dokumentere efterfølgende kommunikation med myndigheder [33].

Til trods for at Tyskland ikke har åbnet portalen endnu, og dermed muliggjort registrering, så har de stadig været på forkant i forhold til hjælpeværktøjerne til vurdering om virksomhederne er underlagt NIS2 og hvilken sektor, hvilket højst sandsynligt fører til en mere problemfri national implementering [32] [34] [35].

6.4 Rumænien

Rumænien indførte NIS2 på nationalt plan gennem regeringsdekret (OUG) nr. 155 af 30. december 2024 om cybersikkerhed i netværks- og informationssystemer i det civile nationale cyberspace [36]. Dekretet blev offentliggjort i Monitorul Oficial nr. 1332 af 31. december 2024 [36].

Det rumænske parlament godkendte efterfølgende OUG 155/2024 gennem lov nr. 124/2025 [37].

Rumænien har i deres nationale center for cybersikkerhed (DNSC) ordrenr. 1 af 11. august 2025, fastlagt hvilke oplysninger der skal indsendes og i hvilket format og til hvilke kanaler i forbindelse med registreringen. Ordren er offentliggjort i Monitorul Oficial nr. 776 af 20 august 2025. Desuden vil der også blive stillet et portal-værktøj til rådighed, til hjælp for at vurdere om virksomheden er underlagt NIS2 og hvilken sektor [38] [39].

Overordnede mekanismer og deres indvirkning på revisionen:

- Det juridiske grundlag er fastlagt via offentliggørelsen i Monitorul Oficial. DNSC udvikler to værktøjer/portaler til at hjælpe med registreringen. Et risikovurderingsværktøj (ENIRE) og et værktøj til registrering / underretning / kommunikation [39].
- Registrering kan udføres via en fil der genereres i et lokalt downloadet program, eller direkte via online portal-værktøj. Der anbefales dog at bruge online-portalen hvis muligt [38].
- Der forklares at kopi / kvittering af registreringsformular og underretninger skal arkiveres som brug for til revisionsdokumentation, frem for skærmbilleder [38].
- Foruden online-portalen kan der også indsendes via e-mail og endda også fysisk post, hvor der vil blive kvitteret for modtagelsen inden for 5 arbejdsdage [38].

Rumænien har udarbejdet vejledninger / bilag til den nationale lov, samt stiller en bred vifte af værktøjer til rådighed som hjælp til registreringen. Ligeledes imødekommes der mange muligheder for indsendelse, også

fysisk post, hvor de fleste andre lande har begrænset sig til online-delen, som dog nok også vil generere de bedste revisionsbeviser [38] [39].

6.5 Slovakiet

Slovakiet indførte NIS2 på nationalt plan gennem lov nr. 366/2024, der blev offentliggjort i lovsamlingen (Zbierka zákonov) som en lovændring til den eksisterende nationale lov om cybersikkerhed [40].

Deres nationale cybersikkerhedsmyndighed (NBÚ) har udarbejdet vejledninger og online-portal [41].

Online-portalen er en samlet portal, for både interaktiv vejledning, underretninger og korrespondance i forbindelse med NIS2 [42] [43] [44] [45].

Overordnede mekanismer og deres indvirkning på revisionen:

- Den samlede online-portal omdanner præcist de juridiske forpligtelser til et interaktivt værktøj til klassificering, underretning og korrespondance. Dette letter arbejdet både for de underlagte virksomheder og revisor, da det betydeligt reducerer antallet af eksterne kilder hvorfra der skal søges information [41] [42].
- Officielle vejledninger fra NBÚ er angivet med version, hvilket kan hjælpe revisor under igangværende revision til at fastfryse kriterier [44] [45].
- Inputs i portal-værktøjet, sammen med dokumentation for grundlaget, og de kvitteringer og korrespondance der dannes fra portalen, kan fungere som klart revisionsbevis og gør det muligt at genteste beslutninger for klassificering [46].

Slovakiet har fokuseret fuldt ud på en samlet, enkel online-løsning, der indeholder alt fra det juridiske grundlag, interaktive vejledninger, registrering, underretning og korrespondance med myndigheder, hvilket letter arbejdet betydeligt for både de underlagte virksomheder og revisor [41] [42] [44] [45].

6.6 Ungarn

Ungarn indførte NIS2 på nationalt plan gennem lov LXIX (69) om cybersikkerhed fra 2024 (2024. évi LXIX. Törvény), som trådte i kraft d. 1. januar 2025 [47].

Den ungarske tilsynsmyndighed for regulerede aktiviteter (SZTFH) fører et offentligt register over IT-revisorer [48] [49]. SZTFH har en online-formular (SZTFH 411) til indsendelse af IT-revisionsrapporter og fører et centralt register over tilhørende formularer og specifikationer til rapporterne [50].

