

Samenhangend Inspectiebeeld cybersecurity vitale processen

2024

Inhoud

Voorwoord 3

Samenvatting 4

Summary 6

1 Inleiding 8
- 1.1 Aanleiding 9
- 1.2 Betrokken toezichthouders 11
- 1.3 Leeswijzer 12

2 Rode draden van de toezichtresultaten 13
- 2.1 Inleiding 14
- 2.2 Risicomanagement blijft speerpunt 14
  - 2.2.1 Toenemende aandacht voor certificeringen 15
  - 2.2.2 Risicomanagement als onderdeel van goed bestuur 15
  - 2.2.3 Guidance risicomanagement: de rode draden 17
- 2.3 Geen informatiebeveiligingsincidenten boven melddrempel 19

3 Uitdagingen en ontwikkelingen in het toezicht 20
- 3.1 Inleiding 21
- 3.2 Nieuwe Europese richtlijnen leiden tot uitdagingen voor toezicht 21
- 3.3 Samenwerking nodig voor doelgericht en doelmatig toezicht 22

4 Doorontwikkeling samenwerkend toezicht 23
- 4.1 Inleiding 24
- 4.2 Risicomanagement ook komend jaar centraal 24
- 4.3 Uitbreiding met het onderwerp assetmanagement 24
- 4.4 Versteviging governance samenwerkende toezichthouders 24

bijlage 1: Toezichtresultaten per toezichthouder 26
- Toezichtresultaten per toezichthouder 27
- ANVS 28
- AP 29
- DNB 30
- IGJ 32
- IJenV 35
- ILT - Drinkwater 36
- ILT - Luchtvaart 38
- ILT - Spoor 39
- RDI - eIDAS 41
- RDI - Wbni 43

bijlage 2: Bronnen 45

Voorwoord

Schouder aan schouder



Met veel genoegen presenteer ik het Samenhangend Inspectiebeeld 2024. In dit inspectiebeeld maken de Nederlandse toezichthouders hun gezamenlijke inspanningen op het gebied van cybersecurity inzichtelijk. Schouder aan schouder voor een digitaal weerbaar Nederland.

Samenwerking is de enige weg: het is noodzakelijk om op de best mogelijke wijze uitvoering te geven aan de Europese regelgeving die op ons afkomt. Daarnaast is het essentieel om effectief toezicht te houden op ons dynamische werkveld. Artificiële intelligentie en quantumcomputers zijn daarin veelomvattende en impactvolle ontwikkelingen, die vragen om een gezamenlijke aanpak. Ook de huidige geopolitieke situatie en actuele dreigingen zijn gebaat bij een eensgezind optreden.

Natuurlijk is daarmee niet alles te voorkomen. Er zijn altijd cyberrisico's - en dat zal zo blijven. Dat is dan ook niet waar dit Samenhangend Inspectiebeeld in de kern om gaat. Veel meer dan dat draait het inspectiebeeld om de vraag hoe je de voortdurende cyberrisico's tegemoet treedt en hoe je je als organisatie voorbereidt. En hoe zorg je er als organisatie voor dat je na een incident weer snel verder kunt?

Risicomanagement is daarom het overkoepelende en meerjarige thema van de samenwerkende toezichthouders. Niet zozeer vanuit technisch, maar vooral vanuit bestuurlijk oogpunt. Daar valt winst te behalen. Het onderwerp verdient meer prioriteit op de bestuurlijke agenda's.

Risicomanagement en bestuursaansprakelijkheid nemen in de nieuwe NIS2-richtlijn een prominente positie in. Ik wil bestuurders op het hart drukken zich daar rekenschap van te geven, zich nu voor te bereiden en maatregelen te treffen op het gebied van risicomanagement. Mijn advies: wacht daarbij niet tot de nieuwe wetgeving daadwerkelijk in Nederland van kracht is. Ga er mee aan de slag: vandaag nog!

Met vriendelijke groet,
mede namens alle betrokkenen,

Angeline van Dijk
Inspecteur-generaal, Rijksinspectie Digitale Infrastructuur

Samenvatting

De digitale transformatie gaat snel en biedt unieke kansen voor onze maatschappij. Artificiële intelligentie (AI) heeft haar intrede gedaan en de mogelijkheden van quantumcomputers komen steeds vaker in het nieuws. De toenemende afhankelijkheid van de digitale infrastructuur maakt onze vitale processen echter ook kwetsbaar voor uitval en verstoringen. Adequate digitale weerbaarheid is daarom essentieel.

Voorliggend Samenhangend Inspectiebeeld is tot stand gekomen in een samenwerking tussen verschillende toezichthouders: de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), Autoriteit Persoonsgegevens (AP), De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Justitie en Veiligheid (IJenV), Inspectie Leefomgeving en Transport (ILT) en Rijksinspectie Digitale Infrastructuur (RDI).

In het Samenhangend Inspectiebeeld beschrijven deze toezichthouders jaarlijks de staat van de cybersecurity van vitale processen en vitale aanbieders. Dit vierde inspectiebeeld (2024) behandelt het inspectiejaar 2023 en de toekomstige ontwikkelingen.

Risicomanagement blijft speerpunt, verbetering mogelijk op bestuursniveau

De inspecties van de verschillende toezichthouders focusten in 2023 op het meerjarige thema risicomanagement. Ze merken op dat de vitale aanbieders steeds meer aandacht hebben voor de certificering van het *information security management system* (ISMS) en onderschrijven het belang hiervan. De toezichthouders hechten daarnaast veel betekenis aan het aansluiten van het ISMS op het *Enterprise Risk Management* (ERM) van de organisatie. Een ISMS bekijkt de risico's rondom informatiebeveiliging. ERM kijkt organisatiebreed naar risico's. Het expliciet vastleggen van de risicobereidheid is essentieel bij het implementeren van zowel een ERM-systeem als een ISMS en de toezichthouders stellen dit in enkele sectoren dan ook verplicht.

De toezichthouders zien ruimte voor verbetering op het gebied van risicomanagement op bestuursniveau. De belangrijkste verbeterpunten zijn:

- Vanuit een risico-oogpunt actuele ontwikkelingen volgen, zoals artificiële intelligentie en quantumcomputers.
- De aansluiting tussen het ERM-systeem en het ISMS waarborgen.
- De effectiviteit van het ERM-systeem en de ISMS onafhankelijk laten beoordelen.

Verder vinden de toezichthouders het belangrijk dat organisaties een governancestructuur hebben. De meest gebruikte opzet daarbij is het *three lines model* (3LM).

In 2023 zijn er geen meldingen van informatiebeveiligingsincidenten boven de drempelwaarde ontvangen

Bij informatiebeveiligingsincidenten gelden wettelijke meldplichten voor de vitale aanbieders. Als door het incident de gevolgen voor de continuïteit van een dienstverlening een sectorspecifieke drempelwaarde overschrijden, moet een organisatie vanuit de huidige cybersecurity-wetgeving het incident melden bij het Nationaal Cyber Security Centrum (NCSC) en de betreffende toezichthouder. In 2023 werden geen incidenten gemeld die de drempelwaarde overschreden.

Governance samenwerking toezichthouders verstevigd ten behoeve van implementatie CER en NIS2

Het toezicht op cybersecurity wordt de komende periode aanzienlijk uitgebreid door de komst van twee nieuwe Europese richtlijnen: de *Critical Entities Resilience*-richtlijn (CER) en de *Network and Information Security*-richtlijn (NIS2). Deze richtlijnen worden omgezet in nationale wet- en regelgeving. Dit is een omvangrijk en complex traject dat zorgvuldigheid vergt, ook omdat de impact voor Nederlandse organisaties die onder de richtlijnen vallen, groot is. Het omzetten van de richtlijnen kost meer tijd dan van tevoren werd gedacht. Daarom is de Tweede Kamer eind januari 2024 geïnformeerd over het niet halen van de implementatiedeadline van oktober 2024. Dit betekent dat de nationale wet- en regelgeving later in werking treedt. Totdat de wetten van kracht zijn, blijven de toezichthouders toezicht uitvoeren op basis van de huidige wetgeving. Op 21 mei 2024 is de internetconsultatie voor de Nederlandse implementatie van de NIS2 en de CER begonnen. De NIS2 krijgt vorm in de Cyberbeveiligingswet en de CER in de Wet weerbaarheid kritieke entiteiten.

Met de komst van de CER en de NIS2 is meer toekomstgerichte samenwerking tussen toezichthouders nodig. Gelet hierop is er een noodzaak om de *governance* rondom samenwerking te versterken. Daarom is recentelijk het 'directeurenoverleg toezicht digitale weerbaarheid' opgericht. Dit gremium fungeert als opdrachtgever van de werkgroep 'samenwerkend toezicht digitale weerbaarheid'. Met de inrichting van deze samenwerkingsvormen streven de toezichthouders naar effectief en efficiënt toezicht en een zo laag mogelijke gezamenlijke werklast voor organisaties die onder toezicht staan.

Onderwerp van gesprek tussen de toezichthouders is de doorontwikkeling van het Samenhangend Inspectiebeeld. Aan het meerjarige thema risicomanagement wordt voor het inspectiejaar 2024 het thema assetmanagement toegevoegd. Het doel is om daar in het volgende inspectiebeeld op in te gaan. Het proces van de totstandkoming van het jaarlijkse Samenhangend Inspectiebeeld blijft onderhevig aan continue verbetering.

Summary

The digital transformation is progressing rapidly and offers unique opportunities for our society. Artificial intelligence (AI) has arrived on the scene, and the advanced capabilities of quantum computers are increasingly in the news. However, increasing reliance on the digital infrastructure also makes our vital processes vulnerable to outages and disruptions. Therefore, ensuring adequate digital resilience is essential.

The present Inspection Overview is the result of a collaboration between several supervisory authorities: the Authority for Nuclear Safety and Radiation Protection (ANVS), the Dutch Data Protection Authority (DPA), De Nederlandsche Bank (DNB), the Health and Youth Care Inspectorate (IGJ), the Inspectorate of Justice and Security (IJenV), the Human Environment and Transport Inspectorate (ILT) and the Dutch Authority for Digital Infrastructure (RDI).

Each year, these supervisory authorities identify the cybersecurity status of vital processes and vital providers in the Inspection Overview. This fourth Inspection Overview (2024) reviews the 2023 inspection year and examines upcoming developments.

Risk management remains a primary area of focus, improvement possible at executive board level

The inspections carried out by the various supervisory authorities in 2023 focused on the multi-year theme of risk management. They note that the vital providers are increasingly devoting attention to certification of the information security management system (ISMS) and endorse its importance. In addition, the supervisory authorities attach high importance to effective alignment between the ISMS and the organisation's Enterprise Risk Management (ERM). An ISMS focuses on the risks associated with information security. ERM considers risks across the entire organisation. Explicitly identifying the degree of risk appetite is essential when implementing both an ERM system and an ISMS and has therefore been imposed by the supervisory authorities as a mandatory requirement in some sectors.

The supervisory authorities see room for improvement in risk management at executive board level. The main areas for improvement are:

- Tracking current developments from a risk perspective, e.g. artificial intelligence and quantum computers.
- Acting to ensure alignment between the ERM system and the ISMS.
- Arranging independent assessments of the effectiveness of the ERM system and ISMS.

Furthermore, the supervisory authorities strongly believe that organisations should have a governance structure. The most common approach in this regard is the three lines model (3LM).

There were no reports of information security incidents that exceeded the threshold in 2023

When information security incidents occur, the vital providers are subject to various legal notification obligations. Under current cybersecurity laws, if the impact on service continuity caused by the incident exceeds an industry-specific threshold, an organisation must report the incident to the National Cyber Security Center (NCSC) and the appropriate supervisory authority. In 2023, no incidents that exceeded the threshold were reported.

The CER and NIS2 require strengthened collaborative governance on the part of the supervisory authorities

In the coming period, the supervision of cybersecurity will be significantly extended by the introduction of two new European directives: the Critical Entities Resilience Directive (CER) and the Network and Information Security Directive (NIS2). These directives will be transposed into national laws and regulations. This is an extensive and complex process that requires proper diligence, even more so because the impact on Dutch organisations affected by the directives is significant. Transposing the directives is taking longer than previously thought. Consequently, the Dutch parliament was informed of the failure to meet the October 2024 implementation deadline in late January 2024. This means that the national laws and regulations will be enacted at a later date. In the period up to enactment, the supervisory authorities will continue to conduct supervision based on current legislation. 21 May 2024 marks the start of the internet consultation for the Dutch implementation for the NIS2 and the CER. The NIS2 and CER respectively take shape in the Cyberbeveiligingswet (Cyber Security Act) and the Wet weerbare kritieke entiteiten (Critical Entity Resilience Act).

The advent of the CER and the NIS2 directives requires more forward-looking collaboration between supervisory authorities. In view of this, there is a need to strengthen governance with respect to collaboration. The 'director-level consultation on the supervision of digital resilience' was established for this in the recent past. This body determines and controls the activities of the 'collaborative supervision of digital resilience' working party. By setting up these forms of collaboration, the supervisory authorities aim to ensure effective and efficient organisation of the supervision and that the overall supervisory burden on organisations subject to the supervision remains as low as possible.

