NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Cyber Security Assessment & Inherente Cyber Risicoanalyse (NOREA CSA & ICR)

Introductie, handreiking en vragenlijst

Versie 4.0.1

Januari 2026

Handreiking Cyber Security Assessment & Inherente Cyber Risicoanalyse (NOREA CSA & ICR)

Deze methodische handreiking is uitgegeven door de NOREA, de beroepsorganisatie van IT-auditors in Nederland en mag vrijelijk worden gebruikt, mits met bronvermelding.

Voor vragen en opmerkingen kunt u zich wenden tot:

NOREA, de beroepsorganisatie van IT-auditors
Postbus 242, 2130 AE Hoofddorp
Telefoon: 0884960380
E-mail: norea@norea.nl
Meer informatie kunt u vinden op:
http://www.norea.nl

De CSA en ICR worden geëvalueerd en in de toekomst verbeterd. Het is de bedoeling de CSA en ICR op basis van ervaring en evaluatie als NOREA-handreiking (conform artikel 15 Reglement Beroepsuitoefening) vast te stellen.

Inhoud

Wat verstaat de NOREA onder Cyber Security? 8

Deel 1a: Introductie: over de ICR 9

- Wat is de ICR? 9
- Wat is het belang van een ICR? 10
- Hoe verhoudt de ICR zich tot andere informatiebeveiligings-instrumenten? 10
- Achtergrond van de ICR 10

Deel 1b: Introductie: Over de CSA 11

- Wat is een CSA? 11
- Wat levert een CSA op? 11
- Wanneer voert u een CSA uit? 12
- Hoeveel tijd kost het om een CSA uit te voeren? 12
- Andere (Cyber) Securityinstrumenten 12

Deel 2: Handreiking voor het ICR & CSA proces 15

- Wat zijn de stappen in een ICR & CSA proces? 15
- 1. Voer de Inherente Cyber Risicoanalyse (ICR) uit 16
- 1a. Vul de ICR vragenlijst in 16
- 1b. Behorende tot vitale aanbieders (AED of AAVA) 17
- 1c. Bepaal de ICR score 17
- 2. Voer de Cyber Security Assessment (CSA) uit 18
- 2a. Bepaal het team dat de CSA gaat uitvoeren en hoe dit moet gebeuren 18
- 2b. Verzamel en bestudeer relevante informatie 19
- 2c. Vul de CSA vragenlijst in 19

Deel 3: Acties o.b.v. ICR & CSA 21

- 3a. Schat de impact in en raadpleeg de relevante standaarden 22
- 3b. Stel het ICR & CSA verslag op 22
- 3c. Bespreek de ICR & CSA met het verantwoordelijke management 23

Bijlage 1: ICR vragenlijst 24

Bijlage 2: CSA vragenlijst 25

Voorwoord

Onze samenleving bevindt zich in een fase van exponentiële digitalisering, waarin IT een steeds crucialere rol speelt in vrijwel alle aspecten van ons leven en de samenwerking tussen organisaties. Deze ontwikkelingen bieden enorme kansen, maar vergroten tegelijkertijd onze afhankelijkheid van IT en de daarmee samenhangende cybersecurity risico's. Organisaties en overheden staan voor de uitdaging om deze risico's effectief te beheersen.

Om IT-auditors en andere professionals binnen het risicomanagement te ondersteunen bij het in kaart brengen en beheersen van deze risico's, heeft de NOREA (de beroepsorganisatie van IT-auditors in Nederland) de publiek beschikbare hulpmiddelen Cyber Security Assessment (CSA) en Inherente Cyber Risicoanalyse (ICR) ontwikkeld.

De Inherente Cyber Risicoanalyse (ICR) is gericht op het bepalen van het fundamentele risicoprofiel van een organisatie op het gebied van cybersecurity, uitgaande van de aard van de activiteiten en de omgeving waarin de organisatie opereert zonder rekening te houden met getroffen maatregelen.

De Cyber Security Assessment (CSA) richt zich vervolgens op het inzichtelijk maken van de risico's voor de organisatie, processen, systemen en gegevens en biedt handvatten voor het identificeren en mitigeren van deze risico's.

Dit document is bedoeld als handreiking die het volgende omvat:

- Introductie tot de ICR als de CSA (Deel 1a en 1b);
- Praktische handreiking voor het effectief uitvoeren van het ICR & CSA proces (Deel 2);
- Inzichten in mogelijke acties op basis van de resultaten (Deel 3);
- Verwijzing naar de bijbehorende vragenlijsten (Deel 4a en 4b).

Het doel van de ICR en de CSA is om op hoofdlijnen de risico's rondom cybersecurity te identificeren en te beoordelen en daarmee de beheersing van deze risico's binnen de risicomanagementcyclus te verbeteren om risico's tot een aanvaardbaar niveau terug te brengen.

De NOREA kennisgroep CyberSecurity is van mening dat de ICR & CSA een belangrijke bijdrage kunnen leveren aan de weerbaarheid van organisaties tegen cyberdreigingen. Wij nodigen u dan ook uit om uw ervaringen en suggesties voor verdere ontwikkeling met ons te delen, zodat we de NOREACSA & ICR continu kunnen verbeteren.

