Boardroom Training guideline

Met de nadruk op DORA en NIS2

Een guideline van NOREA

Postbus 242, 2130 AE Hoofddorp

Telefoon: +31 (0) 88 4960 380

Nederland

e-mail: norea@norea.nl

Deelnemers aan de taskforce

De auteurs van deze guideline van de Regulatory taskforce zijn:

Naam	Rol	Bedrijf
Danny Bos	Senior Manager Cyber Security & Privacy	Eraneos
Harry Boersen	CTO	ANVA
Iliass el Attoti	Manager Technology Risk	EY
Jesper de Boer	Director IT-audit	Deloitte
René Zendijk	Head of Internal Audit	Scildon
Shankar Sahtie	Consultant Cyber Security	SVJ Consultancy
Sandeep Gangaram Panday	Consultant Cyber Security	Brightlyn

Voor de volledige ledenlijst en overige door de Taskforce gemaakte content, zie https://www.norea.nl/regulatory

De guideline is gereviewed door:

Naam	Rol	Bedrijf
Arno Kroese	Partner Business & Digital Risk	Grant Thornton
Bart Pieters	Adviseur Informatiebeveiliging & Privacy	CIO Rijk van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Freddy Dezeure	Onafhankelijk adviseur	Freddy Dezeure BV
Martin van Vessem	CISO	CZ
Steven Debets	Partner	Highberg Digital

Toezichthouders

Deze guideline is gedeeld met diverse toezichthoudende instanties (DNB, AFM, Cbw toezichthouders) en het CIO Rijk, dat onderdeel uitmaakt van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De toezichthoudende autoriteiten en CIO Rijk hebben gezamenlijk de volgende reactie gegeven:

"Deze kennisdoelstellingen zijn opgesteld door NOREA om de sector te begeleiden bij de praktische implementatie van trainingen voor bestuursleden. DNB, AFM en de Cbw-toezichthoudende autoriteiten hebben niet bijgedragen aan de ontwikkeling ervan. De ontwikkeling van deze kennisdoelstellingen sluit aan bij eerdere initiatieven van DNB, AFM, de Cbw-toezichthoudende autoriteiten en CIO Rijk om binnen de sector samen te werken aan het vergroten van de algehele cyberweerbaarheid. DNB, AFM, de Cbw-toezichthoudende autoriteiten en CIO Rijk waarderen deze sectorale initiatieven die bijdragen aan het algemene bewustzijn van cyberweerbaarheid. DNB, AFM, de Cbw-toezichthoudende autoriteiten en CIO Rijk benadrukken dat het naleven van de toepasselijke wet- en regelgeving te allen tijde de verantwoordelijkheid van de instelling is. Het gebruik van deze guideline geeft geen garantie dat partijen daarmee handelen in overeenstemming met de wet- en regelgeving."

Disclaimer : Deze guideline voor bestuurstraining is een praktisch hulpmiddel om organisaties te ondersteunen bij het naleven van de toepasselijke regelgeving. Hoewel deze guideline waardevolle inzichten kan bieden, is het belangrijk te benadrukken dat de wettelijke vereisten zelf leidend blijven. Bovendien kan de relevante nationale wetgeving, die NIS2 implementeert via nationale wetgeving, aanvullende eisen bevatten.

Feedback kan gedeeld worden via norea@norea.nl

Inhoudsopgave

1. Inleiding

Naarmate de afhankelijkheid van ICT-systemen in alle sectoren van de samenleving toeneemt, heeft de Europese Unie (EU) twee belangrijke wetgevingen ingevoerd om de veelzijdige risico's waarmee kritieke sectoren worden geconfronteerd beter te beheersen: Verordening (EU) 2022/2554, beter bekend als de Digital Operational Resilience Act (DORA), en Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de hele Unie (de NIS2-richtlijn/NIS2). Deze twee wetten betekenen een aanzienlijke verschuiving in de EU-aanpak van cyberbeveiliging; samen dragen ze aanzienlijk bij aan een meer samenhangende en alomvattende EU-strategie voor cyberbeveiliging.

De NIS2-richtlijn is breed van toepassing op essentiële en belangrijke entiteiten in diverse sectoren, waaronder drie typen financiële instellingen [1]. In Nederland is de NIS2-richtlijn toegepast via de Nederlandse implementatiewet Cyberbeveiligingswet (Cbw), die verder is uitgewerkt in het Cyberbeveiligingsbesluit (Cbb). DORA is specifiek afgestemd op financiële instellingen, aangezien deze van toepassing is op organisaties die actief zijn in of diensten verlenen aan de financiële sector. Voor meer achtergrondinformatie over DORA kunt u de NOREA-publicatie over DORA raadplegen [2].

