NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

Introductie, handreiking en vragenlijst

Versie 3.0.2

Mei 2023

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 7984, 1008 AD Amsterdam
Telefoon: 020-3010380
E-mail: norea@norea.nl
Meer informatie kunt u vinden op:
https://ww.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. Dit document heeft tot dat moment de formele status van studierapport (conform artikel 18 Reglement Beroepsbeoefening).

Inhoud

Voorwoord

Onze samenleving digitaliseert exponentieel. Wie kan zich de introductie van de smartphone in 2007 nog herinneren? En dat er slechts een klein groepje “nerds” als *early adopters* enthousiast mee aan de slag ging? Inmiddels heeft 87% van de Nederlanders een smartphone of tablet. Als gevolg van deze ontwikkelingen is een samenleving zonder IT eigenlijk niet meer voor te stellen. Het belang van IT zal ook alleen maar sneller toenemen. De samenwerking tussen organisaties is steeds meer gebaseerd op (soms volledig) geautomatiseerde uitwisseling van gegevens. Hierbij heeft digitalisering een steeds grotere impact op de fysieke wereld, van zelfsturende auto’s, een groeiend aantal digitale identiteits- en betaalmiddelen tot en met het bestellen van dagelijkse boodschappen via het internet.

Deze ontwikkelingen vormen een belofte voor de toekomst. Ze vormen echter ook een uitdaging omdat onze afhankelijkheid van IT steeds groter wordt. Hoe gaan organisaties en overheden de risico’s die spelen rondom de beveiliging van deze steeds verdergaande digitalisering beheersen? Wat is het belang en invloed van de typologie van het bedrijf en de daaraan verbonden inherente risico’s? En hoe moet worden omgegaan met wat dit betekent voor medewerkers bij die organisaties? De impact van misbruik van en/of fouten in de digitale gegevensverwerking zal hierdoor in de toekomst verder toenemen. Wet- en regelgeving geven momenteel beperkt handvatten hoe hiermee om te gaan. De Wet van Moore, die een exponentiële groei van opslagcapaciteit en snelheid van computerchips voorspelde, heeft bijna vijftig jaar standgehouden en de gevolgen daarvan zullen voorlopig nog doorwerken. Bovendien worden belangrijke vorderingen gemaakt met de ontwikkeling van de quantumcomputer, die nog meer rekenkracht kan ontwikkelen, dus dit gaat ook niet veranderen. Er zijn veel internationale gremia met specialisten die zeer bruikbare normen en richtlijnen ontwikkelen om te helpen bij het beheersen van de risico’s rondom digitalisering, zonder in te boeten op de kansen die geboden worden. Vanwege de snelheid en het belang van deze ontwikkelingen is de NOREA van mening dat publiek beschikbare hulpmiddelen als de *Cyber Security Assessment* en de *Inherente Cyber Risicoanalyse* (NOREA-CSA&ICR) bijdragen om op hoofdlijnen de risico’s rondom cybersecurity in kaart te brengen en daarmee de beheersing van deze risico’s binnen de risicomanagement cyclus te verbeteren.

De NOREA-kennisgroep CyberSecurity wenst u veel succes met het gebruik van deze hulpmiddelen. De kennisgroep nodigt u uit om haar op de hoogte te stellen van nieuwe normenkaders en richtlijnen die naar uw mening nuttig zijn. Aangezien dit een publiek beschikbare aanpak is, rekenen we op uw bijdrage in het verder ontwikkelen van de NOREA-CSA&ICR.

De NOREA-kennisgroep CyberSecurity, mei 2023.

Versiebeheer

Versie	Datum	Aanpassing
1.1	Augustus 2015	Initieel document
2.0	April 2019	Invoeging Inherente Cyber Risicoanalyse (ICR)
2.1	September 2019	Reviewversie t.b.v. de Vaktechnische Commissie
2.1.1	Oktober 2019	Verwerking commentaar en tekstredactie
2.2	Oktober 2020	Integratie CSA en ICR in één tabel, update referenties
3.0	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.
3.0.1	April 2023	Reviewversie t.b.v. de Vaktechnische Commissie
3.0.2	Mei 2023	Verwerking commentaar en tekstredactie

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 deze instrumenten gebruikt worden door de actoren binnen de risicomanagementcyclus, zoals Internal/External Audit, securitymanagement en risk management, ondersteund door een IT-auditor. Dit document bestaat uit de volgende delen:

Deel 1a: Introductie: over het instrument 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 het instrument 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)?