SZTFH har en vidensdatabase (Tudástár), som indeholder vejledninger, artikler og øvrigt materiale til de underlagte virksomheder, om IT-revisioner. Her er der også beskrevet at den første IT-revision omfattet af NIS2, skal være gennemført senest 30. juni 2026 [51] [52] [53].

Overordnede mekanismer og deres indvirkning på revisionen:

- Det offentlige register over IT-revisorer, hjælper virksomheder og tilsynsmyndigheder samt eventuelle tredjeparter med at kontrollere hvor vidt revisionen er udført af en kvalificeret revisor [48] [49].

- Online-formular til indsendelse, med forbindelse til centralt register hvor der arkiveres rapporter med tilhørende formularer og specifikationer, gør revisionskonklusionerne sammenlignelige på tværs af revisorer, og kan bruges som revisionsdokumentation [50].
- Vidensdatabasen hjælper til at skabe standardiserede forventninger til revisionskravene og fastfrysning af kriterier [51] [52].

Ungarn skiller sig ud ved ikke kun at have lavet portaler til registrering og indberetning, samt vidensdatabasen. De har også lavet register og revisorer og de indsendte rapporter, med tilhørende formularer og specifikationer. Derudover har de allerede sat en deadline for den første revision. [48] [50] [53].

6.7 Hvad kan Danmark lære fra de andre lande

Gennemgangen af de udvalgte andre landes implementeringsprocesser tyder på at revisionsmulighederne forbedres når der fra officielle kilder implementeres interaktive portaler, vejledninger med eksempler og beslutningstræ, versioneret og dateret lovgrundlag og vejledninger. Dette skaber lidt forståelige revisionsmål med troværdig (officiel vejledning) kobling fra det juridiske til det praktiske. Mange af disse elementer er bredt overholdt i alle sammenligningslandene. Der er dog enkelte variationer. Nedenstående er de tiltag som jeg mener at Danmark kan lære af. Der ses ikke i forhold til landenes trusselniveau i relation til hinanden, men udelukkende ud et revisionsteknisk perspektiv.

- Én samlet online NIS2-portal, hvor vejledning, værktøj til klassificering/omfang, underretninger, korrespondance og sagsstyring er samlet (se Slovakiet).
- Et samlet register med alle IT-revisionsrapporter, udfyldte formularer og specifikationer (se Ungarn).

7. Konklusion

Dette kapitel konkluderer specialet, ved at sammenfatte resultaterne fra kapitel 2-6, samt besvare undersøgelsesspørgsmål 1-3. Specialet vurderer overholdelse af NIS2 som et revisionsproblem. De lovbestemte forpligtelser skal omdannes til revisionskriterier, tydelige beviser, gentagelige testprocedurer og klare afvigelsesregler. Sammenfatningen følger det kildehierarki som der er beskrevet i kapitel 2, samt den bevisdisciplin og rapporteringslogik der er beskrevet i kapitel 4.

Det praktiske revisionsgrundlag dannes ud fra en samlet pakke af kriterier: NIS2-forpligtelser på EU-niveau, dansk lovgivning, officielle danske vejledninger og portalworkflows. Især arbejdshandlingerne i portalen skaber brugbare eksterne beviser, i form af kopier af indberetninger og kvitteringer for medtagelse, dateret med tidsstempel og referencenummer, som kan opbevares som en del af dokumentationen for hændelsesforløbet. Da vejledninger og portalworkflows kan ændre sig over tid, anvender specialet kriteriefastfrysning og kortlægning af ændringer til kriterier (enten i det juridiske grundlag eller fra den officielle fortolkning), for at sikre at revisionskonklusioner er forståelige og sammenlignelige på tværs af de årlige revisioner (se 2.2 – 2.4, 3.3 og 4.6).

7.1 Besvarelse af undersøgelsesspørgsmål 1

U1 spørger: Hvilke krav i NIS2 er mest relevante for IT-revisionen og hvordan kan IT-revisionen struktureres til at vurdere de krav til risikostyring, hændelseshåndtering, governance og rapportering, som NIS2 stiller? Specialet besvarer U1, ved at kombinere den danske fortolkning af implementeringen som beskrevet i kapitel 3, med den gentagelige revisionsmodel i kapitel 5. Modellen indarbejder transformationskæden (Kontrolmål -> Beviser -> Testprocedurer -> Afvigelsesregler) fra afsnit 2.3 og bruger bevis- og afvigelseslogikken fra kapitel 4, for at sikre gentagelighed og ensartede konklusioner (se 2.3, 3.1 – 3.7, 4.4 – 4.7 og 5.1 – 5.8).