Hoewel de reikwijdte en focus verschillen, hebben beide wetgevingen hetzelfde doel: het versterken van de cyberbeveiliging en operationele weerbaarheid om de stabiliteit en integriteit van kritieke sectoren binnen de EU te waarborgen. Het belangrijkste is dat beide wetgevingen voorschrijven dat het management een actieve, persoonlijke rol moet spelen in cyberbeveiliging. Dit betekent dat managers nu een fundamenteel begrip moeten hebben van de principes en best practices op het gebied van cyberbeveiliging.

Ons doel is om duidelijke richtlijnen te bieden over wat deze eisen inhouden, zodat organisaties deze wetten effectief kunnen implementeren en hun verantwoordelijkheden vanuit een eensgezind perspectief kunnen nakomen.

2. Scope van de training voor bestuursleden

Hoewel sommige artikelen van DORA en NIS2 zeer gedetailleerd zijn, blijven andere vaag. In combinatie met het feit dat beide regelgevingen gebaseerd zijn op risico en proportionaliteit, hebben instellingen moeite om de diepte en reikwijdte van bepaalde vereisten te bepalen. In dit document presenteren we een richtlijn voor de training van de raad van bestuur, ofwel de training van het "managementorgaan" (conform DORA) of "managementorganen van de essentiële of belangrijke entiteiten" (conform NIS2).

DORA definieert, via aanvullende wetgeving en richtlijnen, het managementorgaan als de raad van toezicht en de raad van commissarissen. NIS2 geeft geen expliciete definitie van wat onder het bestuursorgaan van essentiële of belangrijke entiteiten wordt verstaan (dit is gedaan om rekening te houden met de uiteenlopende organisatiestructuren binnen de

[1] Kredietinstellingen en financiële marktinfrastructuren, exploitanten van handelsplatformen en centrale tegenpartijen (CCP's)

[2] https://www.norea.nl/uploads/bfile/52ee1e0f-54ae-4157-9a43-524c746c2ff1

EU), maar algemeen wordt aangenomen dat deze definitie verwijst naar het bestuurs- en leidinggevend team van de organisatie.

De basis voor de opleiding van bestuursleden, inclusief hun verantwoordelijkheid voor de scholing van personeel, van organisaties vindt zijn oorsprong in de artikelen 5.4 en 13.6 van de DORA. Artikel 5.4 vereist dat *"leden van het managementorgaan van de financiële instelling actief hun kennis en vaardigheden op peil houden om ICT-risico's en de impact daarvan op de bedrijfsvoering van de financiële instelling te begrijpen en te beoordelen, onder meer door regelmatig specifieke trainingen te volgen die aansluiten bij het beheerde ICT-risico."* Daarnaast vereist artikel 13.6 dat *"financiële instellingen programma's voor bewustwording van ICT-beveiliging en trainingen in digitale operationele weerbaarheid ontwikkelen als verplichte modules in hun personeelsopleidingen. Deze programma's en trainingen zijn van toepassing op alle werknemers en het hoger management en hebben een complexiteitsniveau dat aansluit bij hun takenpakket. Waar nodig betrekken financiële instellingen ook externe ICT-dienstverleners bij hun relevante opleidingen overeenkomstig artikel 30(2), punt (i)."*

In artikel 5.4 hierboven wordt verwezen naar ICT-risico. ICT-risico wordt in artikel 3(5) gedefinieerd als: " *elke redelijkerwijs identificeerbare omstandigheid met betrekking tot het gebruik van netwerk- en informatiesystemen die, indien zich die voordoet, de veiligheid van de netwerk- en informatiesystemen, van elk technologieafhankelijk instrument of proces, van activiteiten en processen, of van de dienstverlening in gevaar kan brengen door nadelige gevolgen te veroorzaken in de digitale of fysieke omgeving.* "

In NIS2 wordt in artikel 20.2 verwezen naar de opleiding van de bestuursorganen: " *De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten verplicht zijn een opleiding te volgen en moedigen essentiële en belangrijke entiteiten aan om hun werknemers regelmatig soortgelijke opleidingen aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en de praktijken voor het beheer van cyberbeveiligingsrisico's en de impact daarvan op de door de entiteit verleende diensten te kunnen beoordelen.* "

De eisen die voortvloeien uit de hierboven beschreven artikelen zijn duidelijk. DORA en NIS2 vereisen dat organisaties ervoor zorgen dat hun managementorgaan voldoende is opgeleid op het gebied van cyberbeveiliging in het algemeen, en goed op de hoogte is van de ICT-omgeving van hun organisatie in het bijzonder. Dit brengt een aanzienlijke kennisvereiste met zich mee, waarvoor de bestuursleden zelf direct verantwoordelijk zijn.