Further development of the Inspection Overview is a further topic of discussion between the supervisory authorities. The theme of asset management will be added to the multi-year theme of risk management for the 2024 inspection year. The goal is to explore this activity in greater detail in the next Inspection Overview. The process for creating the annual Inspection Overview remains subject to continuous improvement.

1 Inleiding



1.1 Aanleiding

De digitale transformatie gaat snel en biedt unieke kansen voor onze maatschappij. Artificiële intelligentie (AI) heeft haar intrede gedaan en de mogelijkheden van quantumcomputers komen steeds vaker in het nieuws. De toenemende afhankelijkheid van de digitale infrastructuur maakt onze vitale processen echter ook kwetsbaar voor uitval en verstoringen. Adequate digitale weerbaarheid is daarom essentieel.

In de Nederlandse cybersecuritystrategie 2022-2028 (NLCS)[1] beschrijft het kabinet de visie op een digitaal veilig Nederland waarin iedereen ten volle kan profiteren van deelname aan de digitale samenleving. In het bijbehorende actieplan[2] gaat het kabinet nader in op de ambities en acties voor een digitaal veilige samenleving. Effectief toezicht vormt daarbij een essentieel onderdeel. Het belangrijkste wettelijk kader voor het toezicht is de Wet beveiliging netwerk- en informatiesystemen (Wbni).

De bij de Wbni betrokken toezichthouders analyseren dreigingen en kansen vanuit hun expertise en maken de doorontwikkeling van het toezicht jaarlijks inzichtelijk in het Samenhangend Inspectiebeeld. Het inspectiebeeld beschrijft de staat van de cybersecurity van vitale processen en aanbieders. Dat gebeurt aan de hand van de inspectieresultaten en bevindingen van de toezichthouders. Dit vierde inspectiebeeld uit 2024 behandelt het inspectiejaar 2023 en de toekomstige ontwikkelingen.

Het begrip 'vitaal'

Dit Samenhangend Inspectiebeeld past de term 'vitaal' in brede zin toe:

***Vitale processen** zijn processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring ervan tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid[3].*
Voorbeelden: de productie van elektriciteit, de verwerking van nucleair materiaal en drinkwatervoorzieningen.

***Vitale aanbieders** zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. De betrokken ministeries hebben een beleidsmatige verantwoordelijkheid om te bepalen welke aanbieders vitaal zijn[4]. Daarnaast wijst de Wbni een groot aantal aanbieders van vitale processen al als vitale aanbieders aan.*
Voorbeelden: netbeheerders, banken en ziekenhuizen.

1 Nederlandse cybersecuritystrategie 2022-2028 (NLCS)

2 Actieplan Nederlandse cybersecuritystrategie 2022-2028 (NLCS)

3 https://www.nctv.nl/onderwerpen/vitale-infrastructuur

4 https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders



Benamingen voor organisaties onder toezicht

Het toezichtdomein voor cybersecurity kent verschillende benamingen voor organisaties die onder toezicht staan vanuit de Wbni.

***Huidige benamingen: vitale aanbieder** (NIB-richtlijn)*
De De Europese Netwerk- en Informatiebeveiliging Richtlijn (NIB-richtlijn) en de Wbni spreken over 'vitale aanbieder' en maken onderscheid tussen:

- *Aanbieder van essentiële diensten (AED) en digital service provider (DSP). Voor beide geldt zowel de meldplicht als de zorgplicht.*
- *Andere vitale aanbieder (AVA). Hiervoor geldt de meldplicht, maar niet de zorgplicht.*

***Toekomstige benamingen: entiteit** (NIS2-richtlijn en CER-richtlijn)*
De NIS2-richtlijn laat de termen 'aanbieder' en 'DSP' los en gebruikt voortaan de term 'entiteit'.
NIS2 maakt onderscheid tussen:

- *essentiële entiteit;*
- *belangrijke entiteit.*

De CER-richtlijn gebruikt ook de algemene term 'entiteit' en specifiek 'kritieke entiteit'.

Benamingen vanuit toezichthouders
De benamingen die de toezichthouders hanteren voor organisaties onder toezicht, verschillen. Zo zijn bijvoorbeeld in gebruik: 'onder toezicht staande instellingen', 'onder toezicht staande organisaties', 'ondertoezichtstaanden' en 'toezicht genietende organisaties'.

Dit Samenhangend Inspectiebeeld hanteert de termen 'vitale aanbieder' en 'organisatie'.

Naast de sectorspecifieke dreigingen die voortdurend flexibele, specifieke inzet van de toezichthouders vragen, kennen de sectoren onderlinge afhankelijkheden en generieke dreigingen die vragen om samenhang en samenwerking tussen toezichthouders. In dit licht stelden de betrokken toezichthouders in 2021 het eerste Samenhangend Inspectiebeeld op. Dit ging over het inspectiejaar 2020 en de ontwikkelingen in die periode. Deze samenwerking ontwikkelt en verbetert zich sindsdien continu. Bovendien laten de inspectiebeelden zien dat de vitale aanbieders hard werken aan het versterken van de digitale weerbaarheid. In dit inspectiebeeld laten de toezichthouders - aan de hand van het meerjarige thema risicomanagement - zien dat de lijn van de afgelopen jaren doorzet.

Het begrip 'cybersecurity'

Het eerste Samenhangend Inspectiebeeld ontleende de definitie van 'cybersecurity' gedeeltelijk aan het Cybersecurity Woordenboek, een publicatie van Cyberveilig Nederland. Die beschreef cybersecurity als volgt:

"Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als die toch is ontstaan. Een voorbeeld van schade is dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terechtkomt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen."

De Wbni verwijst bij de term 'cybersecurity' specifiek naar de NIB-richtlijn en geeft de volgende definitie:

"Beveiliging van netwerk- en informatiesystemen: het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen."

1.2 Betrokken toezichthouders

Dit Samenhangend Inspectiebeeld is opgesteld door de toezichthouders die sinds de implementatie van de NIB-richtlijn in de Wbni samenwerken. Dit zijn:

- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS);
- Autoriteit Persoonsgegevens (AP);
- De Nederlandsche Bank (DNB);
- Inspectie Gezondheidszorg en Jeugd (IGJ);
- Inspectie Justitie en Veiligheid (IJenV);
- Inspectie Leefomgeving en Transport (ILT);
- Rijksinspectie Digitale Infrastructuur (RDI).

Niet alle bij dit inspectiebeeld betrokken toezichthouders voeren toezicht uit onder de Wbni. Dat kan zijn omdat sprake is van een ander wettelijk kader op het gebied van cybersecurity dan de Wbni. Bijvoorbeeld in de financiële sector (DORA) en de telecomsector (TW). In andere gevallen komt het doordat in een bepaalde sector nog geen organisaties als aanbieder van essentiële diensten zijn aangewezen.

Zo is de sector gezondheidszorg, waar de Inspectie Gezondheidszorg en Jeugd (IGJ) toezicht op houdt, wel benoemd in de NIB-richtlijn, maar zijn daar in het kader van de Wbni tot op heden geen vitale aanbieders aangewezen. Ook duidt de NIB-richtlijn geen essentiële diensten aan. Met de implementatie van de nieuwe NIS2-richtlijn[5] komt hier naar verwachting verandering in. Ondanks het ontbreken van vitale aanbieders voor deze sector in de Wbni, heeft de term 'vitaal' in dit inspectiebeeld ook betrekking op de gezondheidszorg en de IGJ. De IGJ houdt nu al toezicht op de wettelijke verplichtingen van zorginstellingen op het gebied van informatiebeveiliging. Dat doet deze inspectie op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).

Met betrekking tot vitale processen is de Inspectie Justitie en Veiligheid (IJenV) geen toezichthouder in de zin van de Wbni. Wel houdt de IJenV toezicht op de vitaal verklaarde processen 'communicatie met en tussen hulpdiensten middels 112 en C2000' en 'inzet politie' binnen de sector openbare orde en veiligheid (OOV). Deze processen zijn wel vitaal, maar niet opgenomen in de Europese NIB-richtlijn of de Wbni. Daarom zijn voor deze processen geen aanbieders van essentiële diensten (AED's) en andere vitale aanbieders (AVA's) aangewezen. Deze vitale processen vallen onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De IJenV sluit zoveel mogelijk aan bij de risicogebaseerde aanpak en werkwijze van de toezichthouders die wel toezicht houden in het kader van de Wbni.

De Autoriteit Persoonsgegevens (AP) heeft bij dit inspectiebeeld een ander perspectief dan de andere toezichthouders. De AP houdt namelijk geen toezicht op een specifiek soort organisatie of sector of een vitaal proces. Wel monitort de AP namens de Algemene Verordening Gegevensbescherming (AVG) álle organisaties, publiek of privaat, die persoonsgegevens verwerken. Hieronder vallen ook de vitale aanbieders, voor zover zij hierbij persoonsgegevens verwerken. De AP heeft hierdoor een toezichthoudende rol door verschillende vitale processen heen. Daarbij richt het toezicht zich onder andere op cybersecurity. Het adequaat beveiligen van persoonsgegevens vormt namelijk een belangrijk vereiste voor AVG-conforme gegevensverwerking. De AP werkt daarbij nauw samen met de bij dit inspectiebeeld betrokken toezichthouders in het geval van cybersecurityincidenten waarbij sprake is van inbreuken in persoonsgegevens.

Zoals gezegd houden de betrokken toezichthouders toezicht op grond van diverse wettelijke kaders. Hierdoor komt het voor dat verschillende toezichthouders dezelfde aanbieders van vitale processen monitoren, op grond van andere wettelijke kaders. Zo houdt de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) toezicht op situaties waarbij ioniserende straling kan vrijkomen. Deze situaties vinden bijvoorbeeld plaats in ziekenhuizen, waarop ook de IGJ toezicht houdt. De verschillende toezichthouders hebben dan met elkaar te maken en daardoor is samenwerking noodzakelijk.

5 Hoofdstuk 3 'Uitdagingen in het toezicht' gaat uitgebreid in op de NIS2-richtlijn.

1.3 Leeswijzer

Hoofdstuk 2 gaat over de uitkomsten van het toezicht op de cybersecurity van de vitale processen. Daarnaast beschrijft het de rode draden volgens de verschillende toezichthouders aan de hand van de inspectieresultaten. Het hoofdstuk licht de opgehaalde *best practices* ten aanzien van risicomanagement toe.

In hoofdstuk 3 staan de uitdagingen in het toezicht centraal. Het gaat over de ontwikkelingen voortkomend uit de nieuwe Europese richtlijnen rondom de digitale en fysieke weerbaarheid van vitale processen en de impact daarvan op het toezicht. Verder zet het hoofdstuk de uitdagingen in de samenwerking tussen de toezichthouders uiteen en de ontwikkelingen daarbinnen.

Hoofdstuk 4 beschrijft de voorziene doorontwikkeling van het Samenhangend Inspectiebeeld. Het behandelt de verbeterpunten uit het voorgaande inspectiebeeld en licht de ambitie voor de komende jaren toe. Daarnaast gaat het hoofdstuk over de doorontwikkeling van de *governance* van het samenwerkend toezicht.



2 Rode draden van de toezichtresultaten

2.1 Inleiding

Dit hoofdstuk schetst de rode draden aan de hand van de inspectieresultaten van de toezichthouders. Deze zijn gebaseerd op de inspectiewerkzaamheden van de toezichthouders in 2023. Paragraaf 2.2 zet de conclusies en aanbevelingen uiteen. In de bijlage van dit inspectiebeeld staat een gedetailleerd overzicht van de resultaten per toezichthouder. Paragraaf 2.3 gaat over de informatiebeveiligingsincidenten in 2023.

2.2 Risicomanagement blijft speerpunt

Net als in de twee voorgaande jaren versterkten de toezichthouders in 2023 elkaars inzet door aandacht te besteden aan het gezamenlijke thema risicomanagement. Hierdoor ontstaat een breed beeld over de stand van risicomanagement binnen de verschillende sectoren. Nieuw voor het inspectiejaar 2023 is dat de toezichthouders voorafgaand aan het jaar 2023 afspraken maakten over de aandachtsgebieden voor de risicobeelden per sector.

De verantwoordelijkheden van de besturen van de geïnspecteerde organisaties krijgen specifieke aandacht in de opgestelde rode draden. Organisaties moeten risicobeheersmaatregelen nemen op het gebied van cybersecurity en de bestuurders zijn daarvoor verantwoordelijk. Daarom schrijft de NIS2-richtlijn voor dat het bestuur deze maatregelen goedkeurt en toeziet op de uitvoering ervan. Bestuursleden moeten een opleiding volgen en beschikken over kennis en vaardigheden om risico's op het gebied van cybersecurity te herkennen. Ook moeten ze de gevolgen van deze risico's voor de diensten die de organisatie levert, kunnen beoordelen. Vooruitlopend op de NIS2-richtlijn gaan de rode draden verder in op de verantwoordelijkheden van besturen.

Risicomanagement

Risicomanagement is een proces dat bedrijfsrisico's voortdurend bewaakt. Onderdelen zijn bijvoorbeeld het identificeren, evalueren en prioriteren van risico's en het nemen van maatregelen (accepteren, mitigeren, overdragen of vermijden). Door middel van risicoanalyses krijgen organisaties inzicht in de risico's[6].