Vurderinger af reviderbarheden, starter med en vurdering af omfanget der kan gentages: Er virksomheden underlagt NIS2? Hvilken sektor er virksomheden klassificeret som? Er virksomheden væsentlig eller vigtig i henhold til de danske regler? Fastlæggelse af omfanget er ikke kun vigtigt i forhold til planlæggelsen, men i sig selv en revisionskontrol, da det afgør hvilke juridiske forpligtelser der påhviler virksomheden, samt hvilke tilsynsmæssige forventninger der følger heraf. Kapitel 3 forklarer at Danmarks registreringsworkflow kræver at virksomheden angiver sin klassificering og sektor, hvilket gør den underliggende klassificeringsbegrundelse til en del af det krævede bevismateriale (se. 3.2 – 3.3). I forhold til revisionen, betyder det at omfangsmemoet skal kunne henføres til den konkrete virksomhed, dateret og underbygget af den dokumentation der lå til grund for klassifikationen. Ellers vil senere test for korrekt registrering, governance, sikkerhedsforanstaltninger og hændelsesunderretning, ikke være funderet i et forsvarligt sæt revisionskriterier (se afsnit 3.2 og 5.3).

Kapitel 3 fastslår at de vigtigste danske NIS2-forpligtelser er overholdt gennem den obligatoriske digitale arbejdsgang i portalen. Da output fra denne portal kan fungere som primært bevismateriale (kopier / kvitteringer, tidsstempel, referencenummer, digital post). Specialet behandler derfor registreringen som en kontrol i sig selv, der skal ajourføres løbende og ikke bare en enkeltstående opgave. De underlagte virksomheder skal kunne påvise fuldstændighed (alle omfattede enheder er registreret), nøjagtighed (korrekt input og beslutningsgrundlag), rettidighed (registrering og ajourføring inden for de fastlagte tidsfrister) og integritet (personen der har indsendt, er autoriseret og der opbevares dokumentation). Disse

påstande og tilhørende beviser er forklaret i afsnit 3.3 og 5.2, og de udgør et praktisk grundlag for gentagelige revisionstest, der kan udføres revision efter revision (se afsnit 3.1 -3.3 og 5.2).

Både EU-loven og den danske lov gør ledelsesinvolvering til et revisionsmål. Ledelsen skal indledningsvist godkende foranstaltninger til styring af cybersikkerhedsrisici, løbende overvåge implementeringen og selvfølgelig være tilstrækkeligt uddannet for at kunne varetage ansvaret. Kapitel 3 forklarer dette ud fra konkrete beviser (referater, godkendelses, overvågningsrapportering, sporing af afhjælpende foranstaltninger og dokumentation for gennemført relevant uddannelse / kursus). Disse beviser hører alle sammen under governance og skal testes særskilt og ikke bare som en del af vurderingen af de enkelte hændelser, da governance-vurderingen danner grundlag for den overordnede risikovurdering af virksomheden og dens kritiske tjenester (se afsnit 3.4 og 5.2).

Kapitel 3 identificerer minimumsforanstaltningerne og forklarer hvorfor udtrykkende ”hensigtsmæssig” og ”proportionel” skal gøre reviderbare, ud fra dokumenteret begrundelse knyttet til vurdering af risiko og eventuel konsekvens. Kapitel 5 implementerer dette, ved at kræve at hver foranstaltning kortlægges i forhold til et kontrolmål og underliggende dokumentation, der er specifikt for de kritiske tjenester (f.eks. adgangskontrol, håndtering af sårbarheder og patch, logning og overvågning, sikkerhedskopiering og gendannelse, leverandørstyring). Revisionsopgaven vil derfor ikke være begrænset til at bekræfte om der findes politikker, men der skal testes om de er designet og implementeret med henblik på at reducere de dokumenterede risici der er forbundet med de kritiske tjenester, og hvis der findes historik, om disse beviser understøtter driftseffektiviteten i perioden (se afsnit 3.5, 4.4 og 5.1 – 5.2).

Kapitel 3 forklarer at rapportering om hændelser kun kan kontrolleres, når den interne dokumentation stemmer overens med hvad der er generet af eksterne beviser fra indberetningsportalen. Der kræves trinvise underretninger gennem portalen, med lovbestemte tidsfrister, ud fra hvornår virksomheden blev opmærksom på at hændelsen var væsentlig. Dette gør kendskabet til om ikke bare hændelsen, men beslutningen om hvorvidt den var væsentlig til et kontrolmål. Der er derfor defineret et minimumssæt af beviser for hændelser (tidsstemplede log og overvågning heraf, dokumenterede og begrundede beslutninger om klassificering og omfang, generede kvitteringer fra portalindberetninger og eventuel efterfølgende korrespondance). Kapitel 5 indeholder et praktisk eksempel fra start til slut, der afstemmer interne registreringer med portalindberetninger, så indhold og rettidighed kan vurderes (se 3.6 og 5.7).

U1 besvares ikke kun ud fra hvad der skal testes, men også hvordan testresultaterne skal fortolkes. I afvigelsesmodellen behandles påvist manglende overholdelse af et krav i henhold til de fastfrosne kriterier, som en manglende overholdelse. Hvorimod manglende evne til at indhente tilstrækkelige og relevante beviser, efter forsøg på alternative procedurer, behandles som en begrænsning af omfanget. Sondringen herimellem er central i de første revisioner underlagt NIS2, hvor vejledninger, portalworkflows er nyligt implementerede og stadig under udvikling (se 4.7 og 5.1).