3. Waarom zou er training moeten plaatsvinden?

Er moet training worden gegeven om het managementorgaan in staat te stellen risico's te beheersen, weloverwogen beslissingen te nemen en de weerbaarheid van de organisatie tegen ICT-incidenten te waarborgen.

De training moet zich richten op en afgestemd zijn op het begrijpen van de specifieke ICT-risico's waarmee de organisatie te maken kan krijgen. De training moet regelmatig worden herhaald en aangepast om gelijke tred te houden met de snelle ontwikkeling van digitale dreigingen en regelgeving. De trainingen moeten daarom flexibel zijn (afhankelijk

van de aard en behoeften van de organisatie), wat betekent dat de inhoud van de trainingen periodiek kan variëren. Dit kan variëren van inzicht in cyberdreigingen tot het effectief inzetten van technologische oplossingen voor risicobeheer en -respons. De training moet ook scenario's en best practices omvatten om voorbereid te zijn op gebeurtenissen zoals digitale verstoringen of cyberdreigingen.

Als onderdeel van de training moet het managementorgaan ook inzicht hebben in de belangrijkste elementen van digitale operationele veerkracht. De focus moet liggen op het vermogen van de organisatie om verstoringen te weerstaan en kritieke activiteiten te blijven uitvoeren tijdens en na een groot ICT-incident. De training moet zich bovendien richten op risicopreventie en -beheer in plaats van op reactie na een incident.

Een bijkomend doel van de training voor het managementorgaan is ervoor te zorgen dat het raamwerk voor ICT-risicomanagement en de bijbehorende risico's worden begrepen. Dit betreft niet alleen inzicht in interne risico's, maar ook in externe bedreigingen die de organisatie kunnen beïnvloeden.

4. Soorten training

De in hoofdstuk 2 aangehaalde artikelen vermelden dat de leden van het managementorgaan actief hun kennis moeten blijven bijwerken. Dit impliceert dat de training geen eenmalige of louter initiële training kan zijn. Er kan daarom onderscheid worden gemaakt tussen twee soorten training:

- Initiële training: gericht op het overdragen van kennis en het vergroten van inzicht in de belangrijkste aspecten van digitale weerbaarheid. Deze training is met name belangrijk tijdens de implementatiefasen van DORA en NIS2 en tijdens managementwisselingen, wanneer een gedegen basiskennis essentieel is. Voor deze initiële training raden we aan alle 8 domeinen van het trainingsschema uit hoofdstuk 8 te behandelen.
- Terugkerende training: gericht op het waarborgen dat het kennisniveau van het management actueel blijft. Voor terugkerende trainingen adviseren wij om de domeinen van het trainingsschema in hoofdstuk 8 te selecteren die (aanzienlijke) veranderingen binnen de instelling hebben ondergaan, gekoppeld zijn aan de grootste risico’s en/of negatieve impact kunnen hebben op de organisatie.

5. Vorm en frequentie van de training

De training kan verschillende vormen aannemen, zoals:

- Intern, bij voorkeur tijdens een reguliere bestuursvergadering
- Groepstraining
- Discussie (bijvoorbeeld dilemma-discussies)
- E-learning
- Crisisoefening (simulatie en/of tabletop)
- Evaluaties van grote incidenten

Afhankelijk van het risico, de omvang van de organisatie, de volwassenheid en de dreigingsniveaus kan de frequentie van de trainingen verschillen (zie ook hoofdstuk 4).

Instellingen kunnen er ook voor kiezen om Permanente Educatie trainingen te gebruiken als aanvulling op of in plaats van sommige thema's.

6. Specifieke NIS2-vereisten voor Nederland

In Nederland is NIS2 geïmplementeerd via de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb), die een aantal aanvullende eisen bevatten bovenop de reeds door NIS2 voorgeschreven eisen.

Het Cbb bevat specifieke eisen met betrekking tot:

- Het doel: Artikel 21 stelt dat het doel van de training is om bestuursleden van essentiële en belangrijke entiteiten te voorzien van de kennis en vaardigheden om risico's voor de beveiliging van netwerk- en informatiesystemen te identificeren, de impact ervan op de geleverde diensten te beoordelen en maatregelen voor cyberbeveiligingsrisicobeheer en de gevolgen daarvan voor die diensten te evalueren.
- Vereisten voor de training: Artikel 22 stelt dat de training bestuursleden in staat moet stellen risico's voor netwerk- en informatiesystemen te identificeren en te beoordelen, met inbegrip van:
    - soorten risico's,
    - risicobeheerprocessen en
    - methoden voor risicobeoordeling.