6 https://www.cybersecurityalliantie.nl/ecp_images/2021/12/Cybersecurity-Woordenboek-2021_ZonderSpreads.pdf



2.2.1 Toenemende aandacht voor certificeringen

De toezichthouders signaleren dat organisaties steeds meer aandacht hebben voor certificering van het *information security management system* (ISMS). Dit is in lijn met de aanbevelingen in het inspectiebeeld over 2022. De toezichthouders onderschrijven in dit beeld namelijk het belang van het onafhankelijk laten beoordelen van risicomanagementprocessen. Het gaat hierbij meestal om de ISO 27001-certificering. Voor zorgorganisaties, zoals ziekenhuizen, betreft het de NEN 7510.

Certificeringen van het *information security management system* (ISMS)

ISO 27001

Met deze certificering geven organisaties aan dat ze voldoen aan de eisen voor het opzetten, implementeren, onderhouden en verbeteren van een informatiebeveiligingsbeheersysteem. ISO 27001 dient als richtlijn voor het voortdurend beoordelen van de informatieveiligheid.

NEN 7510

Deze certificering is gebaseerd op de ISO 27001 en is in Nederland de wettelijke norm voor informatiebeveiliging bij zorgaanbieders. NEN 7510 houdt rekening met de specifieke kenmerken van de zorgsector.

2.2.2 Risicomanagement als onderdeel van goed bestuur

De toezichthouders constateren dat de bestuurders van organisaties oog hebben voor uitval en verstoringen van vitale processen als gevolg van *ransomware*, sabotage en *insider threat*. Ze vragen aandacht voor risico's in het kader van nieuwe ontwikkelingen rondom AI[7] en quantumcomputers[8].

Inzicht in mogelijke risico's helpt een organisatie om gebeurtenissen die effect hebben op het bereiken van de bedrijfsdoelstellingen te identificeren en te beheersen. Om deze reden kan het bestuur van een organisatie *Enterprise Risk Management* (ERM) inrichten. Dit kunnen ze doen op basis van een zelfontwikkelde methode of een bewezen effectieve methode, ook wel een *best practice* genoemd. Voorbeelden van gebruikte *best practices* zijn COSO en ISO 31000.

De toezichthouders leggen de focus in dit inspectiebeeld op de beheersing van cybersecurityrisico's door het bestuur van organisaties. Uitgangspunt hierbij is dat de specifieke cybersecurityrisico's uit het *Information Security Management System* (ISMS) gekoppeld zijn aan de risico's uit het ERM-systeem.

Best practice

Een best practice is een techniek, werkmethode of activiteit die in de praktijk heeft bewezen effectief te zijn. Belangrijk bij het inzetten van best practices is het evalueren van het handelen en de resultaten, zodat bijsturing kan plaatsvinden.

Om risicomanagement effectief te implementeren, is het van belang dat het bestuur een zogenaamde risicobereidheid (*risk appetite*) opstelt. Al dan niet aangevuld met de risicotolerantie (*risk tolerance*), oftewel in welke mate het risico mag afwijken van de risicobereidheid. De vastgestelde risicobereidheid helpt de organisatie bij de vraag of aanvullende maatregelen nodig zijn. Daarom stellen de toezichthouders het vastleggen en hanteren van een risicobereidheid binnen enkele sectoren verplicht. Uit de inspectiewerkzaamheden blijkt dat bij het merendeel van de organisaties het bestuur de risicobereidheid - vaak met bijbehorende risicotolerantie - vooraf heeft vastgesteld. De meeste organisaties hanteren daarbij een apart risicoacceptatieproces met risicoacceptatieformulieren voor het bewust accepteren van risico's boven hun tolerantiegrens.

7 https://www.rdi.nl/actueel/nieuws/2024/02/21/rdi-publiceert-jaarplan-2024#:~:text=In%20het%20jaarplan%202024%20staan,veilige%20en%20betrouwbare%20digitale%20infrastructuur

8 https://www.dnb.nl/nieuws-voor-de-sector/oud/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/

Naast de inrichting van ERM-systeem vinden de toezichthouders het van belang dat de organisatie een governancestructuur heeft. In een aantal sectoren dient deze *governance* een specifieke, vooraf vastgestelde structuur te hebben. De meeste organisaties hanteren het *three lines model* (3LM) als leidraad.

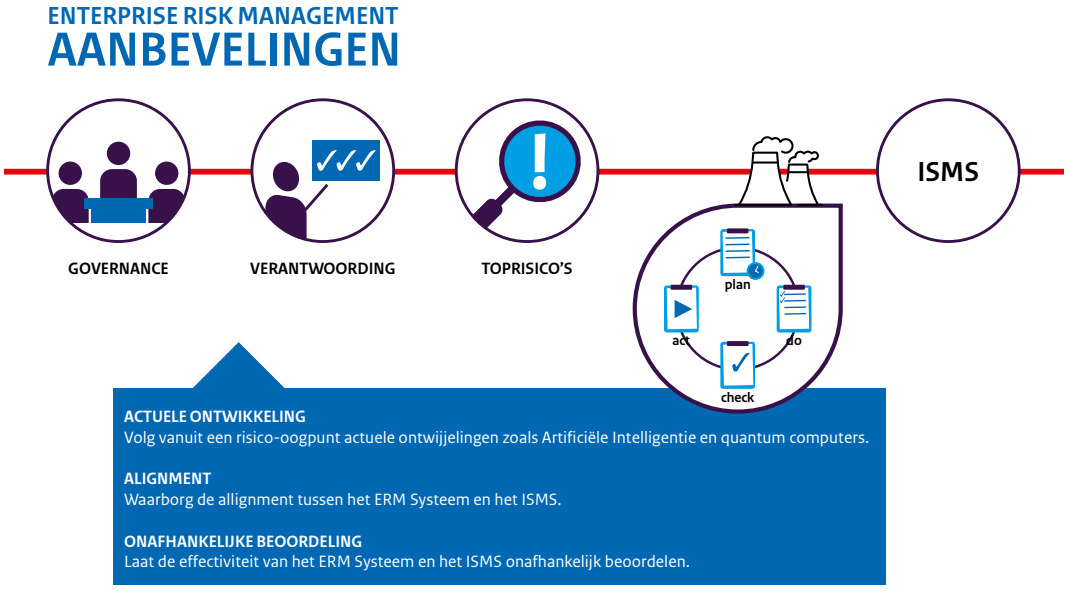
Het three lines model (3LM)

Het three lines model (3LM) is een wereldwijde standaard binnen risicomanagement. Het beschrijft een structuur waarin de organisatie de taken en rollen voor haar interne beheersing over drie lijnen verdeelt:

- *De eerste lijn - ofwel het lijnmanagement - is verantwoordelijk voor de eigen processen;*
- *De tweede lijn adviseert, coördineert en bewaakt of de eerste lijn de verantwoordelijkheden ook daadwerkelijk neemt;*
- *De derde lijn controleert tot slot of het samenspel tussen de eerste en tweede lijn naar behoren functioneert en geeft een objectief en onafhankelijk oordeel over de processen.*

De toezichthouders zien ruimte voor verbetering op het gebied van risicomanagement op bestuursniveau. De belangrijkste verbeterpunten zijn:

- Vanuit een risico-oogpunt actuele ontwikkelingen volgen, zoals AI en quantumcomputers.
- De aansluiting tussen het ERM-systeem en het ISMS waarborgen.
- De effectiviteit van het ERM-systeem en de ISMS onafhankelijk laten beoordelen.



Afbeelding 1: Aanbevelingen op het gebied van Enterprise Risk Management

2.2.3 Guidance risicomanagement: de rode draden

De toezichthouders vinden het ontwikkelen van *empowerment* en het bevorderen van het lerend vermogen van de vitale aanbieders belangrijk. Uitgangspunt hierbij is dat de verantwoordelijkheid voor de digitale weerbaarheid van de vitale processen primair bij de organisaties zelf ligt. De toezichthouders bieden onder andere *guidance* aan om deze verantwoordelijkheid van de organisaties te ondersteunen en het zelflerend vermogen te stimuleren. Het delen van *best practices* is daar een vorm van. De toezichthouders delen daarom vanuit de rode draden de geconstateerde *best practices* voor risicomanagement met organisaties. Tabel 1 beschrijft deze rode draden op basis van het gezamenlijk beeld van de betrokken toezichthouders. De onderliggende informatie per toezichthouder voor de betreffende sectoren staat in bijlage 1.

Empowerment, guidance & best practices

Empowerment en guidance dragen bij aan het lerend vermogen van organisaties. Empowerment is het proces van versterking, dat organisaties stimuleert om zelfstandig te beslissen en te handelen. Guidance via gesignaleerde best practices biedt hierbij ter inspiratie voorbeelden uit de praktijk.

Tabel 1. Rode draden aan de hand van de inspectieresultaten

RODE DRADEN	
ERM - Enterprise risk management	
1. Welke *best practice* gebruiken organisaties voor de inrichting van ERM?	Voor de inrichting van ERM gebruiken organisaties verschillende methoden. Dit kan zowel een zelfontwikkelde methode zijn als een *best practice*. Gebruikte *best practices* zijn onder andere COSO, ISO 31000 of een sectorspecifieke opzet. In enkele gevallen zijn de risico's vanuit het ISMS en de risico's in het organisatiebrede, centrale risicoregister nog niet met elkaar in lijn.
2. Hoe ziet de governancestructuur van organisaties eruit?	Elke inspectie verlangt bij een organisatie een governancestructuur te zien. In een aantal sectoren dient de *governance* een vastgestelde structuur te hebben, bijvoorbeeld het *three lines model* (3LM). Het 3LM is in ieder geval het model dat de meeste organisaties hanteren.
3. Is de risicobereidheid van organisaties vastgelegd?	Bij het merendeel van de organisaties heeft het bestuur de risicobereidheid - vaak met bijbehorende risicotolerantie - vooraf vastgesteld. Voor enkele sectoren vormt het expliciet hanteren van een risicobereidheid vanuit de vereiste governancestructuur een verplicht onderdeel. Verder hanteren de organisaties vaak ook een apart risicoacceptieproces met risicoacceptatieformulieren voor het bewust accepteren van risico's boven hun risicotolerantiegrens.
Toprisico's	
4. Welke toprisico's van de besturen van organisaties zijn gerelateerd aan cybersecurity?	Een toprisico dat besturen noemen is verstoring van de continuïteit van de processen en dienstverlening vanwege uitval van systemen door *ransomware*, sabotage en *insider threat*. Andere genoemde toprisico's zijn *ransomware* zelf, informatiediefstal en identiteitsfraude. Informatiediefstal kan verschillende soorten gegevens betreffen, zoals persoons- en bedrijfsgegevens, en kent diverse vormen, zoals identiteitsfraude, gijzelneming en spionage.

RODE DRADEN	
ISMS - Information Security Management System	
Plan	
5. Welke *best practice* hebben organisaties gebruikt voor de inrichting van ISMS?	Organisaties gebruiken voor de inrichting van hun ISMS over het algemeen de ISO 27001. De gezondheidszorg gebruikt de sectorspecifieke variant NEN 7510.
6. Is het ISMS gecertificeerd?	De meeste organisaties kijken serieus naar certificering van het ISMS. Over het algemeen hanteren ze de ISO 27001-certificering. Voor zorgorganisaties zoals ziekenhuizen gaat het om de NEN 7510. Nog niet alle organisaties zijn daadwerkelijk gecertificeerd. Bij organisaties met een certificering, is de certificering vaak op een beperkt aantal systemen van toepassing. Een aantal organisaties zet op korte termijn een certificeringstraject in.
Do	
7. Hebben organisaties een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	De organisaties leggen over het algemeen vast wat hun essentiële dienst(en) zijn, samen met de systemen die daarvoor van belang zijn. Dit gebeurt op verschillende manieren. Bijvoorbeeld door het bepalen van de *scope*, kritieke systemen en/of kroonjuwelen, door het uitvoeren van een *business impact analyse* (BIA) en/of door het vastleggen van een dienstbeschrijving met elementaire componenten.
8. Hebben organisaties een dreigingsanalyse uitgevoerd op de essentiële dienst?	Alle organisaties hebben een risicoanalyse uitgevoerd. Een dreigingsanalyse vormt daar in principe het startpunt van. Vanuit onderkende dreigingen ontstaan de bijbehorende risico's. Vastgestelde risico's kennen impliciet altijd een achterliggende dreiging. Organisaties maken echter voor hun risicoanalyse nog niet altijd gebruik van gangbare of zelf opgestelde dreigingsanalyses. In enkele gevallen diende de organisatie door een gewijzigde dreiging haar risicoanalyse te actualiseren, te verrijken en/of aan te scherpen.
9. Hebben organisaties bij elke dreiging de kans en impact ingeschat?	Alle organisaties hebben bij elk risico de kans en impact ingeschat en vastgelegd.
10. Hebben organisaties bij elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Alle organisaties hebben bij elk risico maatregelen vastgelegd. De diepgang van deze vastlegging en van het acceptatieproces van de restrisico's verschilt en hangt af van de volwassenheid van de organisatie.
Check	
11. Hebben organisaties *key controls* ten behoeve van de maatregelen gedefinieerd en voeren organisaties deze uit?	Over het algemeen hebben de organisaties *key controls* om de maatregelen te monitoren. Hier is echter nog wel aandacht voor nodig. *Key controls* zijn niet altijd expliciet vastgelegd en ontbreken in enkele gevallen. De volwassenheid en diepgang in de uitvoering verschilt. De organisaties hebben daarnaast in hun auditplanning vaak nog onvoldoende aandacht gegeven aan cybersecurity.
12. Op welke wijze legt het management van organisaties verantwoording af over de resultaten van de *key controls*?	De organisaties zetten verschillende instrumenten in voor de verantwoording richting het management over de werking van de *key controls*. Deze informatie gaat in samengevatte vorm weer richting het hoger management, zoals directie, bestuur en commissarissen. Voorbeelden zijn interne rapportages, KPI's, dashboards en managementrapportages. Deze bevatten vaak ook de resultaten van interne en externe audits. Ook kennen veel organisaties een *management review*, directiebeoordeling of een interne controle verklaring (ICV).