De NOREA kennisgroep CyberSecurity, januari 2026.

Versiebeheer

Versie	Datum	Aanpassing
1.1	Augustus 2015	Initieel document
2.0	April 2019	Invoeging Inherente Cyber Risicoanalyse (ICR)
2.2	Oktober 2020	Integratie CSA en ICR in één tabel, update referenties
3.0.2	Maart 2023	Update vragenlijst en handreiking: 1. De vragen zijn aangepast zowel voor de ICR (bepaling impact) als de CSA (bepaling beheersing). 2. De Excel tool bevat nu 7 standaarden zoals ISO27002, NIST CSF, COBIT en DNB GP IB. Diverse standaarden zijn bijgewerkt naar de nieuwste versie, oude en niet meer relevante standaarden zijn verwijderd. 3. Het toevoegen van een dashboard in de spreadsheet: 4. Diverse berekeningen voor het bepalen van de scores.
4.0.1	Januari 2026	Update vragenlijst en handreiking: 1. De vragen zijn aangepast zowel voor de ICR (bepaling impact) als de CSA (bepaling beheersing). 2. De Excel tool bevat nu 9 standaarden zoals NIS2, DORA, ISO27002, NIST CSF, COBIT en DNB GP IB. Diverse standaarden zijn bijgewerkt naar de nieuwste versie, oude en niet meer relevante standaarden zijn verwijderd. 3. Het updaten van het dashboard in de spreadsheet. 4. Diverse berekeningen voor het bepalen van de scores.

Leeswijzer

De CSA en ICR zijn primair bedoeld als middel voor IT-auditors in hun werkzaamheden voor directies en senior management van organisaties. Daarnaast kunnen ze gebruikt worden door andere professionals zoals de actoren binnen de risicomanagementcyclus, Internal/External Audit, securitymanagement en riskmanagement, ondersteund door een IT-auditor. Dit document bestaat uit de volgende delen:

Deel 1a: Introductie: over de ICR

In dit deel wordt ingegaan op de achtergrond en het belang van de ICR. U krijgt antwoord op vragen als: Wat is een ICR? Wat is het belang van een ICR? Hoe verhoudt de ICR zich tot andere informatie-beveiligingsinstrumenten?

Deel 1b: Introductie: over de CSA

In dit deel wordt ingegaan op de achtergrond en het belang van de CSA. U krijgt antwoord op vragen als: Wat is een CSA? Wat levert een CSA op? Wanneer voert u een CSA uit? Hoeveel tijd kost dat? Hoe verhoudt de CSA zich tot andere (Cyber) Security-instrumenten?

Deel 2: Handreiking voor het ICR & CSA proces

Dit deel bevat een handreiking voor het effectief en efficiënt uitvoeren van:

- De ICR. U krijgt antwoorden op vragen als: Uit welke stappen bestaat het ICR proces? Wie kan ik betrekken bij de ICR?
- De CSA. U krijgt antwoorden op vragen als: Uit welke stappen bestaat het CSA proces? Wie kan ik betrekken bij de CSA?

Deel 3: Acties o.b.v. ICR & CSA

Na de impactbepaling op basis van de ICR- en CSA-vragenlijsten heeft u antwoord op de vraag:

- Welke maatregelen kunnen worden overwogen om risico's te verkleinen of weg te nemen?

Deel 4a: ICR-vragenlijst

Na het doorlopen van de ICR-vragenlijst heeft u antwoord op de vraag:

- Wat is het inherente risicoprofiel van mijn organisatie op het gebied van cybersecurity?

Deel 4b: CSA-vragenlijst

Na het doorlopen van de CSA-vragenlijst heeft u antwoorden op de vragen:

- Wat zijn voor mijn organisatie de belangrijkste cyberrisico's van de verwerking en beheersing van gegevens?
- Hoe kan mijn organisatie deze risico's mitigeren (verkleinen of wegnemen)?

Wat verstaat de NOREA onder Cyber Security?

- Cybersecurity is een veelomvattend begrip. In de huidige samenleving communiceren organisaties en personen steeds meer via geautomatiseerde systemen die zijn aangesloten op het internet.
- Het belang van deze systemen wordt steeds groter, waardoor de impact bij misbruik ook toeneemt. Door de toename van bedreigingen neemt ook de kans op verstoringen toe. Daarom wordt cybersecurity steeds belangrijker.
- Wij hanteren voor de definitie van het begrip "Cybersecurity" de formulering van het NCSC, te weten: "Volgens het Nationaal Cyber Security Centrum (NCSC) (onderdeel van de NCTV) is cybersecurity het geheel aan beveiligingsmaatregelen om schade door verstoring, uitval of misbruik van informatiesystemen te voorkomen, en om, indien er toch schade is ontstaan, deze te beperken en te herstellen. Het omvat de hele digitale weerbaarheid en de risico's die daarbij komen kijken, met als doel de digitale veiligheid van Nederland te waarborgen." Cybersecurity is daarmee direct gelieerd aan begrippen als Cybercrime, Datalekken & Privacy, DDoS, Phishing en Hacking.
- Voor het begrip Cybercrime worden eveneens verschillende interpretaties gehanteerd. Wij hanteren in deze CSA voor dit begrip de brede definitie van het NCSC: "Het Nationaal Cyber Security Centrum (NCSC) definieert cybercrime als alle vormen van criminaliteit waarbij een ICT-systeem als middel of doelwit wordt gebruikt, zoals hacking, phishing en het verspreiden van malware, met als doel het stelen van gegevens, het afpersen van slachtoffers of het toebrengen van schade aan systemen."
- Daarnaast zien we dat naast techniek uiteraard ook organisatorische aspecten, ketenverantwoordelijkheden (inclusief outsourcing) en menselijk gedrag van belang zijn bij de beheersing van risico's rondom cybercrime. Dit blijkt uit de toename van wet- en regelgeving rondom het informatiebeveiligingsdomein en recente publicaties in de media.