  Daarnaast inzicht verkrijgen in en de beoordeling uitvoeren van maatregelen voor het beheer van cyberbeveiligingsrisico's, waarbij aandacht wordt besteed aan de onderwerpen genoemd in artikel 21(3)(a-j) van de wet (zoals beleid, incidentafhandeling, bedrijfscontinuïteit, beveiliging van de toeleveringsketen en het gebruik van cryptografie).
- Certificering: Artikel 23 benadrukt dat de training moet worden afgesloten met een certificaat van deelname. Het certificaat moet ten minste het volgende bevatten:
    a) de naam van het bestuurslid van de essentiële entiteit of belangrijke entiteit;
    b) de data waarop de training werd gevolgd;
    c) de onderwerpen die tijdens de training aan bod zijn gekomen; en
    d) de naam van de opleidingsaanbieder.

7. Inleiding tot de kennisdoelstellingen voor het managementorgaan

Hoewel het niet nieuw is dat de raad van bestuur uiteindelijk verantwoordelijk en aansprakelijk is voor alle beveiligingsactiviteiten, is persoonlijke aansprakelijkheid dat wel. Over het algemeen is de reflex van de raad van bestuur om taken te delegeren en anderen opdrachten te geven. Zij worden verantwoordelijk voor de uitvoering van specifieke taken, terwijl de raad van bestuur zich voornamelijk richt op strategisch toezicht. Wat cybersecurity betreft, delegeert de raad van bestuur de

verantwoordelijkheid vaak aan de CIO en CISO. Door de veranderde eisen moet de raad van bestuur nu echter direct betrokken zijn bij het sturen en nemen van beslissingen met betrekking tot cybersecurity.

De specifieke verantwoordelijkheden van de raad van bestuur hangen af van vele factoren, maar zowel DORA als NIS2 hebben bepaalde minimumeisen vastgelegd.

Voor de NIS2 gelden de volgende eisen:

- De bestuursorganen keuren de maatregelen voor het beheer van cyberbeveiligingsrisico's goed.
- De bestuursorganen houden toezicht op de implementatie van de cyberbeveiligingsrisicobeheersingsmaatregelen.

Onder DORA gelden de volgende vereisten:

- Het bestuursorgaan draagt de eindverantwoordelijkheid voor het effectief beheersen van alle ICT-risico's van de financiële entiteit,
- Het bestuursorgaan stelt de strategie voor digitale operationele weerbaarheid vast en keurt deze goed en actualiseert deze periodiek indien nodig,
- Het bestuursorgaan herziet en keurt periodiek (bijv. jaarlijks) het ICT-bedrijfscontinuïteitsbeleid en de ICT-respons- en herstelplannen goed,
- Het bestuursorgaan herziet en keurt periodiek (bijv. jaarlijks) interne ICT-auditplannen, ICT-audits en materiële wijzigingen van de audits goed,
- Het bestuursorgaan herziet en keurt periodiek (bijv. jaarlijks) het beheerbeleid voor ICT-derden dienstverleners goed.

De persoonlijke betrokkenheid van de directie is cruciaal voor het bevorderen en uitdragen van een sterke veiligheidscultuur. Op basis van ervaring en geïnspireerd door de Nederlandse Corporate Governance Code [3], omvatten typische cyberactiviteiten voor de directie onder meer:

- Het opzetten van duidelijke governance en rapportage voor cyberbeveiliging.
- Het identificeren en definiëren van kritieke functies en activa die bescherming behoeven,
- Het bepalen van de risicobereidheid van de organisatie op het gebied van cyberbeveiliging.
- Het toewijzen van voldoende budgetten en middelen om geïdentificeerde risico's aan te pakken en naleving van wettelijke voorschriften te waarborgen.
- Het afstemmen van cybersecurity prioriteiten op de algemene bedrijfsdoelstellingen en wettelijke verplichtingen.
- Het bevorderen van een cultuur van verantwoordelijkheid en veerkracht.

Zoals hierboven vermeld, hangt de precieze rol van de directie af van vele factoren en kan deze variëren afhankelijk van de behoeften van de organisatie. In de onderstaande tabel vindt u een overzicht van alle kennis- en verantwoordelijkheidsdoelstellingen voor een

[3] https://www.mccg.nl/documenten/2025/03/corporate-governance-code-2025

organisatie. Deze tabel kan dienen als inspiratiebron voor het afstemmen van de cybersecurity op het risicoprofiel en de risicoproportionaliteit van de organisatie .