RODE DRADEN	
Act	
13. Onderkennen organisaties verbeteringen op basis van de resultaten van de *key controls*?	De organisaties voeren over het algemeen verbeteringen door op basis van de resultaten vanuit *key controls*. Ze leggen deze nog niet altijd expliciet vast. Ook hebben organisaties pas recent hun Plan-Do-Check-Act-cyclus (PDCA-cyclus) ingericht en nog niet vaak doorlopen. De werking en aantoonbaarheid van de stap *Act(ualize)* kan daarmee nog beter.
14. Op welke wijze bewaken organisaties de opvolging van verbeteracties?	De organisaties hanteren verbeterplannen, *roadmaps*, projecten en wijzigingen voor het uitzetten en het monitoren van verbeteracties. De organisaties registreren deze in overzichtsdocumenten, dan wel in specifieke applicaties, zoals een *IT Service Management System* (ITMS) of projectsoftware. Het bijhouden en rapporteren is belegd bij verantwoordelijke functionarissen. De organisaties hebben de controle op de opvolging van deze activiteiten over het algemeen ook geborgd in de lijn. De voortgang is meestal onderdeel van de informatiestroom naar het (hoger) management.
Verantwoording	
15. Op welke wijze leggen organisaties verantwoording over het ISMS af aan het bestuur?	De eerder vermelde verantwoordingsinstrumenten bevatten, naast zaken als *key controls* en voortgang op verbeteractiviteiten, ook de verantwoording over het ISMS. De interne en eventuele externe audit nemen de werking van het ISMS mee. De resultaten en bevindingen van deze audits vormen bijna altijd een standaarddeel van de verantwoording naar het hoger management.

2.3 Geen informatiebeveiligingsincidenten boven melddrempel

De vitale aanbieders kennen verschillende wettelijke meldplichten voor informatiebeveiligingsincidenten. Een voorbeeld is de meldplicht bij een datalek vanuit de AVG. Onder de Wbni zijn vitale aanbieders verplicht om alle informatiebeveiligingsincidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening onmiddellijk te melden bij het Nationaal Cyber Security Centrum (NCSC). Bij overschrijding van een drempelwaarde dient de vitale aanbieder hiervan ook melding te maken bij de betreffende toezichthouder. Deze drempelwaarde verschilt per sector. De toezichthouder beoordeelt de melding en onderzoekt, indien nodig, of en op welke vlakken de vitale aanbieder de digitale weerbaarheid en het lerend vermogen moet vergroten. In 2023 zijn, net als in 2022, geen incidenten aan de toezichthouders gemeld waarbij de drempelwaarde werd overschreden.

3 Uitdagingen en ontwikkelingen in het toezicht



3.1 Inleiding

Dit hoofdstuk schetst de uitdagingen en ontwikkelingen in het toezicht. Het gaat in op de Europese richtlijnen NIS2 en CER en de daarmee gepaarde uitbreidingen van toezichtstaken. Daarnaast onderstreept dit hoofdstuk het belang van samenwerken in het toezicht in het licht van de komende ontwikkelingen.

3.2 Nieuwe Europese richtlijnen leiden tot uitdagingen voor toezicht

Het inspectiebeeld van vorig jaar ging in op twee nieuwe Europese richtlijnen die gezamenlijk moeten leiden tot een verbeterde bescherming van de EU-lidstaten. Het gaat om de *Critical Entities Resilience*-richtlijn (CER) en de *Network and Information Security*-richtlijn (NIS2). De CER richt zich op de bescherming tegen fysieke risico's zoals natuurrampen en terroristische aanslagen. De NIS2 focust op het versterken van de digitale weerbaarheid.

Het omzetten van de richtlijn tot nationale wetgeving is een omvangrijk en complex traject dat zorgvuldigheid vergt. De impact voor Nederlandse organisaties die onder de NIS2-richtlijn vallen is namelijk groot. Het omzetten van de richtlijnen in nationale wet- en regelgeving kost meer tijd dan van tevoren werd gedacht. Daarom is de Tweede Kamer eind januari 2024 geïnformeerd over het niet halen van de implementatiedeadline van oktober 2024. Hierdoor zullen de implementatiewetten later in werking treden. Totdat de wetten van kracht zijn, blijven de toezichthouders het toezicht uitvoeren vanuit de huidige wetgeving.

Op 21 mei 2024 is de internetconsultatie voor de Nederlandse implementatie van de NIS2 en de CER begonnen. De NIS2 krijgt vorm in de Cyberbeveiligingswet en de CER in de Wet weerbaarheid kritieke entiteiten.

Critical Entities Resilience (CER-richtlijn)
De CER-richtlijn is bedoeld om organisaties te beschermen tegen fysieke risico's, zoals de gevolgen van misdrijven, natuurrampen en gezondheidscrises. Het gaat hierbij om organisaties die essentiële diensten verlenen binnen bepaalde sectoren (bijvoorbeeld energie, drinkwater en overheidsdiensten) en als zogenaamde 'kritieke' entiteit zijn aangewezen. De verantwoordelijke ministeries voor deze sectoren bepalen welke organisaties kritieke entiteiten zijn en zorgen ervoor dat ze worden geïnformeerd.

Network and Information Security (NIS2-richtlijn)
De NIS2-richtlijn, net als de CER aangeduid in het Engels, vergroot de reikwijdte van de eerste NIS-richtlijn, doordat deze meer sectoren omvat. De NIS werd voorheen en ook in dit inspectiebeeld aangeduid in het Nederlands met Netwerk- en informatiebeveiligingsrichtlijn.

Onder de NIS2 vallen organisaties die behoren tot sectoren als afvalwater, overheidsdiensten, ruimtevaart, post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek, beheer van ICT-diensten en de maakindustrie. Daarnaast bevat de richtlijn een zorgplicht die organisaties verplicht zelf een risicoanalyse uit te voeren, op basis waarvan zij passende en evenredige maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen die ze gebruiken voor hun diensten. De leden van het bestuur van entiteiten moeten de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Daarvoor dienen zij een opleiding te volgen. Verder benoemt de richtlijn een meldplicht voor incidenten en een wettelijke registratieplicht voor organisaties die eronder vallen.

De komst van de CER en NIS2 levert voor een aantal toezichthouders nieuwe toezichtstaken op. Organisaties die binnen de *scope* van de richtlijnen vallen komen ook onder toezicht te staan. Dit betekent een aanzienlijke uitbreiding in het aantal organisaties en sectoren onder toezicht. Dit levert uitdagingen op voor zowel bestaande toezichthouders als nieuwe toezichthouders op het gebied van cybersecurity. Ze moeten toezicht gaan houden op een bredere en meer diverse groep organisaties. Om effectief om te gaan met deze uitbreiding is doorontwikkeling van het toezicht nodig. Momenteel wordt uitgewerkt welke sectoren onder welke toezichthouder gaan vallen.

Daarnaast breidt de *scope* van het toezicht uit naar fysieke weerbaarheid. Hierdoor wordt het delen van kennis en ervaring tussen toezichthouders extra belangrijk.

3.3 Samenwerking nodig voor doelgericht en doelmatig toezicht

Naast nieuwe vormen van toezicht, vragen de CER en NIS2 om een meer toekomstgerichte samenwerking tussen toezichthouders. Het kan bijvoorbeeld zo zijn dat een organisatie die onder de CER en/of NIS2 valt, actief is in meerdere sectoren en lidstaten. Deze organisatie krijgt dan te maken met verschillende toezichthouders. Een ander voorbeeld is dat een informatiebeveiligingsincident vanuit verschillende meldplichten bij meerdere toezichthouders gemeld moet worden. Daarom werken de bij dit inspectiebeeld betrokken toezichthouders samen in de werkgroep ‘samenwerkend toezicht digitale weerbaarheid’. De werkgroepleden brengen onder meer in beeld waar toezichthouders gedeelde verantwoordelijkheden hebben en maken afspraken om samen te komen tot doelgericht en doelmatig toezicht.

Gelet op het bovenstaande is er een noodzaak om de *governance* rondom de samenwerking te versterken. Daarom is recentelijk het ‘directeurenoverleg toezicht digitale weerbaarheid’ opgericht. Dit gremium fungeert als opdrachtgever van de werkgroep ‘samenwerkend toezicht digitale toezichthouders’. Het directeurenoverleg heeft, naast dit samenhangend inspectiebeeld, ook zaken op de agenda staan zoals de implementatie van toezicht, gezamenlijke communicatie en informatie-uitwisseling. Met de inrichting van deze samenwerkingsvormen streven de toezichthouders naar efficiënt toezicht en een zo laag mogelijke werklast voor organisaties die onder toezicht staan.

De CER en NIS2 zijn Europese richtlijnen die in alle lidstaten via nationale wetgeving van toepassing zijn. Zoals eerder aangegeven zijn organisaties soms actief in meerdere lidstaten. Grensoverschrijdende samenwerking is daarom ook van belang. De Europese NIS-toezichthouders werken in verschillende *workstreams* samen onder de Europese *NIS Cooperation Group*. In 2023 is de *workstream Supervision* opgericht om de samenwerking tussen Europese NIS-toezichthouders verder te intensiveren in aanloop naar de implementatie van de NIS2. Ook de nieuwe NIS2-toezichthouders zijn onderdeel van dit netwerk, dat de komende jaren verder uitgebouwd wordt. De *workstream Supervision* pakt onderwerpen op die om harmonisatie vragen op Europees niveau of die toezicht en handhaving kunnen versterken. In 2024 stellen de deelnemende toezichthouders het mechanisme van *mutual assistance* vast. Dit beschrijft op hoofdlijnen hoe de NIS2-toezichthouders uit verschillende lidstaten elkaar om assistentie kunnen vragen.

4 Doorontwikkeling samenwerkend toezicht



4.1 Inleiding

Dit hoofdstuk kijkt vooruit naar het komende jaar waarin de betrokken toezichthouders de samenwerking verder inrichten en professionaliseren. Paragraaf 4.2 en 4.3 gaan over de inhoudelijke keuzes ten aanzien van het Samenhangend Inspectiebeeld. Paragraaf 4.4 beschrijft de elementen van de doorontwikkeling van de *governance* in het komende jaar.

4.2 Risicomanagement ook komend jaar centraal

Risicomanagement is het meerjarige thema van het Samenhangend Inspectiebeeld. Het inspectiebeeld van vorig jaar zoomde specifiek in op risicomanagement bij leveranciers. Het huidige inspectiebeeld kijkt naar risicomanagement in brede zin, ofwel *Enterprise Risk Management* (ERM).

Risicomanagement blijft ook in de toekomst van groot belang. Het vormt de basis voor het opzetten en onderhouden van het geheel aan maatregelen dat een organisatie moet nemen. Met de steeds verdergaande digitale transformatie en het continu veranderende dreigingslandschap wijzigen ook de risico's continu. Dit vraagt om een structureel ingericht proces. Naast de behoefte aan inzicht in de risico's die door deze ontwikkelingen ontstaan, bestaat de behoefte om de groei van het volwassenheidsniveau van risicomanagement van organisaties te volgen. Met de komst van de NIS2 en CER komt daarbij de vraag hoe de nieuwe organisaties onder toezicht omgaan met risicomanagement en hoe dit zich verhoudt tot de organisaties die al langer onder het toezicht vallen.

4.3 Uitbreiding met het onderwerp assetmanagement

Eind 2023 maakte een deel van de toezichthouders afspraken over hoe ze invulling gaan geven aan het nieuwe thema assetmanagement. Op basis van de uitwerking van de *scope*, aanpak en analyse, nemen deze toezichthouders het thema zoveel mogelijk op in hun inspectieplanning voor 2024. Doel is om in het volgende Samenhangend Inspectiebeeld over het inspectiejaar 2024 een beeld te schetsen over assetmanagement.

Zicht op de risico's en de effectiviteit van maatregelen begint voor een organisatie namelijk met een goed overzicht van en inzicht in *assets*. De *assets* betreffen met name de ingezette IT- en OT-middelen en omvatten zowel de software als hardware die een organisatie inzet ten behoeve van vitale processen.

Niet alle toezichthouders hebben evenveel tijd en capaciteit beschikbaar. Dit hangt samen met uiteenlopende sectorale risico's, kaders, prioriteiten en manieren van inspecteren. Ondanks deze verschillen is afgesproken om daar waar mogelijk samen te werken aan het thema assetmanagement en de verdere doorontwikkeling ervan.