Deel 1a: Introductie: over de ICR

In dit deel wordt ingegaan op de achtergrond en het belang van de ICR. U krijgt antwoord op vragen als: Wat is een ICR? Wat is het belang van een ICR? Hoe verhoudt de ICR zich tot andere informatie-beveiligingsinstrumenten?

Wat is de ICR?

ICR staat voor *Inherente Cyber Risicoanalyse*.

De Inherente Cyber Risicoanalyse (ICR) is gericht op het bepalen van het inherente risicoprofiel van een organisatie op het gebied van cybersecurity. Met andere woorden in welke mate loopt de organisatie een cybersecurity risico gezien de activiteiten en werkzaamheden die de organisatie uitvoert in de omgeving waarin de organisatie functioneert als er geen maatregelen voor worden getroffen. Een ICR is daardoor primair gericht op de omgeving van de organisatie en externe dreigingen die hierin een rol spelen, met uiteraard als startpunt (het karakter van) de werkzaamheden die de organisatie uitvoert. De ICR omvat de volgende categorieën:

1. Algemeen
2. Organisatie karakteristieken
3. Technologie & derde partijen
4. Online aangeboden producten of diensten
5. Externe cyberdreigingen

Als voorbeeld: een organisatie, die via het Internet onlinediensten aanbiedt zoals het verkopen van goederen, heeft een hoger inherent risicoprofiel op cybergebied dan een organisatie die via traditionele kanalen zoals fysieke winkels haar diensten aanbiedt. Een hoog inherent risico betekent veelal dat de organisatie voldoende maatregelen moet treffen om de beheersing op een acceptabel niveau te krijgen en te houden. Zonder deze maatregelen kan de organisatie financiële- en imagoschade oplopen.

De Cyber Security Assessment (CSA – zie verder deel 1b.) richt zich vervolgens op het toetsen van deze maatregelen die een organisatie kan nemen om de weerbaarheid binnen die omgeving te verhogen. De urgentie en inhoud van mogelijke vervolgstappen kan hierdoor alleen bepaald worden o.b.v. een gezamenlijke weging van de uitkomsten van zowel een ICR als CSA. De uitkomsten van de ICR zijn input voor de CSA.

De ICR wordt uitgedrukt in een classificatie “laag” / “midden” / “hoog”. De ICR bepaalt daarmee:

- primair de urgentie waarmee vervolgens een CSA uitgevoerd moet worden en;

- secundair het gewicht / de prioriteit die gegeven moet worden aan het uitvoeren van de aanbevelingen die uit een CSA naar voren komen.

Wat is het belang van een ICR?

Het belang van de ICR is het bepalen van het vertrekpunt voor de treffen maatregelen op het gebied van cybersecurity risico's. Aan de hand van 32 vragen verdeeld over de hierboven genoemde categorieën, kan het inherente risicoprofiel bepaald worden op het gebied van cybersecurity. Dit profiel draagt bij aan het prioriteren van verbeteracties die voortkomen uit de CSA.

Hoe verhoudt de ICR zich tot andere informatiebeveiligings-instrumenten?

Dit model kan goed gebruikt worden in combinatie met het volwassenheidsmodel van NBA/LIO (zie Volwassen Informatiebeveiliging (nba.nl) om vanuit cybersecurity perspectief invulling te geven aan het inherente cybersecurity risico binnen de bredere informatiebeveiligingscontext.

Figuur 1: Verhouding volwassenheidsmodel van NBA/LIO en ICR&CSA NOREA

Achtergrond van de ICR

De tool is door NOREA gebruikt als uitgangspunt voor de ICR en verder aangepast voor de Nederlandse situatie en ook geschikt gemaakt voor andere sectoren.

Deel 1b: Introductie: Over de CSA

In dit deel wordt ingegaan op de achtergrond en het belang van de CSA. U krijgt antwoord op vragen als: Wat is een CSA? Wat levert een CSA op? Wanneer voert u een CSA uit? Hoeveel tijd kost dat? Hoe verhoudt de CSA zich tot andere (Cyber) Securityinstrumenten?

Wat is een CSA?

CSA staat voor *Cyber Security Assessment*. De CSA legt in de eerste plaats mogelijke risico's bloot van een organisatie, processen, systemen en gegevens die raakvlakken hebben met cybersecurity. Daarmee draagt zij bij aan het vermijden of mitigeren van deze *cybersecurity* risico's. De CSA kan als zelfstandig *assessment* worden uitgevoerd of als onderdeel van bijvoorbeeld een algemene dreigingen- of impactanalyse. De CSA ondersteunt hiermee een *top-down* benadering om vanuit risico's in het bedrijfsproces te komen tot technische en organisatorische maatregelen.