In de tabel wordt onderscheid gemaakt tussen kennisdoelstellingen en verantwoordelijkheidsdoelstellingen. **Kennisdoelstellingen** richten zich op wat bestuursleden moeten begrijpen, zoals het kunnen bijdragen aan de definitie van de risicobereidheid of het begrijpen van het belang van een inventarisatie van activa. Deze kennis biedt hen het fundamentele inzicht dat nodig is om weloverwogen beslissingen te nemen. **Verantwoordelijkheidsdoelstellingen** daarentegen beschrijven de wettelijke en strategische plichten waaraan bestuursleden moeten voldoen, zoals het toezicht houden op risicomanagementkaders, het monitoren van compliance en het waarborgen van een degelijke en geteste bedrijfscontinuïteitsstrategie. Door deze twee categorieën te onderscheiden, kunnen organisaties de training van bestuursleden beter structureren en zorgen voor afstemming met wettelijke eisen en best practices voor cyberweerbaarheid. Dit onderscheid benadrukt tevens de dubbele rol van het bestuur als zowel lerende als leidende partij in het complexe digitale landschap van vandaag.

In hoofdstuk 8 presenteren we de kennis- en verantwoordelijkheidsdoelstellingen voor het bestuursorgaan aan de hand van de volgende structuur:

- Domein: Identificeert specifieke aandachtsgebieden die aandacht vereisen.
- Kennisdoelstellingen: Beschrijven de essentiële kennis die bestuursleden moeten begrijpen[4] met betrekking tot hun verantwoordelijkheden op het gebied van digitaal risicomanagement.
- Verantwoordelijkheidsdoelstellingen: Beschrijven de wettelijke en strategische plichten die bestuursleden moeten nakomen om te voldoen aan de regelgeving en om de bedrijfscontinuïteit te waarborgen.
- Praktische vragen voor een betere dialoog in de directiekamer: Bevat praktische vragen ter bevordering van discussies in de bestuurskamer, gebaseerd op het NCSC-factsheet en de CSR-richtlijn voor cyberbeveiliging voor bestuurders.

[4] Het woord "begrijpen" is gebaseerd op de taxonomie van Bloom; https://wij-leren.nl/taxonomie-van-bloom.php

8. De kennisdoelstellingen voor het bestuursorgaan

Domein	Kennisdoelstellingen	Verantwoordelijkheidsdoelstellingen	Praktische vragen voor een betere dialoog in de directiekamer, gebaseerd op het factsheet van de NCSC [5] en CSR.[6]
1. Bestuur en risicomanagement	• Begrijp de rollen, verantwoordelijkheden en aansprakelijkheid van de leden van het managementorgaan, inclusief de 3LoD. • Begrijp het ICT-risicomanagementkader van de organisatie en de risicocyclus (plannen, uitvoeren, controleren en handelen). • In staat zijn bij te dragen aan de definitie van de risicobereidheid en risicotolerantie van de organisatie. • Begrijp de cruciale functies van de organisatie en de mate waarin deze afhankelijk zijn van ICT-diensten. • Begrijp de verwachtingen van de strategie voor digitale operationele veerkracht (DORA-specifiek) of de IT-beveiligingsstrategie. • In staat zijn de belangrijkste beveiligingsrichtlijnen te begrijpen en goed te keuren.	• Voer de verantwoordelijkheid van het managementorgaan voor digitale weerbaarheid uit en actualiseer het ICT-risicokader door rekening te houden met de omgeving van de organisatie (bijvoorbeeld toegenomen dreigingen of geopolitieke ontwikkelingen). • Toezicht houden op de veerkracht van de meest kritieke ICT-systemen en het beperken van de cyberbeveiligingsrisico's van de organisatie binnen de vastgestelde risicobereidheid. • Het jaarplan voor de interne audit begrijpen en goedkeuren, met name de prioritering en de toegevoegde waarde van de audits in relatie tot de belangrijkste IT-risico's. • Toezicht houden op de naleving van wettelijke cyberbeveiligingsvoorschriften (specifiek voor DORA en NIS2) of de IT-beveiligingsstrategie.	NCSC: • Wat zijn de meest dringende kwesties waar ik me op moet richten? • Wat moet ik doen om ervoor te zorgen dat het management voldoende mensen en middelen inzet om de doelstellingen te bereiken? • Welk mechanisme is er binnen de organisatie aanwezig om de cybersecuritystrategie te waarborgen en de goedkeuring van beleid inzake risicobeheer door het management te garanderen? • Hoe vaak staat cyberbeveiliging op de agenda om ervoor te zorgen dat er voldoende vooruitgang wordt geboekt op dit gebied? • Wat is de rol en taak van de CISO wanneer hij of zij deelneemt aan bestuursvergaderingen? • Wat moet ik als bestuurslid weten om voldoende inzicht te krijgen in de cyberbeveiligingsrisico's van deze organisatie? • Worden er risicoanalyses uitgevoerd, en zo ja, wat zijn de belangrijkste aandachtspunten en uitkomsten daarvan? • Wat zijn onze grootste risico's en bedreigingen en hebben we daar voldoende controle over?