7.2 Besvarelse af undersøgelsesspørgsmål 2

U2 spørger: Hvordan kan internationale standarder og frameworks som ISA 500, ISAE 3000/3402, ISO 27001, COBIT og COSO, anvendes som revisionskriterier for NIS2-overholdelse, og hvilke udfordringer skaber forsinket national implementering for planlægning, væsentlighedsvurdering og bevisindsamling for IT-revisionen? Specialet besvarer U2 gennem de handlinger der er beskrevet i kapitel 2 og 4. Loven er fundamentet for kriterierne, mens standarder og rammeværktøjer bruges til at strukturere kontrolmål, vurdere beviskvalitet og udtrykke konklusioner med klare afvigelsesregler (se 2.2, 4.1 – 4.7 og 5.3).

Kapitel 2 definerer et kildehierarki for at forhindre afvigelser mellem de juridiske forpligtelser og kriterierne. NIS2 på EU-niveau og den danske lov er bindende, mens de officielle danske retningslinjer / vejledninger og portalworkflows anvendes til at implementere hvordan forpligtelserne skal udføres og dokumenteres. Kildehierarkiet behandles som et kriteriesæt, der skal dokumenteres og fastfryses ved opstart af hver revision, da vejledninger og portal-workflows kan ændres løbende. Det betyder at som del af planlægningen skal de fastfrosne kriterier defineres pr. en given dato, så der er rød tråd fra kriterier til konklusionen, hvis kriterierne ændres undervejs (se 2.2 - 2.4 og 4.6).

ISAE 3000 anvendes som rammeværktøj for om kriterier er egnede. Der indarbejdes 2 kontroller: et kriterieregister som knytter de juridiske forpligtelser / kriterier til reviderbare kontrolmål, samt afvigelsesregler og potentiel indvirkning på den endelige konklusion. Dette understøtter gentagelighed af revisionstest og reducerer risikoen for fejlfortolkning af kriterierne, da der er knyttet konkrete kontrolmål (og afvigelsesregler) til de enkelte forpligtelser (se 4.1 – 4.2 og 4.7).

ISA 500's principper om tilstrækkelighed og hensigtsmæssighed, anvendes til at vurdere og prioritere beviser med høj pålidelighed. Som bevis for indberetninger gennem portalen, vil der blive genereret beviser i form af kopier af indberetninger, kvittering for modtagelse, korrespondance gennem digital post, alle med tidsstempel og referencenummer. Disse eksternt generede beviser har højere pålidelighed end internt generede beviser og mundtlige forklaringer, da disse kan ændres. Når de eksternt generede beviser understøttes af den internt arkiverede dokumentation, vil det være muligt at gentage beslutnings- og hændelsesforløb, for at vurdere om omfanget er tilstrækkeligt og tidsfrister er overholdt.

Kapitel 4 forklarer hvordan rammeværktøjer kan understøtte en konsekvent opbygning af kontrolmål og revisionsprogrammer, men at følge disse rammeværktøjer til punkt og prikke, ikke i sig selv er lig med overholdelse af NIS2-forpligtelser. Rammeværktøjerne bruges til at udtrykke hvordan en god kontrol ser ud med hensyn til governance, risikostyring og intern kontrol, samt hvordan kontrollen kan henføres til de juridiske forpligtelser i det udarbejdede kriterieregister. Dette gør at man kan vurdere hvilke yderligere handlinger der skal til (udover rammeværktøjerne) for at overholde NIS2-forpligtelserne (se 4.3 og 5.5).

Det er ganske få virksomheder som ejer hele forsyningskæden selv. Kapitel 5 beskriver hvordan der kan indhentes leverandørbevis hos kritiske leverandører (særligt med ISAE 3402-erklæring), hvor underliggende rapporter og erklæringer, kan underbygge test hos leverandøren, men ikke i sig selv helt erstatte dem. Der kræves derfor altid en individuel vurdering af den underlagte virksomheds kritiske leverandører, gennem kontraktuelle forpligtelser, ansvarsfraskrivelser og leverandørens eget kontrolmiljø, da en virksomheds leverandørers overholdelse af NIS2 kan være mindst lige så vigtig som virksomhedens egen overholdelse (se 4.3 og 5.6).

Kapitel 4 forklarer hvorfor fastfrysning af kriterier er nødvendigt, både i forhold til mulige ændringer i lovgivning, men særligt fordi den forsinkede implementering kan betyde at kriterier og officielle retningslinjer ikke endnu er stabiliseret og muligvis vil ændre sig væsentligt i den første tid. Fastfrysning af kriterier og sporing af ændringer hertil, gør revisioner sammenlignelige, da der kan specificeres hvordan disse ændringer har påvirket grundlaget for den næste revision i forhold til den tidligere, så hvad der kan ligne fejl og mangler fra tidligere revision, vil kunne begrundes ud fra daværende kriteriegrundlag (se 2.4, 4.6 og 5.3).