Op basis van de antwoorden van de CSA wordt op gestructureerde wijze inzichtelijk gemaakt of er een kans is dat de organisatie, processen, systemen en gegevens kunnen worden geschaad door een cybercrime aanval en op welke gebieden.

De CSA doet dit door op gestructureerde wijze de risico's voor de betrokken organisaties, processen, systemen en gegevens zo veel mogelijk te identificeren. Op basis van de uitkomsten van de CSA kunt u gericht acties ondernemen om deze risico's nader te identificeren en te mitigeren. De CSA biedt een oplossingsrichting door te verwijzen naar bestaande *frameworks* die hierbij kunnen helpen.

De CSA is de door NOREA aanbevolen handreiking voor de IT-auditor om organisaties te helpen om de *cybersecurity* risico's inzichtelijk te maken. Dit kan bijvoorbeeld in de vorm van een adviesopdracht. Daardoor kan de CSA bescherming van organisaties, processen, systemen en gegevens op een gestructureerde manier ondersteunen. Hiermee is het een essentieel onderdeel van de belangenafweging en besluitvorming over de informatiebeveiligingsstrategie. Dit levert een wezenlijke bijdrage aan de weerbaarheid van een organisatie tegen cybercrime.

De CSA kan gebruikt worden door alle typen organisaties. Echter, de CSA is vooral zinvol voor organisaties die voor hun bedrijfsvoering in hoge mate afhankelijk zijn van online dienstverlening via het internet.

Wat levert een CSA op?

De CSA kent een aantal belangrijke doelen:

1. Het verhogen van het *security* bewustzijn binnen een organisatie.
2. Het verstevigen van het vertrouwen van de klanten, investeerders, werknemers of burgers in de wijze waarop vertrouwelijke gegevens worden verwerkt.

3. Het verbeteren van de communicatie over security en de bescherming van vertrouwelijke gegevens.

Wanneer voert u een CSA uit?

In ieder geval éénmaal per jaar voor het te beoordelen object zoals een organisatie of een specifiek project. Een CSA kan het beste in een zeer vroeg stadium van een project uitgevoerd worden. Immers, als u de CSA in een vroeg stadium uitvoert, helpt de CSA u om het belang van *cybersecurity* mee te nemen bij het verdere ontwerp van een systeem (security by design). Ook aanpassingen of wijzigingen van bestaande systemen rechtvaardigen het uitvoeren van een CSA. Op die manier kunt u voorkomen dat later kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot *cybersecurity* te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de CSA te herhalen en/of te evalueren bij de afsluiting van een project.

Hoeveel tijd kost het om een CSA uit te voeren?

Er zijn verschillende factoren van invloed op de tijd die het kost om een CSA uit te voeren. De belangrijkste zijn:

- het aantal belanghebbenden bij het te beoordelen object en de mate waarin deze vragen of twijfels hebben over de consequenties voor *cybersecurity*;
- de impact en het belang van het object op de organisatie en de samenleving;
- de (technische en organisatorische) complexiteit van de processen, systemen en gegevensverwerkingen.

De hoeveelheid tijd en doorlooptijd die het uitvoeren van een CSA kost, zal per geval verschillen en hangt van verschillende factoren af. Het uitvoeren van de gehele CSA voor een eenvoudige gegevensverwerking zal enkele dagdelen kosten, dit is inclusief het verzamelen van gegevens en het uitvoeren van een controle.

Andere (Cyber) Securityinstrumenten

Voor het opstellen en ontwikkelen van de CSA hebben we gebruik gemaakt van een aantal algemeen erkende frameworks en standaarden, namelijk:

Framework/standaard	Versie
National Institute of Standards and Technology (NIST)/Cyber Security Framework (CSF)	Version 2.0

International Standards Organisation (ISO)/International Electrotechnical Commission (IEC)	ISO27002:2022-03 Information Security, cybersecurity and privacy protection - Information security controls
Information Systems Audit and Control Association (ISACA)	COBIT 2019
De Nederlandsche Bank (DNB)	Good practice IB/Cyber - 58 controls 2023
Payment Card Industry (PCI)/Data Security Standard (DDS)	V4.01
Critical Security Controls (CIS)	V8.1 June, 2024
Cloud Security Alliance (CSA)/Cloud Controls Matrix (CMM)	V4.0.10
Network and Information Security Directive (NIS2)	V2, 10 oktober 2024
Digital Operational Resilience Act (DORA)	V1, 17 januari 2025
IIA Cybersecurity Topical Requirement	5 February 2025

Toepasbaarheid van bovenstaande standaarden hangt sterk af van de omgeving en het gekozen object. Deze standaarden zijn gericht op cybersecurity dat bijdraagt aan het grotere, overkoepelende doel van informatiebeveiliging.

Het uitgangspunt van onze aanpak is dat de NOREA u helpt de risico's in kaart te brengen en aangeeft in welke van deze bovenstaande normen aanknopingspunten zijn opgenomen voor verdere verbetering van de beheersing.