[5] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/vragen-voor-bestuurder-aan-ciso
[6] https://www.cybersecuritycouncil.nl/documents/2025/08/14/guide-to-cyber-security-for-directors-and-business-owners

Domein	Kennisdoelstellingen	Verantwoordelijkheidsdoelstellingen	Praktische vragen voor een betere dialoog in de directiekamer, gebaseerd op het factsheet van de NCSC [5]en CSR.[6]
	• Begrijp de noodzaak van transparante cyberrapportage aan en actief toezicht door het managementorgaan.		• Zijn onze risico's incidenteel of structureel? • Hoe bepalen en berekenen we de waarschijnlijkheid en de impact, en hoe onderscheiden we de verschillende soorten risico's? Welke rol speel ik daarin? • Welke resterende risico's zijn er? Zijn deze aanvaardbaar? • Zijn de resterende risico's besproken met de toezichthoudende autoriteiten? • Hebben we als organisatie een cybersecuritystrategie? Zo ja, hoe ziet die eruit?
2. Operationeel management	• Begrijp het belang van IT-activaclassificatie en inventarisatie. • Begrijp de belangrijkste principes van veerkrachtige systemen.	• Geef richting aan verbeteringsacties, prioriteiten en tijdlijnen voor belangrijke activa en processen.	NCSC: • Wat zijn onze belangrijkste applicaties en processen? CSR: • Hebben we een volledige inventarisatie van onze ICT-systemen? Hebben we *shadow* en/of *legacy* systemen? Voorgestelde aanvullende vraag: • Hoe kunnen we lacunes in belangrijke controlemechanismen opsporen?
3. Continuïteitsbeheer	• Begrijp het bedrijfscontinuïteitsbeleid en de respons- en herstelplannen. • Begrijp het mediabeheer, de crisisorganisatie en het communicatieplan. • Begrijp de rol van het management bij het nemen van snelle beslissingen tijdens ernstige aanvallen of verstoringen. • Begrijp de verschillende soorten back-up- en herstelstrategieën.	• Ken de maatregelen voor de veerkracht van kritieke functies onder druk of verstoringen en evalueer deze periodiek. • Rentmeesterschap in NO-IT scenario's en het vermogen om overeengekomen maatregelen en verantwoordelijkheden uit te voeren. • Oefen diverse crisisscenario's of cyberoefeningen (tabletop, walkthroughs, simulatiespellen).	NCSC: • Stel dat er onverwacht iets misgaat, hebben we dan een noodplan (back-up-/redundantiesystemen) en een incidentresponsplan? Zo ja, hoe zien die eruit?