4.4 Versteviging governance samenwerkende toezichthouders

Sinds enkele jaren komen vertegenwoordigers van de betrokken toezichthouders op structurele basis bijeen in het overleg 'samenwerkend toezicht digitale weerbaarheid' voor afstemming over 1) het Samenhangend Inspectiebeeld en 2) ontwikkelingen in het toezicht zoals NIS2 en CER. Voordat deze wijze van samenwerken startte, was er sprake van losstaande bijeenkomsten en initiatieven tussen toezichthouders.

Het afgelopen jaar is aan dit structurele overleg een overleg op directeursniveau toegevoegd, zoals vermeld in paragraaf 3.3. Daarnaast is de insteek om - net als de tussenliggende laag met verantwoordelijk directeuren - ook de inspecteur-generaals en de andere algemeen directeuren expliciet op te nemen in de *governance*. Samen met het Bureau Inspectieraad geven de betreffende toezichthouders daar in 2024 vorm aan. Naar verwachting krijgt de Inspectieraad hierin een expliciete rol. Met deze governancestructuur krijgt de samenwerking tussen de betrokken toezichthouders een meer volwassen vorm.

Verder is het voornemen om meer structureel vorm te geven aan het onderling delen van kennis over de manieren van toezicht en handhaving. De toezichthouders gaan onderzoeken welke onderwerpen generiek kunnen worden opgepakt en welke onderwerpen een sectorspecifieke aanpak vereisen. Dit helpt om - naast het delen van kennis - elkaar concreet te versterken in het toezicht houden. De lopende implementatie van de NIS2 geeft hieraan een extra stimulans.



bijlage 1
Toezichtresultaten per toezichthouder



Toezichtresultaten per toezichthouder

	Sector	Vitaal proces	Grondslag
Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)			
Bekijk	Nucleaire sector	Bescherming van nucleaire inrichtingen en splijtstoffen	Regeling beveiliging nucleaire inrichtingen en splijtstoffen (Rbnis)
Autoriteit Persoonsgegevens (AP)			
Bekijk	Alle sectoren	*N.v.t.*	Algemene verordening gegevensbescherming (AVG)
De Nederlandsche Bank (DNB)			
Bekijk	Financiële sector	Betalings- en effectenverkeer	Wet op het financieel toezicht (Wft); Wet beveiliging netwerk- en informatiesystemen (Wbni).
Inspectie Gezondheidszorg en Jeugd (IGJ)			
Bekijk	Gezondheidszorg *Focus op ziekenhuizen in 2023*	Zorg	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz); Informatiebeveiligingsstandaard voor de zorg NEN 7510.
Inspectie Justitie en Veiligheid (IJenV)			
Bekijk	Openbare orde en veiligheid	Communicatie met en tussen hulpdiensten via 112 en C2000	Politiewet 2012; Wet veiligheidsregio's.
Inspectie Leefomgeving en Transport (ILT)			
Bekijk	Drinkwater	Drinkwatervoorziening	Wet beveiliging netwerk- en informatiesystemen (Wbni)
Bekijk	Luchtvaart	Vlucht- en vliegtuigafhandeling	Wet beveiliging netwerk- en informatiesystemen (Wbni)
Bekijk	Spoor	Vervoer over en beheer van het spoor	Wet beveiliging netwerk- en informatiesystemen (Wbni)
Rijksinspectie Digitale Infrastructuur (RDI)			
Bekijk	Diverse sectoren	Authenticatie vanuit eIDAS-vertrouwensdiensten	eIDAS-verordening; Wet digitale overheid (Wdo).
Bekijk	Energie en digitale Infrastructuur	• Landelijk en regionaal transport en distributie elektriciteit; • Gasproductie, landelijk en regionaal transport en distributie gas; • Olievoorziening; • Internettoegang en datadiensten.	Wet beveiliging netwerk- en informatiesystemen (Wbni)

Overzichtstabel met sector, vitaal proces en grondslag per toezichthouder.

ANVS

Toezichthouder: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)		
Sector:	Vitaal proces:	Grondslag:
Nucleaire sector	Bescherming van nucleaire inrichtingen en splijtstoffen	Regeling beveiliging nucleaire inrichtingen en splijtstoffen (Rbnis)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De ANVS heeft specifiek op het thema risicomanagement een sectoronderzoek uitgevoerd.
Hoeveel inspecties zijn er uitgevoerd?	Acht inspecties, bij verschillende organisaties.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Nee.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Nee.
ERM – Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Alle organisaties hebben hun ERM ingericht volgens ISO 27001.
2. Hoe ziet de governancestructuur van de organisatie eruit?	Alle organisaties hebben een governancestructuur in de vorm van het three lines model (3LM).
3. Is de risicobereidheid van het bestuur vastgelegd?	Ja, alle organisaties hebben de risicobereidheid vastgelegd.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	De meest vastgelegde security-gerelateerde toprisico's zijn: • insider threat; • informatiediefstal (information theft).
ISMS – Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	De meeste organisaties gebruiken ISO 27001.
6. Is het ISMS gecertificeerd?	Deels. Sommige organisaties zijn ISO 27001-gecertificeerd.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Ja. Alle organisaties hebben aan de hand van businessanalyses bepaald wat hun essentiële diensten zijn.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Ja. Alle organisaties hebben een dreigingsanalyse uitgevoerd op hun essentiële diensten.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. Alle organisaties hebben voor elke dreiging een inschatting gemaakt.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja, alle organisaties hebben risicomaatregelen gedefinieerd. Ja, alle restrisico's zijn geaccepteerd.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Ja. Alle organisaties hebben key controls ten behoeve van de gedefinieerde maatregelen en ze voeren deze toonbaar uit.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	Alle organisaties gebruiken rapportages en overzichten om verantwoording af te leggen over de resultaten van de key controls.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Ja. Alle organisaties gebruiken de resultaten van de key controls om verbeteringen door te voeren.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	Alle organisaties hebben een overzicht van de verbeteracties en hun status. Deze worden continu gemonitord en besproken met het management.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	Alle organisaties hebben het ISMS als onderdeel van een jaarlijkse management review. Sommige organisaties hebben meerdere reviews per jaar.

AP

Toezichthouder: Autoriteit Persoonsgegevens (AP)		
Sector:	Vitaal proces:	Grondslag:
Alle sectoren	N.v.t.	Algemene verordening gegevensbescherming (AVG)
Algemene informatie		
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De AP heeft het thema risicomanagement niet specifiek opgenomen in de toezichtstaken over het jaar 2023. Uit het jaarplan 2023 volgt dat de AP zich vooral heeft gefocust op de volgende drie onderwerpen: • algoritmes en AI; • big tech; • vrijheid en veiligheid.	
Hoeveel inspecties zijn er uitgevoerd?	N.v.t.	
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	N.v.t.	
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	N.v.t.	
ERM – Enterprise risk management		
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	N.v.t.	
2. Hoe ziet de governancestructuur van de organisatie eruit?	N.v.t.	
3. Is de risicobereidheid van het bestuur vastgelegd?	N.v.t.	
Toprisico's		
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	N.v.t.	
ISMS – Information security management system		
Plan		
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	N.v.t.	
6. Is het ISMS gecertificeerd?	N.v.t.	
Do		
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	N.v.t.	
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	N.v.t.	
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	N.v.t.	
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	N.v.t.	
Check		
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	N.v.t.	
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	N.v.t.	
Act		
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	N.v.t.	
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	N.v.t.	
Verantwoording		
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	N.v.t.	

DNB

Toezichthouder: De Nederlandsche Bank (DNB)		
Sector:	Vitaal proces:	Grondslag:
Financiële sector	Betalings- en effectenverkeer	• Art. 1:24 Wet op het Financieel Toezicht (Wft) • Wet beveiliging netwerk- en informatiesystemen (Wbni)
Algemene informatie		
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?		DNB zet risicomanagement in als een vast onderdeel van de gestructureerde uitvragen, om het risicoprofiel van de onder haar toezicht staande instellingen te beoordelen. Daarnaast voert DNB on-site inspecties uit op uiteenlopende risicodomeinen waarvan de beheersing van risico's in het algemeen een vast onderdeel uitmaakt. Ook adresseert DNB risicomanagement via het regulier toezicht, waarbij risicobeheersing één van de overkoepelende gespreksonderwerpen is.
Hoeveel inspecties zijn er uitgevoerd?		DNB houdt toezicht op een groot aantal instellingen in de financiële sector op basis van de Wet op het financieel toezicht (Wft). Hiervan is slechts een klein deel van deze organisaties in scope voor de Wbni. DNB hanteert een breed scala aan risicogebaseerde toezichtinstrumenten. Alle Wbni-instellingen zijn hierbij in scope. De toezichtinstrumenten bestaan naast inspecties onder meer uit basisprogramma's met periodieke gesprekken, verdiepende onderzoeken en uitvragen van specifieke gegevens.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?		De uitkomsten van onderzoeken (surveys) en vragenlijsten (questionnaires) gebruikt DNB onder andere om aanvullende toezichtinstrumenten, zoals gerichte inspecties en onderzoeken, in te zetten. Bevindingen van een onderzoek of inspectie deelt DNB in een rapport met het bestuur van een organisatie. Voor de opvolging van bevindingen wordt van organisaties verwacht dat ze een actieplan met daaraan gekoppelde tijdslijnen opstellen. De opvolging van dergelijke actieplannen wordt gemonitord door voortgangsgesprekken via regulier toezicht. Daarnaast beschikt DNB over formele en informele handhavingsinstrumenten om, indien nodig herstel en verbetering af te dwingen. Afhankelijk van de situatie bepaalt DNB of informeel danwel formeel optreden nodig is, en welke maatregel of combinatie van maatregelen getroffen wordt om het gewenste effect (normconform gedrag) te bereiken.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.		DNB werkt actief samen met de European Supervisory Authorities (ESA's), te weten EBA, EIOPA en ESMA, alsmede met de Europese Centrale Bank (ECB). Daarnaast werkt zij samen met de nationale toezichthouders in Europa inzake het toezicht op financiële instellingen, de Autoriteit Financiële Markten (AFM) en RDI.
ERM – Enterprise risk management		
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?		Sectorale wet- en regelgeving heeft in algemene zin als uitgangspunt dat organisaties verantwoordelijk zijn voor een beheerste bedrijfsvoering.
2. Hoe ziet de governancestructuur van de organisatie eruit?		Op basis van sectorale wetgeving is het gebruik van het three lines model (3LM) voor een deel van de organisaties verplicht, of het 3LM wordt als best practice gezien.
3. Is de risicobereidheid van het bestuur vastgelegd?		De risicobereidheid (risk appetite) en de risicotolerantie (risk tolerance) zijn nagenoeg altijd per risicotype (risk type) vastgelegd.
Toprisico's		
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?		De besturen onderkennen met name technologierisico's als onderdeel van het domein operational risk, alsmede risico's in de keten van uitbesteding.
ISMS – Information security management system		
Plan		
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?		Vanuit DNB zijn geen rode draden gebruikt. Organisaties zijn zelf verantwoordelijk voor de keuze van relevante rode draden.
6. Is het ISMS gecertificeerd?		Vaak. Een veel voorkomende certificering op het gebied van informatiebeveiliging in de financiële sector is ISO 27001.
Do		
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?		Meestal. Het uitvoeren van een business impact analyse (BIA) wordt in de regel uitgevoerd om onder meer de relatie tussen de essentiële diensten en de onderliggende systemen in kaart te brengen.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?		Indirect. Het uitvoeren van zelfbeoordelingen van risicobeheersing (risk control self assessments) is doorgaans een vast onderdeel van de risicomanagementcyclus (risk cycle). Het doel van zo'n risicoanalyse is het identificeren en beoordelen van risico's die de vertrouwelijkheid, integriteit en beschikbaarheid van de essentiële dienst kunnen verstoren.

9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	De kans en impact per risico wordt nagenoeg altijd bij risicoanalyses beoordeeld en geregistreerd, in samenhang met de mitigerende maatregelen. De resultaten van deze risicoanalyses slaan de organisaties op in een GRC-applicatie die fungeert als risicoregister. Met het gebruik van GRC-applicaties kunnen zogenoemde heat maps worden opgesteld. Deze plotten de risico's om visueel inzichtelijk te maken waar ze zich bevinden ten opzichte van de vastgestelde risicobereidheid.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	De organisatie legt mitigerende maatregelen vast. Als een restrisico de vooraf vastgestelde risicobereidheid overstijgt, moet een risicoacceptatie (risk acceptance) worden uitgevoerd. Een risicoacceptatie, ofwel vrijstelling (waiver), wordt doorgaans voor een tijdelijke, specifieke periode door de organisatie geaccepteerd. Na het verlopen van deze periode dient de organisatie de risicoacceptatie te actualiseren en deze opnieuw te beoordelen door het daartoe gemandateerde gremium.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Internal control frameworks zijn nagenoeg altijd geïmplementeerd. Het testen van controls in design en effectiveness wordt met een vastgestelde periodiciteit uitgevoerd. Interne controlefuncties zijn belast met het toetsen of de testprocedures volgens de vastgestelde procedure zijn uitgevoerd.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	Dashboards en interne rapportages over de uitkomsten van het testen van controls zijn over het algemeen aanwezig. De resultaten van het toetsen van de testresultaten door een interne controlefunctie zijn ook beschikbaar in een dashboard en/of interne rapportage. Alle resultaten worden in het algemeen op een geaggregeerd niveau opgenomen in een bedrijfsbrede ERM-rapportage die alle risicodomeinen bevat.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Als bij het testen of toetsen van controls blijkt dat control in design of effectiveness ineffectief is, registreert de organisatie dit doorgaans in de GRC-applicatie. Het opstellen van een verbeterplan is hier een vast onderdeel van.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	De voortgang van de verbeterplannen is te volgen in een GRC-applicatie en wordt visueel weergegeven in dashboards en/of in de overkoepelende ERM-rapportage.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	De inhoud van dashboards en periodieke rapportages met betrekking tot relevante elementen van de risicomanagementcyclus wordt op geaggregeerd niveau weergegeven in een overkoepelende ERM-rapportage.