Afvigelsesregler forklares i afsnit 4.7. Der præsenteres et praktisk eksempel på et regelsæt for hvornår manglende beviser bliver en begrænsning af omfanget, og hvornår disse begrænsninger bør påvirke konklusionen. I praksis kan manglende bevis for indsendelse eller dokumentation for hvornår en virksomhed fik kendskab til hændelsen og hvorvidt den er væsentlig, være lige så vigtig som påviselige

forsinkelser, da tidsfristen defineres ud fra en rimelighedsvurdering af hvornår virksomheden blev bevidst eller burde være blevet bevidst om hændelsen og dens omfang (se 3.6, 4.7 og 5.7).

7.3 Besvarelse af undersøgelsesspørgsmål 3

U3 spørger: Hvilke konkrete tiltag har Belgien, Tyskland, Rumænien, Slovakiet og Ungarn valgt i deres implementering af NIS2, som Danmark kan drage nytte af? Specialet besvarer U3 gennem opsummering af de overordnede tiltag som de enkelte lande har implementeret. For at holde kapitlets omfang nede, er disse tiltag ikke vurderet i samme grad som for Danmarks vedkommende. Der er heller ikke udvalgt specifikke sammenligningspunkter eller lavet rangorden blandt landene og deres tiltag. Kapitel 6 forklarer de forskellige tiltag og sammenhængen mellem de juridiske forpligtelser og arbejdsgange i forhold til revisionen.

Da alle lande er underlagt den samme EU-lov, er det klart at der er overlap i forhold til implementering af de samme tiltag. Fokus har derfor været på de af tiltagene som skiller sig tilstrækkeligt ud, vurderet ud fra om de forbedrer muligheden for revision. Der er vurderet ud fra de på nationalt plan officielle vejledninger og værktøjer til klassificering (sektorvalg), registrerings- og indberetningsmuligheder gennem portal som indarbejder minimums krævede datafelter og tidsfrister, bevismateriale der kan opbevares og bruges til at spore hændelsesforløbet. Disse tiltag reducerer risikoen for fejlfortolkninger af forpligtelser / kriterier og gør det muligt at gentage processen under revision (se afsnit 6.1 – 6.6).

Sammenligningen fremhæver forskellige måder som landene har udmærket sig på. Belgien har særligt nøje beskrevet retningslinjer og portal-workflows (se 6.2). Tyskland stiller interaktivt værktøj til rådighed for klassifikation, sammen med en vejledning med et beslutningstræ, til at vurdere omfanget (se 6.3). Rumænien understøtter brede muligheder for indsendelse, både via portal, e-mail og fysisk post, hvor der stadig vil blive dannet eksterne beviser i form af kvitteringer for modtagelse. Dog vil elektronisk kommunikation generere de stærkeste beviser (se 6.4). Slovakiet har samlet værktøjer og vejledninger i en samlet portal, så der ikke skal vurderes kriterier ud fra forskellige kilder, hvilket reducerer risikoen for fejlfortolkning (se 6.5). Ungarn har centrale registre, både for kvalificerede revisorer og indsendelse af revisionsrapporter med blanketter og specifikationer, hvilket gør det muligt at sammenligne på tværs af revisioner (se 6.6).

Danmark er på forkant med mange af tiltagene, gennem det i forvejen eksisterende økosystem på Virk.dk. I afsnit 6.7 fremhæves dog 2 tiltag som Danmark kunne indføre. Det første er som Slovakiet har gjort at samle alle retningslinjer, vejledning, værktøjer og indberetningsportal og korrespondance på én side, så der kun er en kilde at vurdere kriterier og dokumentation ud fra. Lave et offentligt register som Ungarn, hvor det er tydeligt at se de kvalificerede revisorer, aflagte rapporter og specifikationer. Disse 2 tiltag vil reducere risikoen for fejlfortolkning af kriterier, sporbarheden og sammenlignelighed på tværs af revisioner (se 6.7).

7.4 Bidrag

Specialets vigtigste bidrag er en gentagelig tilgang til revision af overholdelse af NIS2 i Danmark, mens den nationale implementering stadig er under udvikling. Der præsenteres reviderbare elementer og beslutningsregler ud fra de kriterier der er defineret i kapitel 2 og 3.