Domein	Kennisdoelstellingen	Verantwoordelijkheidsdoelstellingen	Praktische vragen voor een betere dialoog in de directiekamer, gebaseerd op het factsheet van de NCSC [5]en CSR.[6]
4. Incidentmanagement	• Begrijp de belangrijkste aspecten van het incidentbeheerbeleid en de escalatieprocedures. • Inzicht in de classificatie en rapportage van incidenten. • Ken de belangrijkste belanghebbenden en hun rollen in geval van een groot incident.	• Houd de specifieke tijdlijnen voor het melden van grote incidenten volgens DORA en NIS2 in de gaten (indien van toepassing ook de SEC – Securities and Exchange Commission). • Weet hoe u ernstige incidenten moet melden aan de toezichthoudende autoriteiten in de verschillende regio's.	CSR: • Hebben we een plan voor incidentbestrijding? • Zijn wij als bedrijf en als raad van bestuur (voldoende) verzekerd tegen cyberrisico's? Voorgestelde aanvullende vraag: Hebben we een overzicht van de gemelde grote incidenten en de huidige status van de benodigde verbeteringen?
5. Software- en systeemontwikkeling	• Begrijp de belangrijkste aspecten van het beleid inzake de aanschaf, ontwikkeling en het onderhoud van software en systemen.	• Begrijp de meest cruciale aspecten van de aanschaf, ontwikkeling en het onderhoud van software en systemen. • Begrijp de belangrijkste aspecten met betrekking tot het testen van systemen. • Inzicht in de prestaties van de vereiste testen.	Niet van toepassing
6. Risicobeheer met betrekking tot derden	• Begrijp het proces van risicobeheer met betrekking tot derden, inclusief leveranciersbeheer, en begrijp dat risico's van derden moeten worden beheerd als een integraal onderdeel van ICT-risico's en het raamwerk voor ICT-risicobeheer. • Begrijp de belangrijkste contractuele afspraken, zoals bijvoorbeeld de exitstrategie, onbeperkte toegangsrechten, inspectie- en auditregelingen, en de kennisgevingstermijnen en rapportageverplichtingen van de TPP (third-party provider).	• Ken de cruciale externe leveranciers van de instelling en houd toezicht op hun periodieke evaluatie om te bepalen of de strategie nog steeds aansluit bij de behoeften van de organisatie. • Inzicht in de impact van veranderingen in de keten van cruciale onderaannemers. • Inzicht verkrijgen in de mate waarin de kritieke externe leveranciers van de instelling voldoen aan de vereiste beveiligings- en contractuele verplichtingen (bijv. exitplan). • Inzicht hebben in de betrokkenheid van de cruciale externe leveranciers van de instelling bij continuïteitstests,	NCSC: • Welke externe partijen maken we gebruik van? CSR: • Kennen we de afhankelijkheden van ICT-leveranciers en beheersen we de daaraan verbonden risico's? Voorgestelde aanvullende vraag: • Op welke ICT-dienstverleners vertrouwen we voor onze kritieke processen/functies? • Welke alternatieven zijn er voor onze meest cruciale ICT-dienstverleners?

Domein	Kennisdoelstellingen	Verantwoordelijkheidsdoelstellingen	Praktische vragen voor een betere dialoog in de directiekamer, gebaseerd op het factsheet van de NCSC [5]en CSR.[6]
	• Verwachtingen van het informatieregister (specifiek voor DORA) • Inzicht in de risicomanagementaspecten in de context van kritieke outsourcing, zoals due diligence, leveranciersbeoordelingen, de impact van veranderingen en monitoring van de interne controle en prestaties van de keten van ICT-dienstverleners, het voorkomen van vendor lock-in en strategische autonomie.	veerkrachttests (TLPT in DORA), security awareness campagnes, enz.	
7. Testen van de veerkracht	• Begrijp het doel van de verschillende soorten digitale operationele veerkrachttesten, zoals Red Teaming en TLPT (specifiek voor DORA).	• Begrijp het testprogramma voor de veerkracht van digitale operaties van de instelling en weet dat het programma de gehele kritieke (ICT) omgeving moet omvatten. • Indien TLPT van toepassing is, moeten de resultaten en de in de test geconstateerde verbeteringen worden gemonitord.	CSR: • Voeren we veerkrachtstests uit? Voorgestelde aanvullende vraag: • Hoe zijn wij betrokken bij de voorbereiding en evaluatie van veerkrachttesten?
8. Beveiligingsbeheer	• Begrijp de belangrijkste beheersmaatregelen (zie een voorbeeldlijst in hoofdstuk 5 van de richtlijn van de Cyber Security Raad [7]).	• Zorg ervoor dat de rollen en verantwoordelijkheden binnen de beveiliging duidelijk zijn en worden nageleefd, inclusief de juiste rapportagelijnen. • Toezicht houden op de implementatiestatus en de dekking van	NCSC: • In hoeverre heerst er een positieve veiligheidscultuur binnen de organisatie? • Welk kennisniveau wordt er binnen de rest van de organisatie vereist? • In hoeverre is scholing en training noodzakelijk voor de organisatie?

[7] https://www.cybersecuritycouncil.nl/documents/2025/08/14/guide-to-cyber-security-for-directors-and-business-owners