Wij hebben op basis van onze ervaringen de volgende categorieën geïdentificeerd die relevant zijn voor informatiebeveiliging:

1. Organisatie & Governance.
2. Gedrag & Cultuur.
3. Waardeketen (stakeholders) versus risico's.
4. Inzicht in het technologie landschap (software, middleware, hardware).

5. Wet- & regelgeving.
6. Detectie.

- Reactie en herstel.

Met behulp van standaarden en normenkaders hebben wij deze categorieën eenduidig benoemd. Op basis van onderzoek hebben we vervolgens bepaald in welke mate de standaarden en normenkaders aandacht besteden aan de verschillende categorieën. De kennisgroep heeft de ambitie om de CSA uit te breiden met aangepaste, andere en nieuwe standaarden op het gebied van cybersecurity. Voorliggende versie 4 is hiervan een uitwerking.

Deel 2: Handreiking voor het ICR & CSA proces

Dit deel bevat een handreiking voor het effectief en efficiënt uitvoeren van een ICR/CSA. Afhankelijk van de omstandigheden waarin de ICR/CSA wordt uitgevoerd kan op het onderstaande stappenplan worden gevarieerd. U krijgt antwoorden op vragen als: Uit welke stappen bestaat het ICR/CSA proces? Wie kan ik betrekken bij de ICR/CSA?

Wat zijn de stappen in een ICR & CSA proces?

De uitvoering van het ICR & CSA proces is in onderstaande figuur weergegeven en bestaat uit de volgende stappen:

Te nemen acties o.b.v. ICR & CSA:

	ICR Laag (>66)	ICR Midden (45-66)	ICR Hoog (<45)
CSA Groen	Geen actie	Actie lange termijn	Actie korte termijn
CSA Geel	Actie lange termijn	Actie korte termijn	Actie korte termijn
CSA Rood	Actie korte termijn	Actie korte termijn	Actie zeer korte termijn

Definitie acties:

Geen actie: Voer na een jaar opnieuw een ICR en CSA uit.
Actie Lange termijn: Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na een jaar opnieuw een ICR en CSA uit.
Actie Korte termijn: Start een project om belangrijke verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Actie Zeer Korte termijn: Start een project en/of programma om belangrijke verbeteringen te implementeren en bewaak de voortgang.

Figuur 2: Stappen ICR & CSA proces

Deze stappen worden hierna toegelicht.

1. Voer de Inherente Cyber Risicoanalyse (ICR) uit

De onderstaande stappen hebben betrekking op het **bovenste grijs gearceerde ICR-deel** als weergegeven in figuur 3.

Te nemen acties o.b.v. ICR & CSA:

	ICR Laag (>66)	ICR Midden (45-66)	ICR Hoog (<45)
CSA Groen	Geen actie	Actie lange termijn	Actie korte termijn
CSA Geel	Actie lange termijn	Actie korte termijn	Actie korte termijn
CSA Rood	Actie korte termijn	Actie korte termijn	Actie zeer korte termijn

Definitie acties:

Geen actie: Voer na een jaar opnieuw een ICR en CSA uit.
Actie Lange termijn: Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na een jaar opnieuw een ICR en CSA uit.
Actie Korte termijn: Start een project om belangrijke verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Actie Zeer Korte termijn: Start een project en/of programma om belangrijke verbeteringen te implementeren en bewaak de voortgang.

Figuur 3: ICR stappen

1a. Vul de ICR vragenlijst in

De vragenlijst is opgenomen in een aparte bijlage (4a). De vragenlijst bestaat uit 32 vragen, verdeeld over de volgende categorieën:

- **Algemeen**: maakt de organisatie deel uit van de vitale sector?
- **Organisatie** karakteristieken: is er sprake van een reorganisatie, wat is het verloop van personeel?
- **Technologie & derde partijen**: in hoeverre is de organisatie afhankelijk van derde partijen zoals software leveranciers, IT-service- en cloudproviders?
- **Online aangeboden producten en diensten**: is de organisatie afhankelijk van het internet?
- **Externe cyberdreigingen**: wordt uw organisatie genoemd in 'hackerfora'?

Per vraag kan aangegeven worden of sprake is van een hoog, midden of laag risico. De criteria hiervoor staan vermeld in de spreadsheet.

Bijvoorbeeld: vraag 17: er is sprake van een hoog inherent cyberrisico indien binnen uw organisatie als meerdere derde partijen via internet toegang hebben tot de interne systemen van uw organisatie.

17	3. Technologie &	Hebben derde partijen toegang tot interne ICT systemen van uw organisatie?	Ja, 1 of meer partijen	NVT	Geen	1

Figuur 4: Voorbeeld van vraag 17

1b. Behorende tot vitale aanbieders (AED of AAVA)

Vitale aanbieders zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van vitale processen. De vakdepartementen (een departement van de overheid die zich met een bepaald vakgebied bezighoudt) zijn beleidsmatig verantwoordelijk voor de vraag welke aanbieders beschouwd moeten worden als vitaal. Vitale aanbieders worden door het vakdepartement hierover geïnformeerd. In de Wet beveiliging netwerk- en informatiesystemen (Wbni) worden 2 categorieën van vitale aanbieders onderscheiden:

- de Aanbieders van een Essentiële Dienst (AED's) en
- andere aangewezen vitale aanbieders (AAVA's).