- Et dokumenteret kildehierarki og kriteriesæt, herunder fastfrysning af kriterier og dokumentation for lovgrundlag pr. en given dato, så revisionskriterier er konsekvente og fortolkelige, selv efter ændringer til lovgrundlag og kriterier (se 2.2 – 2.4 og 4.6).
- En transformationskæde fra de juridiske forpligtelser til kontrolmål, beviser, testprocedurer og afvigelsesregler, der gør det muligt at holde en konsistent struktur i revisionsprogrammet, der kan genbruges på tværs af opgaver (se 2.3).
- En fortolkning ud fra et dansk perspektiv, af de forpligtelser der er mest relevante for IT-revision, herunder omfang, klassificering, registrering, governance, risikostyringsforanstaltninger og hændelsesrapportering, med fokus på de beviser der genereres fra portalen (se 3.1 – 3.7).
- En revisionsmodel bygget på 4 grundprincipper og en praktisk procedure for indhentning af beviser, der prioriterer eksternt generede beviser i forhold til vurdering om tidsfristerne er overholdt, understøttet af både ISA 500 og ISAE 3000 (se 4.4 – 4.5 og 5.2).
- Afvigelsesregler der sondrer mellem påviselig manglende overholdelse og begrænsninger i omfanget af dokumentation, samt hvordan de kan påvirke revisionskonklusionen (se 4.7).
- Et praktisk eksempel på start til slut for en hændelsesunderretning, der kan bruges til gentage revisionstest og genskabe tidslinjen for hændelsesforløbet (se 5.7).
- Oversigt over implementerede tiltag fra sammenligningslandene og hvilke af disse tiltag som Danmark kan implementere, for at forbedre mulighederne for revision og standardisere arbejdsgange lige fra virksomhedens registrering til hændelsesforløbet ved en væsentlig hændelse.

7.5 Begrænsninger

Specialet er udelukkende baseret på dokumenter. Der defineres kontrollerbare kriterier, bevismateriale og procedurer, men der foretages ikke en egentlig validering om hvordan danske myndigheder fører tilsyn og håndhæver forpligtelserne. Der måles heller ikke den praktiske cybersikkerhedskapacitet i henhold til NIS2. Denne begrænsning er iboende i det valgte forskningsdesign og afgræsning, hvor formålet er at gøre overholdelse af NIS2 reviderbar, frem for evaluering af de tekniske foranstaltninger og testresultater (se 2.1 og 2.5).

En anden begrænsning er kriteriernes stabilitet. Lovtekster og vejledninger er versionerede og daterede, men vejledningssider og portaler kan ændres uden ændringslog. Dette øger risikoen for at forventninger til kontroller og beviser ændres, både under skrivning af specialet og ved de fremtidige revisioner underlagt NIS2. Dette adresseres gennem fastfrysning af kilder og kriterier pr. en given dato, samt dokumentation i form af skærmprint fra vejledninger og portaler (se 2.4 og 4.6).

Det fremtidige arbejde skal fokusere på afprøvning og tilpasninger af de foreslåede kriterier. Førstegangsrevisioner baseret på de 4 grundprincipper, test af start til slut arbejdsgange for registrering, hændelsesunderretning samt afhjælpende foranstaltninger. I takt med at de officielle danske vejledninger og værktøjer modnes, vil tilsyns- og håndhævelsessager kunne bidrage til vurdering af væsentligheder og afvigelsesregler og samtidig være i tråd med kriteriegrundlaget (se 2.5, 4.7 og 5.7).

Med hensyn til implementerede foranstaltninger i de øvrige EU-lande (kapitel 6) er der en usikkerhed i forhold til oversættelse og fortolkning af fremmedsprog.

Referencer

[1] European Parliament and the Council of the European Union, »Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive),« 14 12 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[2] IAASB/IFAC, »Standard on Assurance Engagements (ISAE) 3000 (Revised): Assurance Engagements Other Than Audits or Reviews of Historical Financial Information,« 9 12 2013. [Online]. Available: https://www.ifac.org/system/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf.

[3] IAASB/IFAC, »International Standard on Auditing (ISA) 500: Audit Evidence,« [Online]. Available: https://www.iaasb.org/_flysystem/azure-private/publications/files/A022%202013%20IAASB%20Handbook%20ISA%20500.pdf.

[4] Retsinformation, »Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) (LOV nr 434 af 06/05/2025),« 6 5 2025. [Online]. Available: https://www.retsinformation.dk/eli/lta/2025/434/pdf.

[5] SAMSIK, »NIS 2-vejledninger,« [Online]. Available: https://samsik.dk/nis2/nis-2-vejledninger/.

[6] Virk (Styrelsen for Samfundssikkerhed), »Registrering af virksomhed efter NIS2,« [Online]. Available: https://virk.dk/myndigheder/stat/SAMSIK/selvbetjening/registrering-af-virksomhed-efter-nis2/.

[7] Virk, »Vejledning til registrering af virksomhed efter NIS2-direktivet (v4),« 12 6 2025. [Online]. Available: https://virk.dk/assets/5glGpUxe29ziE2oQQy8TG4/Vejledning_registrering_af_virksomhed_NIS2_v4.pdf.

[8] Virk, »Vejledning til indberetning af sikkerhedshændelse efter NIS2-direktivet (v1),« 26 6 2025. [Online]. Available: https://virk.dk/assets/cmhIfcTaAQ7947FMPwhR1/Vejledning_indberetning_af_h%C3%A6ndelse_NIS2_v1.pdf.