Domein	Kennisdoelstellingen	Verantwoordelijkheidsdoelstellingen	Praktische vragen voor een betere dialoog in de directiekamer, gebaseerd op het factsheet van de NCSC [5]en CSR.[6]
	• Inzicht hebben in de meest relevante aanvalsvectoren binnen het domein van de instelling. • Kennis hebben van de verschillende soorten risico's die verbonden zijn aan netwerk- en informatiesystemen, zoals de dreiging van malware, interne dreigingen en DDoS-aanvallen die een risico vormen voor de integriteit en beschikbaarheid (specifiek voor NIS2). • Inzicht hebben in het cyberdreigingsprofiel van de instelling en de mogelijke impact van cyberaanvallen op de organisatie. • Heb inzicht in belangrijke sociale manipulatietechnieken, zoals spoofing, phishing, het infiltreren van subversieve individuen in organisaties en interpersoonlijke manipulaties, en qishing .	de meest cruciale beveiligingsmaatregelen van de instellingen. • Zorg zelf voor een goede cyberhygiëne, geef het goede voorbeeld door het beleid van de organisatie na te leven en zorg ervoor dat het management het belang van cyberveiligheid benadrukt (tone at the top).	• Welke maatregelen hebben we genomen om onze belangrijkste activa te beschermen? • Wat is de status van deze maatregelen en welke maatregelen moeten nog worden genomen om een aanvaardbaar niveau van veerkracht te bereiken? • Welke maatregelen nemen we niet en waarom nemen we deze maatregelen niet? • Wie is verantwoordelijk voor de genomen maatregelen? • Is er een overzicht van de maatregelen die zijn genomen om de systemen (inclusief hun fysieke omgeving) en gegevens van de organisatie te beschermen? • Hoe controleren we de implementatie/naleving van de overeengekomen maatregelen? • Wat moet er gebeuren om de huidige tekortkomingen aan te pakken en wat verwacht u als CISO van mij? CSR: • Welke systemen zijn zo belangrijk dat we de toegang moeten beperken? • Hoe belangrijk is cyberbeveiliging voor onze producten en onze klanten? Of zelfs voor de maatschappij? • Hoe verhoudt onze cyberbeveiliging zich met de sector?

9. Conclusie

In essentie schrijven de Digital Operational Resilience Act (DORA) en de Network and Information Security Directive (NIS2) gezamenlijk niet alleen de implementatie van robuuste risicomanagementkaders voor, maar ook de bevordering van een cultuur van continu leren en bewustwording op alle niveaus binnen een organisatie. Terwijl DORA zich richt op het versterken van de digitale weerbaarheid van financiële instellingen, breidt NIS2 deze eis uit naar organisaties in kritieke sectoren, waarbij de nadruk ligt op een uniforme aanpak van cybersecurity. Beide kaders benadrukken de dubbele rol van het bestuursorgaan, waarbij zowel kennisdoelstellingen als verantwoordelijkheidsdoelstellingen moeten worden nagestreefd. Kennisdoelstellingen richten zich op het voorzien van leiders van het noodzakelijke inzicht in cyberrisico's, dreigingslandschappen en wettelijke vereisten, terwijl verantwoordelijkheidsdoelstellingen ervoor zorgen dat zij verantwoording afleggen voor de implementatie van governancekaders, het bevorderen van weerbaarheid en het afstemmen van cybersecurity-initiatieven op de organisatiestrategie.

Om aan deze wettelijke eisen te voldoen, moet het bestuursorgaan verder gaan dan traditionele toezichtsrollen en een actieve rol spelen in het bevorderen van veerkracht. Dit houdt in dat hun competenties continu worden uitgebreid en bijgewerkt om bedreigingen effectief te identificeren, te beoordelen en te beperken, en zo hun verplichtingen na te komen. Tegelijkertijd zijn ze verantwoordelijk voor het aansturen van de governanceprocessen en het bevorderen van een cultuur van digitale veerkracht, zodat hun organisaties voorbereid blijven op toekomstige uitdagingen. Door proactief aan deze doelstellingen te werken, wordt niet alleen aan de regelgeving voldaan, maar ook blijvende wendbaarheid en vertrouwen gewaarborgd bij het navigeren in een steeds dynamischer digitaal landschap.

Bovendien onderstreept de gedeelde nadruk op continu leren binnen zowel DORA als NIS2 het belang van het verankeren van cyberweerbaarheid in de organisatiecultuur. Door prioriteit te geven aan gestructureerde trainingsprogramma's kunnen instellingen een omgeving creëren waarin paraatheid tegen cyberdreigingen integraal onderdeel uitmaakt van de bedrijfsvoering, wat zowel individueel bewustzijn als collectieve verantwoordelijkheid bevordert. Deze dubbele focus op begrip en actie versterkt de weerbaarheid van de instelling en verbetert haar reputatie als leider in het verantwoord beheren van digitale risico's.

Uiteindelijk fungeren DORA en NIS2 als complementaire raamwerken, die zowel de richtlijnen als de wettelijke verplichting bieden voor bestuursorganen om het voortouw te nemen bij het bouwen van een veerkrachtigere toekomst. Door zowel kennis- als verantwoordelijkheidsdoelstellingen aan te pakken, kunnen organisaties niet alleen voldoen aan de verwachtingen, maar zich ook positioneren als proactieve leiders in het steeds meer onderling verbonden en risicovolle digitale landschap van vandaag.