Als uw organisatie een AED of AAVA is, dan valt het inherente cyberrisico automatisch in de hoogste categorie. Overige vitale aanbieders die niet zijn aangewezen als AED of als AAVA vallen in de midden categorie voor wat betreft het inherente risico. De nieuwe Cyberbeveiligingswet introduceert in plaats daarvan 'essentiële entiteiten' en 'belangrijke entiteiten', gebaseerd op sector en bedrijfsomvang maar is ten tijde van publicatie nog niet van kracht.

Voor meer informatie over vitale aanbieders, zie: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders

1c. Bepaal de ICR score

Na het invullen van de vragenlijst volgt een totaalscore voor het inherent cybersecurity risico: hoog, midden of laag risico.

Totaal inherent cyber risk	50
Risicoscore	Midden risico

Figuur 5: Voorbeeld totaal score

Deze score kan gebruikt worden als vertrekpunt voor het selecteren van de benodigde beheersmaatregelen binnen de CSA.

2. Voer de Cyber Security Assessment (CSA) uit

Te nemen acties o.b.v. ICR & CSA:

	ICR Laag (>66)	ICR Midden (45-66)	ICR Hoog (<45)
CSA Groen	Geen actie	Actie lange termijn	Actie korte termijn
CSA Geel	Actie lange termijn	Actie korte termijn	Actie korte termijn
CSA Rood	Actie korte termijn	Actie korte termijn	Actie zeer korte termijn

Definitie acties:

Geen actie: Voer na een jaar opnieuw een ICR en CSA uit.
Actie Lange termijn: Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na een jaar opnieuw een ICR en CSA uit.
Actie Korte termijn: Start een project om belangrijke verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Actie Zeer Korte termijn: Start een project en/of programma om belangrijke verbeteringen te implementeren en bewaak de voortgang.

Figuur 6: CSA Stappen

De onderstaande stappen hebben betrekking op het **middelste grijs gearceerde CSA-deel** als weergegeven in voorgenoemd figuur.

2a. Bepaal het team dat de CSA gaat uitvoeren en hoe dit moet gebeuren

De CSA is bedoeld voor de IT-Auditor ter ondersteuning van directies van organisaties.

De vragenlijst kan worden ingevuld door een IT-Auditor (RE) of andere professional die deskundig is op het terrein van informatiebeveiliging. Het heeft de voorkeur om de CSA door een team uit te laten voeren. Dit levert betere resultaten op omdat de verschillende deelnemers ieder vanuit hun eigen invalshoek het object kunnen bekijken. Indien dit om praktische redenen niet mogelijk is, kan ervoor gekozen worden om de CSA door één IT-Auditor uit te laten voeren en te laten reviewen door een tweede IT-Auditor.

Voordat begonnen wordt met het uitvoeren van de CSA is het belangrijk vast te stellen wat u wilt bereiken, wie wat met de resultaten gaat doen en op welke manier de resultaten gebruikt worden.

De antwoorden op bovenstaande vragen worden samengevat in een plan van aanpak zodat hier geen verwarring over kan ontstaan.

2b. Verzamel en bestudeer relevante informatie

Om de CSA vragenlijst zo goed mogelijk in te kunnen vullen, is informatie nodig over:

- De organisatie of het te beoordelen object en de maatschappelijke context hiervan.
- De belanghebbenden in de uitkomst van het assessment en welke eisen en wensen zij hebben met betrekking tot de betrouwbaarheid en continuïteit van informatieverwerking.
- De processen die het betreft en in hoeverre deze processen ook via internet worden ontsloten.
- De gegevens of assets die gebruikt gaan worden.
- De wijze waarop deze gegevens verzameld en verwerkt gaan worden.
- De verschillende systemen die gebruikt worden.
- De manier waarop de gegevens tussen de verschillende systemen worden uitgewisseld en de positie in die keten.

Deze informatie kunt u op verschillende manieren verkrijgen, bijvoorbeeld door:

- Opvragen en opzoeken van documentatie over de organisatie of het object.
- Interviews of workshops met belanghebbenden.

Het heeft de voorkeur dat u alle benodigde informatie voorafgaand aan het invullen van de vragenlijst verzamelt. Dit heeft twee voordelen:

- Bij de beantwoording van de vragen wordt een zo compleet mogelijk beeld meegenomen in de overwegingen.
- U vermijdt dat u meerdere keren terug moet naar dezelfde personen om aanvullende informatie te vragen.

2c. Vul de CSA vragenlijst in

De vragenlijst is opgenomen in een aparte Excel bijlage. Om deze in te vullen dient u de volgende stappen te nemen.

<table>
<tr><th>Stap:</th><th>Actie</th></tr>
<tr><td>1</td><td>Bepaal de risico-indicatie per vraag met ja of nee op basis van het actuele beeld. Als een vraag niet kan worden beantwoord, dan is het antwoord in principe 'Nee'. Achter het antwoord is een mogelijkheid om aanvullende informatie op te nemen.