[9] Digitaliseringsstyrelsen, »Registreringspligt (NIS 2),« [Online]. Available: https://digst.dk/tilsyn/nis-2/registreringspligt/.

[10] Digitaliseringsstyrelsen, »Hændelsesunderretning (NIS 2),« [Online]. Available: https://digst.dk/tilsyn/nis-2/haendelsesunderretning/.

[11] Digitaliseringsstyrelsen, »Vejledning til registrering af enheder efter NIS 2-loven,« [Online]. Available: https://digst.dk/media/vondr30l/vejledning-til-registrering-af-enheder-efter-nis-2.pdf.

[12] ENISA, »NIS2 Technical Implementation Guidance version 1.0,« 6 2025. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

[13] Retsinformation, »Bekendtgørelse om udpegning af kompetente myndigheder og digital kommunikation omfattet af NIS 2-loven (BEK nr 620 af 02/06/2025),« 2 6 2025. [Online]. Available: https://www.retsinformation.dk/api/pdf/250196.

[14] Virk (SAMSIK), »Indberetning af brud på sikkerhed – Introduktion,« [Online]. Available: https://virk.dk/myndigheder/stat/SAMSIK/selvbetjening/Indberetning_af_brud_paa_sikkerhed/.

[15] Styrelsen for Samfundssikkerhed (SAMSIK), »Vejledning til implementering af NIS 2-lovens cybersikkerhedsforanstaltninger (1. udgave),« 8 2025. [Online]. Available: https://samsik.dk/wp-content/uploads/2025/08/Vejledning-til-implementering-af-cybersikkerhedsforanstaltninger.pdf.

[16] European Commission, »Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024,« 18 10 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202402690.

[17] International Ethics Standards Board for Accountants (IESBA), »Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards), 2024,« 08 2024. [Online]. Available: https://ifacweb.blob.core.windows.net/publicfiles/2025-02/2024%20IESBA%20HB_ENG_August%202024_Final.pdf.

[18] International Organization for Standardization (ISO), »ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements,« 10 2022. [Online]. Available: https://www.iso.org/standard/27001.

[19] ISACA, »COBIT,« [Online]. Available: https://www.isaca.org/resources/cobit.

[20] Committee of Sponsoring Organizations of the Treadway Commission (COSO), »Internal Control—Integrated Framework: Executive Summary,« 5 2013. [Online]. Available: https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf.

[21] International Auditing and Assurance Standards Board (IAASB), »International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization,« [Online]. Available: https://www.iaasb.org/_flysystem/azure-private/publications/files/B007%202013%20IAASB%20Handbook%20ISAE%203402_0.pdf.

[22] Belgian Official Journal (Moniteur belge / Belgisch Staatsblad), »Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (NIS2 transposition),« 26 4 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=NIM:202402242.

[23] Centre for Cybersecurity Belgium (CCB), »Regulation,« [Online]. Available: https://ccb.belgium.be/regulation.

[24] Safeonweb@Work / Centre for Cybersecurity Belgium (CCB), »La loi NIS2,« [Online]. Available: https://atwork.safeonweb.be/fr/nis2.

[25] Belgian Official Journal (Moniteur belge / Belgisch Staatsblad), »Arrêté royal du 9 juin 2024 (exécution de la loi NIS2),« 9 6 2024. [Online]. Available: https://etaamb.openjustice.be/fr/arrete-royal-du-09-juin-2024_n2024005260.

[26] Safeonweb@Work / Centre for Cybersecurity Belgium (CCB), »Guide_Enregistrement_NIS2_v1.2_EN (Registration guide),« 2 2025. [Online]. Available: https://atwork.safeonweb.be/sites/default/files/2025-02/Guide_Enregistrement_NIS2_v1.2_EN.pdf.

[27] Safeonweb@Work / Centre for Cybersecurity Belgium (CCB), »NIS 2 Quickstart guide,« [Online]. Available: https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide.

[28] Centre for Cybersecurity Belgium (CCB), »NIS2 notifications - Howto?,« [Online]. Available: https://ccb.belgium.be/cert/report-incident/nis2-notifications-howto.

[29] Centre for Cybersecurity Belgium (CCB), »notif.safeonweb.be (NIS2 incident notification portal),« [Online]. Available: https://notif.safeonweb.be/.

[30] Centre for Cybersecurity Belgium (CCB), »Report an incident,« [Online]. Available: https://ccb.belgium.be/cert/report-incident.

[31] Bundesgesetzblatt / recht.bund.de, »BGBl. I 2025 Nr. 301 - Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung,« 5 12 2025. [Online]. Available: https://www.recht.bund.de/bgbl/1/2025/301/regelungstext.pdf?__blob=publicationFile&v=3.

[32] Bundesamt für Sicherheit in der Informationstechnik (BSI), »NIS-2-Umsetzungsgesetz ab morgen in Kraft,« 5 12 2025. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html.