IGJ

Toezichthouder: Inspectie Gezondheidszorg en Jeugd (IGJ)		
Sector:	Vitaal proces[9]:	Grondslag:
Gezondheidszorg	Zorg met focus op ziekenhuizen in 2023	• Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz); • Informatiebeveiligingsstandaard voor de zorg NEN 7510

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De IGJ houdt toezicht op de naleving van de NEN 7510. De wettelijke norm NEN 7510 beschrijft een managementsysteem voor informatiebeveiliging. Deze norm gaat uit van risicoanalyses op het gebied van informatiebeveiliging. Op basis van de uitkomsten van de risicoanalyse moeten organisaties gepaste beheersmaatregelen inrichten. Risicoanalyse is dus een integraal onderdeel van de norm. De NEN 7510 is gebaseerd op de ISO 27001. De NEN 7510 vereist ook dat er regelmatig een onafhankelijke beoordeling is van de status van de informatiebeveiliging. Op basis van de uitkomsten daarvan kan de organisatie bijsturen. Zo ontstaat een kwaliteitscyclus vanuit Plan-Do-Check-Act (PDCA). In de onafhankelijke beoordelingen komt ook het uitvoeren van risicoanalyses als onderwerp aan de orde. De IGJ betrekt in haar toezicht de resultaten van de onafhankelijke beoordeling, waaronder die op het gebied van risicoanalyse. Hoewel het toezicht van de IGJ zich richt op de gehele zorgsector, lag in 2023 wat betreft informatiebeveiliging de focus op ziekenhuiszorg.
Hoeveel inspecties zijn er uitgevoerd?	Ruim vijftig inspecties, bij ziekenhuizen. De inspectie heeft in 2023 ruim vijftig ziekenhuizen intensief gevolgd op het onderwerp informatiebeveiliging. Met vertegenwoordigers van elk ziekenhuis waren meerdere contactmomenten, zoals via schriftelijke vragen, bezoeken en videogesprekken.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Ja. Een veel voorkomende interventie is het laten opstellen en uitvoeren van verbeterplannen. Het laten uitvoeren van de in de norm vereiste, onafhankelijke beoordeling is daar veelal een onderdeel van. Het aantal ziekenhuizen dat aantoonbaar voldoet aan de NEN 7510 is in 2023 met een factor 3 toegenomen.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Nee. Er zijn in dit kader geen gezamenlijke onderzoeken uitgevoerd met een andere toezichthouder bij de desbetreffende ziekenhuizen. Wel is het zo dat ook op basis van de AVG eisen gelden op het gebied van informatiebeveiliging: de naleving van de AVG valt onder toezicht van de Autoriteit Persoonsgegevens (AP). De AP hanteert daarbij ook de NEN 7510 als norm. De autoriteit behandelt meldingen van datalekken en kan in het onderzoek naar meldingen aspecten van de NEN 7510 betrekken als daar aanleiding toe is. IGJ en AP hebben een samenwerkingsovereenkomst waarin de rolverdeling tussen IGJ en AP is opgenomen. De AP let vooral op de aspecten van informatiebeveiliging die raken aan de bescherming van persoonsgegevens. De IGJ let vooral op de relatie met de continuïteit van de zorg. Een ander relevant aspect is dat zorgaanbieders zoals ziekenhuizen gebruikmaken van de producten en diensten van derden, bijvoorbeeld applicaties en netwerkbeheersdiensten. Leveranciersmanagement voor wat betreft informatiebeveiliging is een onderdeel van de norm NEN 7510. Het kan voorkomen, maar het is geen automatisme, dat sommige dienstenleveranciers op hun beurt onder het toezicht van andere inspecties vallen, zoals dat van de Rijksinspectie Digitale Infrastructuur. Met name als de NIS2 van kracht gaat, waardoor meer entiteiten onder het toezicht vallen, is het zinvol om te kijken of er in geval van incidenten bij toeleveranciers samenwerking met een toezichthouder nodig is. Zo kan het toezicht op de keten mogelijk worden versterkt.

9 NB: in het kader van de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) zijn in de Nederlandse gezondheidszorg geen aanbieders van essentiële diensten (AED's) aangewezen. Onder de NIS2 zal dit wel het geval zijn. Het toezicht van de IGJ op het onderwerp informatiebeveiliging is gebaseerd op het wetgevend kader van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, waarin de NEN 7510 verplicht is gesteld voor zorgaanbieders. In 2023 besteedde de IGJ extra aandacht aan de informatiebeveiliging bij ziekenhuizen; deze tabel beperkt zich tot deze subsector (in de praktijk vond steekproefsgewijs ook toezicht plaats bij andere typen organisaties).

ERM – Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Bij het toezicht op informatiebeveiliging hanteert de IGJ vanuit de wettelijke norm – en daarmee ook de best practice – NEN 7510. Het risicomanagement voor informatiebeveiliging is een onderdeel van de NEN 7510. Informatiebeveiliging is in het algemeen onderdeel van thematisch toezicht. Het kan voorkomen dat een zorgaanbieder het risicomanagement voor informatiebeveiliging inbedt in een bredere vorm van ERM, maar dit is niet de focus van het thematisch toezicht op informatiebeveiliging. Uiteraard komt het omgaan met risico's ook ter sprake bij toezicht op andere aspecten van kwaliteit van zorg, zoals patiëntveiligheid of medicatieveiligheid. Zo is het gebruikelijk om bij het introduceren van medische hulpmiddelen een prospectieve risico-inventarisatie uit te voeren.
2. Hoe ziet de governancestructuur van de organisatie eruit?	De NEN 7510 geeft zorgaanbieders de vrijheid om zelf een geschikte organisatievorm voor de informatiebeveiliging in te richten. Daarbij is het wel een expliciete eis dat er een Informatie¬beveilings¬management¬forum (IBMF) wordt ingericht. Dit forum moet zorgen voor een duidelijke aansturing en zichtbare ondersteuning vanuit het management voor beveiligingsinitiatieven. Ook moet tenminste één individu verantwoordelijk zijn voor de beveiliging van gezondheidsinformatie binnen de organisatie. De NEN 7510 vereist ook onafhankelijke beoordelingen en een regelmatige directiebeoordeling. Dit leidt in de praktijk uiteraard tot verschillende organisatiespecifieke inrichtingskeuzes bij ziekenhuizen. In het algemeen is er sprake van een vorm van het 3LM: • Eerste verantwoordelijkheid voor informatiebeveiliging is belegd in het primaire proces (eerste lijn) bij medewerkers en lijnmanagers. • Daarnaast ligt een coördinerende, ondersteunende, adviserende en bewakende rol (tweede lijn) bij één of meer deskundigen, zoals een cyber information security officer (CISO). • Tot slot is er sprake van (derde lijn) onafhankelijke beoordelingen.
3. Is de risicobereidheid van het bestuur vastgelegd?	Nee. De NEN 7510 kent dit specifieke begrip niet. Wel moet de directie ervoor zorgen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en passen bij de strategie van de organisatie. Soms wordt bij onafhankelijke beoordelingen vastgesteld dat de informatiebeveiligingsdoelstellingen niet concreet genoeg zijn.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	In het kader van toezicht op informatiebeveiliging ligt de focus op informatiebeveiligingsrisico's. Bij dergelijk thematisch toezicht worden andere risico's, zoals financiële, over het algemeen buiten beschouwing gelaten. Incidenten op het gebied van informatiebeveiliging kunnen in de zorg onder andere te maken hebben met: • continuïteitsrisico's, zoals het risico op uitval van cruciale systemen bij bijvoorbeeld gijzelsoftware; • risico's op het gebied van vertrouwen of reputatie, zoals datalekken van gevoelige persoonsgegevens.
ISMS – Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	De best practice voor het ISMS in de gezondheidszorg is de NEN 7510.
6. Is het ISMS gecertificeerd?	Grotendeels. In november 2023 was ruim een derde van de ziekenhuizen gecertificeerd. Hoewel certificering niet verplicht is, werkten eind 2023 nog diverse ziekenhuizen vrijwillig aan certificatie. De verwachting is dat ruim 65% van de ziekenhuizen streeft naar certificering. Daarnaast kiest nog eens ruim 20% voor een alternatieve vorm van certificering door een bureau dat niet door de Raad voor Accreditatie is geaccrediteerd. De overige circa 15% ziekenhuizen kiest voor een andere vorm van regelmatig terugkerende, onafhankelijke beoordelingen.

Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Indirect. De zorg viel in 2023 niet onder de Wbni. In termen van de Wbni is deze vraag dus niet van toepassing. Wel moet in het kader van de NEN 7510-certificering de scope (het toepassingsgebied) van de informatiebeveiliging worden vastgesteld.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Indirect. De NEN 7510 spreekt in dit kader over risicobeoordeling. Risicobeoordelingen zijn wat betreft de NEN 7510 verplicht. Om aantoonbaar te kunnen voldoen aan de NEN 7510 moeten organisaties een risicobeoordeling uitvoeren. Uit onafhankelijke beoordelingen blijkt dat er op deze punten soms verbeteringen mogelijk zijn. Bijvoorbeeld dat de risicobeoordeling niet tijdig geactualiseerd is of dat beheersmaatregelen niet altijd duidelijk gekoppeld zijn aan de uitkomst van de risicobeoordelingen. Zulke constateringen leiden dan tot het actualiseren en/of aanscherpen van de risicoanalyse.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. De NEN 7510 spreekt over risicobeoordeling. In het algemeen geldt dat ziekenhuizen gebruikmaken van een methodiek waarbij de kans en impact van risico's wordt ingeschat om de omvang ervan onderling te kunnen wegen.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja. Dit is in het algemeen onderdeel van het risicobeoordelingsproces. Tijdens onafhankelijke beoordelingen komt soms naar voren dat het koppelen van beheersmaatregelen aan specifieke risico's niet helemaal duidelijk is of dat restrisico's niet expliciet zijn vastgesteld.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Meestal. De NEN 7510 vereist dat de organisatie vaststelt wat moet worden gemonitord en gemeten. Bij onafhankelijke beoordelingen van het ISMS is dit vaak een verbeterpunt. Het inrichten van een goede auditplanning en het duidelijk vaststellen van wat gemeten moet worden, is vaak een leerpunt. Dat is met name het geval bij ziekenhuizen waar het ISMS nog relatief nieuw is. Voor certificering is deze inrichting een vereiste.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	De NEN 7510 vereist een regelmatige directiebeoordeling, waarbij de resultaten van interne audits en onafhankelijke beoordelingen worden betrokken. Bij onafhankelijke beoordelingen blijken er vaak nog verbeteringen mogelijk op dit punt. Bijvoorbeeld omdat de directiebeoordeling niet alle elementen omvat die de norm voorschrijft.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Meestal. Zie ook het antwoord op vraag 11. Organisaties stellen niet altijd duidelijk vast wat gemonitord en gemeten moet worden. Daarmee is het dan ook lastig om op basis van de resultaten bij te sturen. Dit is wel vereist om te komen tot een werkende PDCA-cyclus. Zo'n werkende PDCA-cyclus is de kern van de NEN 7510. Ziekenhuizen waarbij het ISMS nog relatief nieuw is, hebben niet altijd al een complete verbetercyclus doorlopen. Dit komt dan naar voren bij onafhankelijke beoordelingen. Voor certificering is het uiteraard een vereiste dat er een aantoonbare verbetercyclus aanwezig is.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	Vaak is er een geconsolideerde actielijst, in een of andere vorm. Door middel van specifieke applicaties bijvoorbeeld, is het eenvoudiger om de acties op te volgen. Die combinatie met specifieke applicaties voor het algemene kwaliteitssysteem kan daarbij voordelen opleveren. Ziekenhuizen maken hier in de praktijk verschillende keuzes in. Soms blijkt uit resultaten van onafhankelijke beoordelingen dat de traceerbaarheid van verbeteracties nog een aandachtspunt is. Dit is met name het geval bij ziekenhuizen waar het ISMS nieuw is.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	Dit kan op de volgende manieren plaatsvinden: • vanuit het IBMF (zie ook het antwoord op vraag 2); • door een verantwoordelijk functionaris zoals de CISO en/of; • via onafhankelijke beoordelingen. Voldoende betrokkenheid vanuit het bestuur is daarvoor wel een vereiste. Met name als het ISMS in een beginstadium is, kan uit onafhankelijke beoordelingen blijken dat het bestuur te veel op afstand staat. Dit is dus een aandachtspunt voor sommige ziekenhuizen.