<table>
<tr><th colspan="2">Reactie & Herstel</th><th>Selecteer score (Ja of Nee)</th></tr>
<tr><td>1</td><td>Is er een incident response plan (CSIRT/SIRT) aanwezig en geoefend, afgestemd op DORA/NIS2 verplichtingen?</td><td>Nee</td></tr>
<tr><td>2</td><td>Worden incidenten geclassificeerd o.b.v. impact en type (bijv. ransomware, datalek, DDoS)?</td><td>Nee</td></tr>
<tr><td>3</td><td>Wordt er binnen 24 uur gerapporteerd aan relevante instanties conform NIS2/DORA?</td><td>Nee</td></tr>
<tr><td>4</td><td>Is er een getest business continuity- en disaster recoveryplan (BCM/DRP)?</td><td>Nee</td></tr>
<tr><td>5</td><td>Worden leveranciers betrokken bij crisissimulaties, Red/Blue teaming of tabletop exercises?</td><td>Nee</td></tr>
<tr><td colspan="2">Totaal score</td><td>0</td></tr>
</table>

</td></tr>
<tr><td>2</td><td>Na beantwoording van alle vragen verschijnt in het dashboard de totale risicoscore (1 – 10).

<table>
<tr><td>Detectie</td><td>0</td><td>U lijkt uw risico's t.a.v. detectie niet te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, DNB controls, PCI/DSS en CIS controls, NIS2 en DORA bieden hier handvatten voor.</td></tr>
<tr><td>Reactie & Herstel</td><td>0</td><td>U lijkt uw risico's t.a.v. reactie & herstel niet te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, PCI/DSS, CIS controls, NIS2 en DORA bieden hier handvatten voor.</td></tr>
<tr><td>Overall cyber risico score (1-10)</td><td>0</td><td></td></tr>
</table>

</td></tr>
<tr><td>3</td><td>Bepaal de relevante standaard(en) die u wenst in te zetten om het risicogebied te beheersen.

U lijkt uw risico's t.a.v. detectie niet te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, DNB controls, PCI/DSS en CIS controls, NIS2 en DORA bieden hier handvatten voor.</td></tr>
</table>

Figuur 7: Voorbeeld van een ingevulde CSA

Deel 3: Acties o.b.v. ICR & CSA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Dashboard – Uitkomsten cyberrisico's

Resultaat ICR en CSA

Aktie korte termijn
Start een project om verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.

ICR staat voor Inherente Cyber Risicoanalyse

De Inherente Cyber Risicoanalyse (ICR) is gericht op het bepalen van het inherente risicoprofiel van een organisatie op het gebied van cybersecurity. Met andere woorden in welke mate loopt de organisatie een cybersecurity risico gezien de activiteiten en werkzaamheden die de organisatie uitvoert in de omgeving waarin de organisatie functioneert. Een ICR is daardoor primair gericht op de omgeving van de organisatie en externe dreigingen die hierin een rol spelen, met uiteraard als startpunt (het karakter van) de werkzaamheden die de organisatie uitvoert.

CSA staat voor Cyber Security Assessment

De CSA legt in de eerste plaats mogelijke risico's bloot van een organisatie, processen, systemen en gegevens die te maken hebben met cybercrime. Daarmee draagt zij bij aan het vermijden of mitigeren van deze cybersecurity risico's. Op basis van de antwoorden van de CSA wordt op gestructureerde wijze inzichtelijk gemaakt of er een kans is dat de organisatie, processen, systemen en gegevens kunnen worden geschaad door een cybercrime aanval en op welke gebieden.

Resultaat Inherente Cyber Risicoanalyse (ICR)

Risicoscore	Midden risico

Resultaat Cyber Security Assessment (CSA)

Overall cyber risico score (1–10)	5

Te nemen actie op basis van ICR en CSA

	ICR Laag (>=7)	ICR Midden (4–6)	ICR Hoog (<4)
CSA Laag (>=7)	Geen aktie	Aktie lange termijn	Aktie korte termijn
CSA Midden (4–6)	Aktie lange termijn	Aktie korte termijn	Aktie korte termijn
CSA Hoog (<4)	Aktie korte termijn	Aktie korte termijn	Aktie zeer korte termijn

Mogelijke acties

Geen aktie	Voer na een jaar opnieuw een ICR en CSA uit.
Aktie lange termijn	Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na 1 jaar opnieuw een ICR en CSA uit.
Aktie korte termijn	Start een project om verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Aktie zeer korte termijn	Start een project of programma om belangrijke verbeterpunten te implementeren en bewaak de voortgang.

Figuur 8: Voorbeeld resultaat ICR & CSA

Te nemen acties o.b.v. ICR & CSA:

	ICR Laag (>66)	ICR Midden (45-66)	ICR Hoog (<45)
CSA Groen	Geen actie	Actie lange termijn	Actie korte termijn
CSA Geel	Actie lange termijn	Actie korte termijn	Actie korte termijn
CSA Rood	Actie korte termijn	Actie korte termijn	Actie zeer korte termijn

Definitie acties:

Geen actie: Voer na een jaar opnieuw een ICR en CSA uit.
Actie Lange termijn: Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na een jaar opnieuw een ICR en CSA uit.
Actie Korte termijn: Start een project om belangrijke verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Actie Zeer Korte termijn: Start een project en/of programma om belangrijke verbeteringen te implementeren en bewaak de voortgang.