[33] Bundesamt für Sicherheit in der Informationstechnik (BSI), »Infos zu NIS-2 (Registration under NIS-2 currently not possible),« [Online]. Available: https://mip2.bsi.bund.de/en/info-nis2-registrierung/.

[34] Bundesamt für Sicherheit in der Informationstechnik (BSI), »NIS-2-Betroffenheitsprüfung,« [Online]. Available: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html.

[35] Bundesamt für Sicherheit in der Informationstechnik (BSI), »NIS-2 Betroffenheit Entscheidungsbaum (PDF),« [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.pdf?__blob=publicationFile&v=15.

[36] Portal Legislativ (Romania), »Ordonanţă de urgenţă nr. 155 din 30 decembrie 2024 privind cadrul național de securitate cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic

național civil,« 30 12 2024. [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocument/293121.

[37] Portal Legislativ (Romania), »Lege nr. 124 din 18 iunie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024,« 18 6 2025. [Online]. Available: https://legislatie.just.ro/public/DetaliiDocument/299675.

[38] Portal Legislativ (Romania) / Directoratul Național de Securitate Cibernetică (DNSC), »Ordin nr. 1 din 11 august 2025 privind aprobarea Cerințelor ... și modalității de transmitere a informațiilor,« 11 8 2025. [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/301473.

[39] Portal Legislativ (Romania) / Directoratul Național de Securitate Cibernetică (DNSC), »METODOLOGIE din 11 august 2025,« 11 8 2025. [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/301477.

[40] Slov-Lex / Zbierka zákonov (Slovak Republic), »Zákon č. 366/2024 Z. z. (PDF, Collection of Laws) – amendment to cybersecurity framework (NIS2 implementation),« 28 11 2024. [Online]. Available: https://static.slov-lex.sk/pdf/SK/ZZ/2024/366/ZZ_2024_366.pdf.

[41] National Security Authority of Slovakia (NBÚ), »NIS2 portal (nis2.nbu.gov.sk),« [Online]. Available: https://nis2.nbu.gov.sk/.

[42] N. S. A. o. S. (NBÚ), »Jednotný informačný systém kybernetickej bezpečnosti (JISKB),« [Online]. Available: https://www.nbu.gov.sk/jednotny-informacny-system-kybernetickej-bezpecnosti/.

[43] National Security Authority of Slovakia (NBÚ), »Hlásenie kybernetických bezpečnostných incidentov (incident reporting),« [Online]. Available: https://www.nbu.gov.sk/cybersecurity-incidents-reporting/.

[44] National Security Authority of Slovakia (NBÚ), »Informácie ohľadom smernice NIS 2 (PDF),« 17 10 2024. [Online]. Available: https://www.nbu.gov.sk/data/files/495_informacie-ohladom-smernice-nis-2.pdf.

[45] National Security Authority of Slovakia (NBÚ), »Metodiky (cybersecurity methodologies),« [Online]. Available: https://www.nbu.gov.sk/metodiky/.

[46] National Security Authority of Slovakia (NBÚ), »Indikatívna pomôcka na určenie subjektu ako poskytovateľa základnej služby (self-identification tool),« [Online]. Available: https://nis2.nbu.gov.sk/indikativna-pomocka-na-urcenie-subjektu-ako-poskytovatela-zakladnej-sluzby/.

[47] U. National Legislation Database (NJT), »2024. évi LXIX. törvény Magyarország kiberbiztonságáról,« 2024. [Online]. Available: https://njt.hu/jogszabaly/2024-69-00-00.

[48] Supervisory Authority for Regulated Activities (SZTFH), »Auditor registry (Auditorok),« [Online]. Available: https://sztfh.hu/nyilvantartasok/auditorok/.

[49] National Legislation Database (NJT), »7/2024. (VI. 24.) SZTFH rendelet a kiberbiztonsági auditorok,« 24 6 2024. [Online]. Available: https://njt.hu/jogszabaly/2024-7-20-8K.

[50] Supervisory Authority for Regulated Activities (SZTFH), »SZTFH 411,« [Online]. Available: https://sztfh.hu/ugyintezes/nyomtatvanyok-es-urlapok/sztfh411/.

[51] Supervisory Authority for Regulated Activities (SZTFH), »Tudástár (knowledge base for cybersecurity certifications/audits),« [Online]. Available: https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitasok/tudastar/.

[52] Supervisory Authority for Regulated Activities (SZTFH), »Kiberbiztonsági audittal kapcsolatos tájékoztatás,« [Online]. Available: https://sztfh.hu/downloads/kiberbiztonsag/tudastar/sztfh_kiberbiztonsagi_audittal_kapcsolatos_tajekoztatas.pdf.

[53] Supervisory Authority for Regulated Activities (SZTFH), »Kiberbiztonsági felügyelet (cybersecurity supervision),« [Online]. Available: https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitasok/kiberbiztonsagi-felugyelet/.