IJenV

Toezichthouder: Inspectie Justitie en Veiligheid (IJenV)		
Sector:	Vitaal proces:	Grondslag:
Openbare orde en veiligheid	Communicatie met en tussen hulpdiensten middels 112 en C2000	• Politiewet 2012 • Wet veiligheidsregio's

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De IJenV heeft risicomanagement niet meegenomen in het toezicht over 2023.
Hoeveel inspecties zijn er uitgevoerd?	Geen.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Geen.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Nee.
ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Geen onderzoek naar gedaan: n.v.t.
2. Hoe ziet de governancestructuur van de organisatie eruit?	De meldkamers zijn onderdeel van het stelsel rampenbestrijding en crisisbeheersing. Op het gebied van informatiebeveiliging is recent het strategisch kader informatiebeveiliging meldkamervoorzieningen gepubliceerd in de Staatscourant.
3. Is de risicobereidheid van het bestuur vastgelegd?	N.v.t.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	N.v.t.
ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	N.v.t.
6. Is het ISMS gecertificeerd?	N.v.t.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	N.v.t.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	N.v.t.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	N.v.t.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	N.v.t.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	N.v.t.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	N.v.t.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	N.v.t.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	N.v.t.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	N.v.t.

ILT - Drinkwater

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)		
Sector:	Vitaal proces:	Grondslag:
Drinkwater	Drinkwatervoorziening	Wet beveiliging netwerk- en informatiesystemen (Wbni)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De ILT heeft in 2023 verdiepende inspecties uitgevoerd bij drinkwaterbedrijven, met als thema detectie en respons. Binnen dit thema komt de werking van risicomanagement aan bod bij de onderwerpen kwetsbaarheden, logging, monitoring, detectie en incidentrespons.
Hoeveel inspecties zijn er uitgevoerd?	Tien inspecties bij drinkwaterbedrijven.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Ja. Naar aanleiding van bevindingen uit deze inspecties hebben de drinkwaterbedrijven diverse verbeterplannen opgesteld. De verbeterpunten betreffen met name de risico's en maatregelen vanuit het thema detectie en respons. Bij een enkel drinkwaterbedrijf gaat het om het opnemen van de monitoringmaatregelen in het eigen risicomanagementraamwerk.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Nee.
ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Een verstoringsrisicoanalyse (VRA) en een leveringsplan (op basis van all hazard) is verplicht voor drinkwaterbedrijven. Deze twee documenten zijn onderdeel van het vergunningsproces. Cybersecurity is onderdeel van de VRA.
2. Hoe ziet de governancestructuur van de organisatie eruit?	De governance is over het algemeen ingericht aan de hand van het three lines model (3LM). De drinkwaterbedrijven nemen zelf interne audits af. De volwassenheid verschilt per organisatie. Vanuit de financiële verantwoording is het 3LM over het algemeen aardig volwassen. Verdere inbedding van cybersecurity in het 3LM vraagt nadere aandacht. Een externe partij, aangesteld vanuit de Vereniging van drinkwaterbedrijven in Nederland (Vewin), neemt bij elk drinkwaterbedrijf voor de tweede keer een externe audit af op de PA-norm (procesautomatisering). PA is hier een expliciet onderdeel van. De eerdere externe audit controleerde de opzet en aanwezigheid van maatregelen. Bij deze audit heeft de externe partij naar de opzet, de aanwezigheid en de werking van de maatregelen gekeken.
3. Is de risicobereidheid van het bestuur vastgelegd?	Ja. Vanuit de VRA hebben alle besturen een risicoacceptatiematrix vastgesteld.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	Vanuit de besturen van de drinkwaterbedrijven komen de volgende toprisico's omtrent security naar voren: • ransomware; • phishing; • sabotage (door zowel interne als externe partijen).
ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	De drinkwaterbedrijven hanteren het ISO 27001-raamwerk.
6. Is het ISMS gecertificeerd?	Nee. Enkele van de organisaties denken na over een eventuele ISO 27001-certificering.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Ja. Alle drinkwaterbedrijven hebben de business-impactanalyse uitgevoerd aan de hand van de VRA en de leveringsplannen.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Ja. De dreigingsanalyse op de essentiële dienst is onderdeel van de VRA.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. Per dreiging zijn de kans en impact meegenomen in de VRA.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja. De organisaties hebben voor de vastgelegde risico's mitigerende maatregelen beschreven. De ILT heeft in het afgelopen jaar, bij de sector drinkwater, de acceptatie van restrisico's niet meegenomen als onderdeel van de verdiepende inspectie.

Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Deels. Op operationeel niveau hebben de drinkwaterbedrijven de maatregelen ingericht, onder meer op basis van het monitoren op key controls. Deze key controls zijn echter niet altijd expliciet vastgelegd. De volwassenheid en diepgang ervan verschilt per organisatie.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	Voor veel van de maatregelen hebben de drinkwaterbedrijven KPI's gedefinieerd om periodiek te rapporteren richting de directie. De directie legt periodiek verantwoording af aan de RvB/RvC, vaak met dezelfde rapportage of een samenvatting hiervan. Een aantal van deze kengetallen zetten de organisaties in als key controls om de effectiviteit van de maatregelen te meten. Het volwassenheidsniveau in de managementverantwoording verschilt per organisatie.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Soms. De drinkwaterbedrijven onderkennen benodigde verbeteringen. Deze verbeteringen zijn echter niet altijd expliciet afkomstig van de resultaten van de key controls.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	De organisaties houden verbeteracties bij in zowel overzichtsdocumenten als met specifieke applicaties. Het bijhouden en rapporteren is belegd bij verantwoordelijk functionarissen.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	In de periodieke managementrapportages staat over het algemeen verantwoording over maatregelen en de eventuele key controls. De verantwoording over het ISMS zelf is tijdens de inspecties niet aan bod gekomen.

ILT - Luchtvaart

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)		
Sector:	Vitaal proces:	Grondslag:
Luchtvaart	Vlucht- en vliegtuigafhandeling	Wet beveiliging netwerk- en informatiesystemen (Wbni)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De ILT neemt het thema risicomanagement voor de sector luchtvaart niet mee in dit Samenhangend Inspectiebeeld over 2023. De ILT heeft in 2023 namelijk geen cybersecurity-inspecties uitgevoerd in deze sector. Gedurende 2021 en 2022 deed de ILT de eerste verkennende inspecties binnen de sector luchtvaart. De ILT voert begin 2024 cybersecurity-inspecties uit bij nieuwe luchtvaartmaatschappijen en luchthavens. Ook vinden nadere inspecties plaats bij luchtvaartorganisaties die de ILT in 2021 en 2022 bezocht.
Hoeveel inspecties zijn er uitgevoerd?	Geen.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	N.v.t.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	N.v.t.
ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	N.v.t.
2. Hoe ziet de governancestructuur van de organisatie eruit?	N.v.t.
3. Is de risicobereidheid van het bestuur vastgelegd?	N.v.t.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	N.v.t.
ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	N.v.t.
6. Is het ISMS gecertificeerd?	N.v.t.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	N.v.t.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	N.v.t.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	N.v.t.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	N.v.t.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	N.v.t.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	N.v.t.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	N.v.t.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	N.v.t.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	N.v.t.

ILT - Spoor

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)		
Sector:	Vitaal proces:	Grondslag:
Spoor	Vervoer over en beheer van het spoor	Wet beveiliging netwerk- en informatiesystemen (Wbni)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	Eind 2022 is de ILT binnen de sector spoor gestart met de verkennende inspecties. Halverwege 2023 rondde de ILT deze af. Risicomanagement is een standaardonderdeel van de verkennende inspectie.
Hoeveel inspecties zijn er uitgevoerd?	Zes inspecties bij spoorbedrijven.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Ja. Naar aanleiding van de uitkomsten van de verkennende inspecties bij de sector spoor zijn enkele verbeterplannen opgesteld.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Nee.
ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	De spoororganisaties leggen de risico's voor informatiebeveiliging en cybersecurity vast op afdelingsniveau. Dit doen ze meestal niet in een centraal risicoregister in de organisatie.
2. Hoe ziet de governancestructuur van de organisatie eruit?	De governance is vaak ingericht aan de hand van het three lines model (3LM). In een aantal gevallen is de derde lijn van dit model nog niet ingericht. Soms zet de organisatie voor de invulling van de derde lijn externe inhuur in.
3. Is de risicobereidheid van het bestuur vastgelegd?	Vaak. Bij veel van de betrokken organisaties heeft de directie het risicoacceptatieniveau vastgesteld.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	Vanuit de betrokken directies komt ransomware als toprisico naar voren.
ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	Voor de inrichting van het ISMS gebruiken de spoororganisaties het ISO 27001-raamwerk.
6. Is het ISMS gecertificeerd?	In een enkel geval. Een enkele organisatie is al ISO 27001-gecertificeerd. De scope van deze certificering is echter veelal beperkt en de organisatie breidt deze nu uit. Andere organisaties zetten ondertussen ook stappen richting het certificeren van het ISMS volgens ISO 27001.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Grotendeels. De meeste spoororganisaties hebben een business-impact-analyse uitgevoerd. In een aantal gevallen betreft dit alleen het domein informatietechnologie (IT). Deze organisaties nemen nu vanuit hun verbeterplannen ook het domein operationele technologie (OT) mee.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Indirect/deels. Naast de risicoanalyses voeren de organisaties veelal dreigingsanalyses uit op de essentiële dienst. Zij hebben het onderdeel leveranciersmanagement in deze analyse echter niet altijd meegenomen. Deze organisaties hebben dit nu opgenomen in hun verbeterplannen.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. Per beschreven risico leggen de organisaties de kans en impact vast. De diepgang van deze vastlegging verschilt per organisatie.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja. Per beschreven risico leggen de organisaties ook de bestaande en te implementeren maatregelen vast, net als het eventuele restrisico. De diepgang van deze vastlegging en het volwassenheidsniveau van het acceptatieproces van de restrisico's varieert per organisatie.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Deels. In de praktijk hebben de spoororganisaties vaak key controls op de maatregelen ingericht, onder meer vanuit monitoring. De organisaties hebben deze key controls echter vaak niet expliciet vastgelegd. Per organisatie verschilt de volwassenheid en diepgang.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	In de meeste gevallen hebben de spoororganisaties voor de maatregelen KPI's gedefinieerd, voor een periodieke rapportage richting de directie. Een aantal van deze kengetallen zet de organisatie in als key controls om de effectiviteit van de maatregelen te meten.

Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Deels. De organisaties onderkennen benodigde verbeteringen. Deze verbeteringen zijn echter niet altijd expliciet afkomstig van de resultaten van de key controls.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	De spoororganisaties hanteren verbeterplannen, roadmaps, projecten en wijzigingen voor het uitzetten en monitoren van verbeteracties. De organisaties registreren deze zaken in overzichtsdocumenten of middels specifieke software. Het bijhouden en rapporteren doen verantwoordelijke functionarissen. Controle op de opvolging van verbeteracties vindt niet altijd plaats.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	De verantwoording aan het bestuur loopt veelal via periodieke rapportages. Deze bevatten over het algemeen de verantwoording vanuit de maatregelen met eventuele key controls. De verantwoording over het ISMS zelf is tijdens de inspecties niet aan bod gekomen.

RDI - eIDAS

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI)		
Sector:	Vitaal proces:	Grondslag:
Diverse sectoren	Authenticatie vanuit eIDAS-vertrouwensdiensten	• eIDAS-verordening • Wet digitale overheid (Wdo)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De RDI voert vanuit de eIDAS-verordening toezicht op de Trusted Service Providers (TSP's). In deze groep onderscheidt men gekwalificeerde en niet-gekwalificeerde partijen. Oftewel: qualified TSP's (qTSP's) en non-qualified TSP's (non-qTSP's). De RDI voert deze inspecties uit vanuit risicoperspectief. Een eerste en tweede inspecteur gaat op basis van een risicoanalyse minstens één keer per twee jaar bij iedere qTSP langs.
Hoeveel inspecties zijn er uitgevoerd?	Acht inspecties, zowel bij non-qTSP's als bij qTSP's.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Ja. In 2023 zijn op verschillende momenten in het jaar twee bezoeken gebracht aan een non-qTSP, naar aanleiding van een melding uit het veld. Tijdens het onderzoek bleek dat deze partij niet voldeed aan een van de artikelen van de eIDAS-verordening. Aan de oproep voor herstel en de gestelde deadline gaf de partij geen juist gehoor. De non-qTSP ontvangt een rapport van bevindingen. Dit traject loopt nog in 2024.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Ja. Logius is beheerder en policy authority van het PKIo-stelsel. Vanuit het toezicht op het PKIo-stelsel controleert zij ook de werkzaamheden van TSP's die certificaten uitgeven voor de overheid onder de betreffende root van deze PKI. Op uitnodiging van het RDI heeft een toezichthouder van Logius als toehoorder meegekeken met de eIDAS-inspecties. Aanleiding is de overlap van elkaars toezichtdomein. Zo zijn de plannen voor de toekomst van de TSP en hedendaagse vraagstukken in het eIDAS-domein ook relevant voor het toezicht dat Logius uitvoert.

ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Alle TSP's gebruiken over het algemeen de 319-familie uit het ETSI-normenkader. Het gebruik van de ETSI-normering vormt overigens geen verplichting voor de TSP. Dit mag ook een ander relevant normenkader zijn.
2. Hoe ziet de governancestructuur van de organisatie eruit?	Dit hangt af van het type organisatie. Zo is voor overheidspartijen de governance over het algemeen anders dan voor commerciële partijen. De eerder genoemde ETSI-kaders en ook de ENISA-richtlijnen geven voor de TSP aan hoe een organisatie een dienst moet inrichten. Daarnaast geven ze voor de toezichthouder RDI aan hoe deze een goed beeld krijgt en hoe daarop te sturen. Voor elke managementlaag is een ander soort risicobeheersing en een aparte verantwoordelijkheid beschreven: • operationeel management: risicobeheersing op basis van incident respons en operationele veiligheid op bijvoorbeeld netwerkniveau; • tactisch management: risicobeheersing van de gehele keten en interne audits; • strategisch management: eindverantwoordelijkheid voor risicobeheersing op alle fronten en het voldoen aan zorg- en meldplicht, opstellen en beheren van een termination plan en risicobeheersing op basis van externe audits.
3. Is de risicobereidheid van het bestuur vastgelegd?	Ja. De risk assessments zijn over het algemeen bij alle TSP's goed beoordeeld. Zo komen major non-conformities zelden voor De confirmity assessment body (CAB) voert deze beoordeling uit. Het vastleggen van de risicobereidheid is onderdeel van de norm (ETSI 319 401). Tijdens inspecties bij de partijen bespreekt de RDI standaard dit onderdeel.

Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	Vanuit het bestuur komen als toprisico's met name naar voren: • identiteitsfraude; • foutief uitgegeven certificaten; • beëindiging van dienstverlening; • gecompromitteerd raken van cryptografisch materiaal; • lekken van persoonsgegevens; • risicoacceptatie door het management. Voor risicoacceptatie door het management geldt: te hoge acceptatie is onwenselijk, te lage acceptatie is mogelijk onwerkbaar.

ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	Vaak wordt ISO 27005 gebruikt.
6. Is het ISMS gecertificeerd?	Ja, aan de hand van het ISO 27001-certificaat. Daarnaast zijn de qTSP's veelal op basis van de ETSI-kaders door CAB's gecertificeerd. De CAB's nemen hierin, meer dan in de ISO 27001-certificering, de eisen mee die aan TSP's worden gesteld.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Ja. De RDI verwacht van de TSP een uitgeschreven beschrijving van de betreffende vertrouwensdienst te ontvangen, als onderdeel van het registratieproces en ten behoeve van een gekwalificeerde dienst. Deze dienstbeschrijving omvat de elementaire componenten om de dienst betrouwbaar te kunnen draaien. Ketenverantwoordelijkheid is een van deze componenten. Daarnaast moet de organisatie inzichtelijk maken dat men oog heeft en houdt voor de specifieke risico's vanuit haar rol als TSP.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Ja. In de meestal jaarlijks of soms tweejaarlijks afgenomen audits door de CAB's, is risicomanagement een specifiek onderdeel. Het beschikbaar stellen van een analyse waarin specifieke dreigingen zijn geadresseerd, hoort hierbij. De RDI neemt als toezichthouder kennis van de CAB's en gaat in overleg met de TSP's als zij ziet dat hier onvoldoende aandacht voor is. De TSP dient te handelen conform artikel 19 in de huidige eIDAS-verordening ('passende technische en organisatorische maatregelen om risico's te beheren'). De TSP is daarbij verantwoordelijk om de toezichthouder binnen 24 uur op de hoogte te stellen in het geval van een (bijna)incident. Hiernaast verwachten wij dat de TSP invulling geeft aan de ETSI-normen die artikel 19 nader specificeert op het gebied van risicomanagement.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. De RDI ziet en verwacht deze invulling als onderdeel van de risico-analyse en van passende maatregelen. Zie ook antwoord 8.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja. Tijdens inspecties kijkt de RDI naar de risk assessment-implementatie. De focus ligt daarbij met name op de eIDAS-gerelateerde risico's, waaronder cybersecurity. De RDI ziet en verwacht ook dat de betreffende partijen cybersecurity-maatregelen als onderdeel van de risicoanalyse hebben beschreven. Zie ook antwoord 8.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Ja. Dit is onderdeel van de verplichte passende maatregelen.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	De TSP's hanteren interne en externe audits en een jaarlijkse management review.
Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Ja. Dit is onderdeel van de interne en externe auditcyclus van de TSP's.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	De TSP's leggen de opvolging veelal vast via een ticketsysteem, zoals Jira, en via interne structurele overleggen. Zo nodig krijgt de opvolging navolging via een escalatieproces of middels ketenoverleggen.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	De TSP's leggen onder andere verantwoording af over het ISMS in managementoverleggen en door het delen van externe audit-resultaten.

RDI - Wbni

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI)		
Sector:	Vitaal proces:	Grondslag:
Energie en digitale infrastructuur	• Landelijk en regionaal transport en distributie elektriciteit; • Gasproductie, landelijk en regionaal transport en distributie gas; • Olievoorziening; • Internettoegang en datadiensten.	Wet beveiliging netwerk- en informatiesystemen (Wbni)

Algemene informatie	
Op welke manier is het thema risicomanagement opgenomen in de toezichtstaken over het jaar 2023?	De RDI voerde thema-inspecties uit bij een risicogebaseerde selectie van energieproducenten. Een thema-inspectie is een diepgaand onderzoek op basis van een principle based normenkader.
Hoeveel inspecties zijn er uitgevoerd?	Zes inspecties bij de grootste energieproducenten.
Zijn er interventies toegepast naar aanleiding van geconstateerde gebreken/tekortkomingen? Zo ja, welke interventie(s)?	Ja. Diverse organisaties hebben verbeteringen onderkend en opgepakt, naar aanleiding van bevindingen uit de inspecties.
Is er in de uitvoering van de toezichtstaak sprake van samenwerking (zoals een gezamenlijk onderzoek) of samenhang met een andere toezichthouder? Beschrijf de samenwerking/ samenhang.	Ja. Met het olietransport vanuit de havens en de olieopslag op de havens kennen de RDI en de ILT een overlap in het inspectiedomein. In 2023 liep een inspecteur van de ILT daarom met twee inspecties van de RDI mee.
ERM - Enterprise risk management	
1. Welke best practice gebruikt de organisatie voor de inrichting van het ERM?	Voor de inrichting van ERM gebruiken de organisaties verschillende methoden. Dit kan zowel een zelfontwikkelde methode zijn als een best practice. Gebruikte best practices zijn onder andere COSO en ISO 31000.
2. Hoe ziet de governancestructuur van de organisatie eruit?	Alle organisaties hebben hun governancestructuur gebaseerd op het three lines model (3LM).
3. Is de risicobereidheid van het bestuur vastgelegd?	Ja. Alle organisaties hebben de risicobereidheid van het bestuur vastgelegd.
Toprisico's	
4. Welke toprisico's van het bestuur van de organisatie zijn gerelateerd aan (cyber)security?	Alle organisaties hebben op bestuursniveau security-gerelateerde risico's onderkend of zijn hier mee bezig. Risico's zijn onder andere: • cyberaanvallen; • OT-malware; • supply chain attacks.
ISMS - Information security management system	
Plan	
5. Welke best practice heeft de organisatie gebruikt voor de inrichting van het ISMS?	Alle organisaties hanteren ISO 27001 als best practice voor de inrichting van hun ISMS.
6. Is het ISMS gecertificeerd?	Nee. Op dit moment is geen een organisatie ISMS-gecertificeerd. Een enkele organisatie heeft dit wel gepland.
Do	
7. Heeft de organisatie een businessanalyse uitgevoerd om te bepalen wat de essentiële dienst is?	Ja. Alle organisaties hebben business-analyses uitgevoerd. Hierdoor hebben zij inzicht op de scope van de essentiële dienst.
8. Heeft de organisatie een dreigingsanalyse uitgevoerd op de essentiële dienst?	Ja. Alle organisaties hebben dreigingsanalyses uitgevoerd op de essentiële dienst.
9. Heeft de organisatie voor elke dreiging de kans en impact ingeschat?	Ja. Alle organisaties hebben per dreiging de kans en impact ingeschat.
10. Heeft de organisatie voor elk risico maatregelen gedefinieerd en eventuele restrisico's geaccepteerd?	Ja. Alle organisaties hebben per risico maatregelen gedefinieerd of zijn hiermee bezig. Bijna alle organisaties accepteren formeel restrisico's.
Check	
11. Heeft de organisatie key controls ten behoeve van de maatregelen gedefinieerd en voert de organisatie deze uit?	Ja. Alle organisaties hebben key controls gedefinieerd ten behoeve van de maatregelen en voeren deze uit.
12. Op welke wijze legt het management verantwoording af over de resultaten van de key controls?	Binnen alle organisatie legt het management verantwoording af over de resultaten van de key controls. De vorm waarin de verantwoording wordt afgelegd verschilt per organisatie. Bijvoorbeeld periodieke rapportages, interne controleverklaringen (ICV) - ook bekend als in control statements (ICS) - en directiebeoordelingen.

Act	
13. Onderkent de organisatie verbeteringen op basis van de resultaten van de key controls?	Ja. Alle organisaties onderkennen verbeteringen op basis van de resultaten van key controls.
14. Op welke wijze bewaakt de organisatie de opvolging van verbeteracties?	Alle organisaties bewaken de opvolging van verbeteracties. Gebruikte middelen hierbij zijn onder andere periodieke rapportages en -overleggen en risicomanagement-software.
Verantwoording	
15. Op welke wijze legt de organisatie verantwoording over het ISMS af aan het bestuur?	Bijna alle organisaties leggen formeel verantwoording over het ISMS af aan het bestuur. Dit vindt plaats middels rapportages of overleggen. Een enkele organisatie richt de verantwoordingsstructuur op dit moment formeel in.

bijlage 2
Bronnen



1. Richtlijn (EU) 2016/1148, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016L1148&qid=1680093737005

2. Wet beveiliging netwerk- en informatiesystemen, via https://wetten.overheid.nl/BWBR0041515/2022-12-01

3. 'Vitale Infrastructuur', NCTV, https://www.nctv.nl/onderwerpen/vitale-infrastructuur

4. 'Vitale aanbieders', NCTV, https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders

5. 'Samenhangend Inspectiebeeld cybersecurity vitale processen 2021-2022', toezichthouders op cybersecurity van vitale processen, https://www.rijksoverheid.nl/documenten/rapporten/2022/07/06/tk-bijlage-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-21-22

6. 'Samenhangend Inspectiebeeld cybersecurity vitale processen 2023', https://www.rijksoverheid.nl/documenten/rapporten/2023/07/03/tk-bijlage-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2023

7. Richtlijn (EU) 2022/2555, via https:/eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022L2555&qid=1680094478347

8. Verordening (EU) 2016/679, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679&qid=1680094520396

9. 'Cybersecurity Woordenboek 2021', Cybersecurity Alliantie, https://www.cybersecurityalliantie.nl/ecp_images/2021/05/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf

10. 'Start een ketensamenwerking, handreiking', NCSC, https://www.ncsc.nl/documenten/publicaties/2019/mei/01/samen-in-keten

11. 'Operational Technology', Digital Trust Centre, https://www.digitaltrustcenter.nl/informatie-advies/operational-technology

12. 'TIBER-NL', DNB, https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl/

13. Basismaatregelen cybersecurity, NCSC, https://www.ncsc.nl/onderwerpen/basismaatregelen

14. Richtlijn (EU) 2022/2557, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022L2557&qid=1680095388684

15. Verordening (EU) 2022/2554, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022R2554&qid=1680096148067

16. 'Nederlandse Cybersecuritystrategie 2022-2028', NCTV, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028

17. 'Nieuwe technologieën en nieuwe samenwerkingen', Inspectieraad, https://www.rijksinspecties.nl/onderwerpen/programma-innovatie-toezicht/nieuwe-technologieen-en-nieuwe-samenwerkingen

18. 'Actieplan Nederlandse Cybersecuritystrategie 2022-2028', NCTV, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

19. 'Jaarplan 2024 - Netwerksamenwerking voor een betrouwbare digitale infrastructuur', https://www.rdi.nl/actueel/nieuws/2024/02/21/rdi-publiceert-jaarplan-2024#:~:text=In%20het%20jaarplan%202024%20staan,veilige%20en%20betrouwbare%20digitale%20infrastructuur

20. 'DNB ziet cyberdreiging toenemen terwijl basismaatregelen niet altijd op orde zijn', https://www.dnb.nl/nieuws-voor-de-sector/oud/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/

Dit is een uitgave in opdracht van het Overleg Toezichthouders cybersecurity vitale processen

Voor meer informatie over deze uitgave:

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen

communicatie@rdi.nl
T: +31 (0) 88 041 60 00 (ma t/m vrij 8.30 - 17.00)

Juni 2024