Figuur 9: Voorbeeld van stappen in te nemen acties

Na beantwoording van de vragen uit de ICR en CSA worden de resultaten/uitkomsten van de ICR en de CSA in het centrale dashboard (eerste tabblad van de spreadsheet) getoond.

De onderstaande stappen hebben betrekking op het **onderste grijs gearceerde ICR & CSA-deel** als weergegeven in voorgenoemd figuur.

3a. Schat de impact in en raadpleeg de relevante standaarden

Op basis van het overzicht van de risicogebieden waar de cybersecurity mogelijk wordt geschaad kan de organisatie, ondersteund door de IT-Auditor, een inschatting maken van de risico's op het object en/of organisatie. Vervolgens kunnen maatregelen gekozen worden om de risico's tot een voor de organisatie aanvaardbaar niveau te beheersen op basis van relevante standaarden.

Deze twee stappen worden hieronder beschreven.

Impactbepaling

De impact (zoals reputatieschade, maar ook materiële financiële schade als gevolg van compliance issues, klachten en incidenten) die geïdentificeerde risico's op uw organisatie hebben kan voor uw organisatie worden ingeschat op basis van de bij u gebruikelijke methoden voor risicomanagement.

Deze wordt onder andere beïnvloed door de branche waarin u zich begeeft en het belang dat uw klanten en ketenpartners aan security hechten.

Maatregelen nemen om risico's te verkleinen of weg te nemen

Op basis van de inschatting van de impact op de betrokkenen of de organisatie moet worden nagegaan op welke wijze de risico's vermeden of verkleind kunnen worden. U wordt geadviseerd na te gaan of een slechte beheersing is gerechtvaardigd. Het belang en doel van het te beoordelen object, de organisatie en de stakeholders moeten hierbij tegen elkaar worden afgewogen.

Het vermijden of mitigeren van risico's houdt overigens niet in dat de doelen moeten worden bijgesteld. Naarmate de inschatting van de impact hoger wordt, is het raadzaam om maatregelen te treffen om de risico's weg te nemen of te mitigeren. In de vragenlijst zijn diverse relevante standaarden opgenomen over de manier waarop dit kan. Deze standaarden zijn niet uitputtend en uiteraard hangt de toepasbaarheid sterk af van de omgeving.

3b. Stel het ICR & CSA verslag op

De resultaten van de ICR & CSA kunnen in een verslag, nota of adviesrapport worden vastgelegd. Op basis van deze vastlegging kan de gebruiker van de resultaten van de ICR & CSA eventueel noodzakelijke beslissingen nemen. Let op dat de resultaten van de ICR & CSA zeer vertrouwelijk zijn en op detailniveau beperkt beschikbaar moeten worden gesteld.

De Inherente cybersecurity risico's en cybersecurity risicogebieden volgen uit de ingevulde ICR & CSA. Vervolgens wordt in de rapportage ruimte geboden om de impact op de organisatie zelf in te vullen. Ook is ruimte opgenomen voor een advies hoe hiermee dient te worden omgegaan. De overwegingen

die ten grondslag liggen aan de antwoorden op de vragenlijst zijn een belangrijk onderdeel van het ICR & CSA verslag.

Het ICR & CSA verslag kan een dynamisch document zijn. Hiermee wordt bedoeld dat in geval van wijzigingen van het object, bijvoorbeeld een project, de ICR & CSA (deels) opnieuw doorlopen kunnen worden en waar nodig het verslag op onderdelen geactualiseerd kan worden.

3c. Bespreek de ICR & CSA met het verantwoordelijke management

Tot slot bevelen wij aan dat u het verslag met de uitkomsten van de ICR & CSA bespreekt met het bestuur of de directie die verantwoordelijk is voor de (IT) beveiliging van de organisatie. Dit gesprek biedt de mogelijkheid de bevindingen die naar voren zijn gekomen bij de uitvoering van de ICR & CSA toe te lichten en verbeteringen planmatig te borgen in de organisatie.

Het is raadzaam bij de bespreking met de directie een (interne) IT-Auditor uit te nodigen die betrokken is geweest bij de uitvoering van de ICR & CSA. Hiermee kunnen adviezen die naar voren zijn gekomen in de bespreking geborgd worden en opgenomen in de risicomanagementcyclus. Hierbij kan tevens een beoordeling plaatsvinden op bijvoorbeeld:

- Interpretatie en inschatting van de (rest)risico's.
- Praktische en inhoudelijke juistheid, haalbaarheid en volledigheid van voorgestelde maatregelen.

De inzet van externe deskundigen bij de bespreking met het management kan behulpzaam zijn om de aanwezigheid van de juiste expertise te waarborgen. Gezien de diepgang van de uitvoering van de ICR & CSA zal wellicht beperkt gebruik gemaakt worden van deze mogelijkheid en de kwaliteit van de uitvoering vooral afhangen van de ervaring van het verantwoordelijke management met risico's van cybercrime.

Bijlage 1: ICR vragenlijst

Deze is als onderdeel van de MS-Excel bijlage beschikbaar op de NOREA-website.

Bijlage 2: CSA vragenlijst

Deze is als onderdeel van de MS-Excel bijlage beschikbaar op de NOREA-website.