Deel 1a: Introductie: over het instrument 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?

Beschrijving van het instrument ICR

Wat is een 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.

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’ (in een getal op de schaal 24 t/m 72). 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.

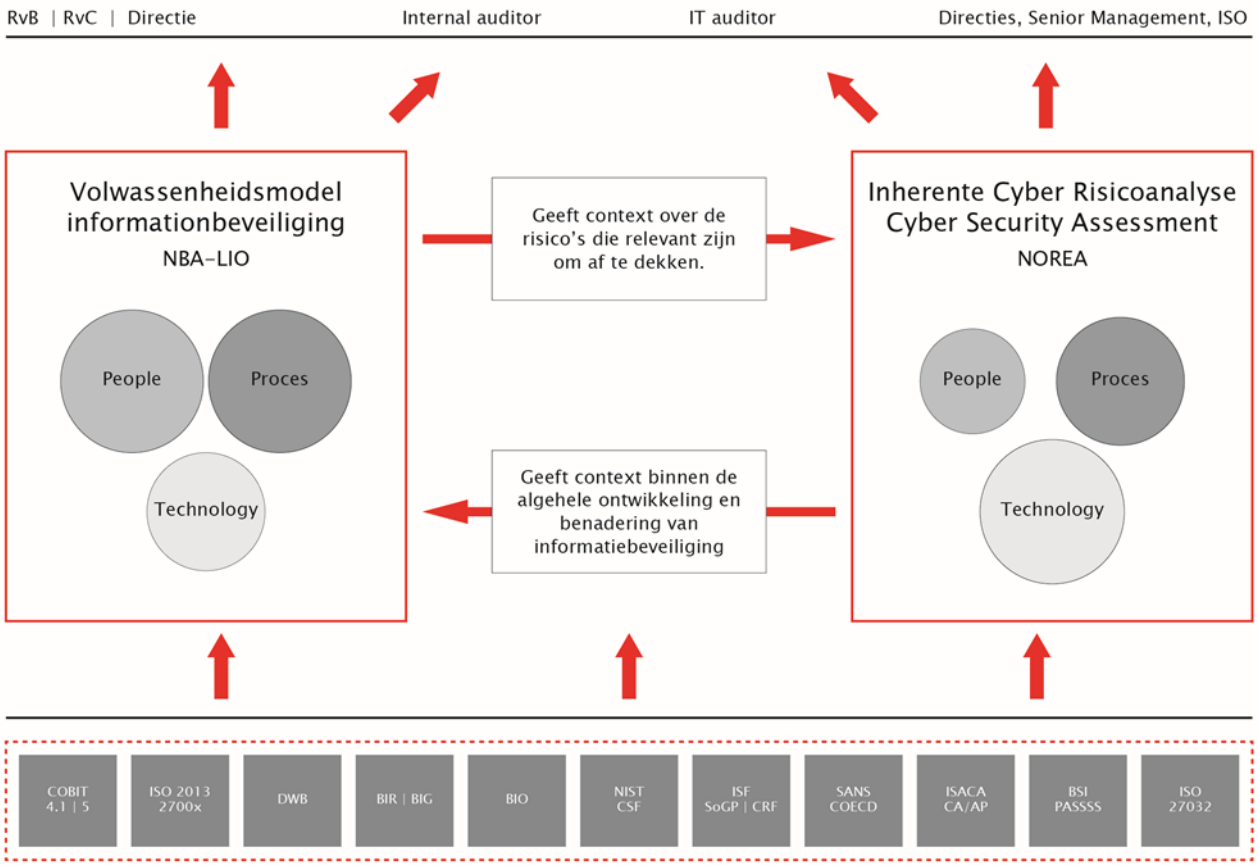
Wat is het belang van een ICR?

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 24 vragen verdeeld over verschillende categorieën zoals organisatiekarakteristieken en aangeboden producten of diensten, 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.



Achtergrond van de ICR

De ICR is gebaseerd op de Cybersecurity Assessment Tool van de Amerikaanse financiële toezichthouder Federal Financial Institutions Examination Council (FFIEC), zie https://www.ffiec.gov/cyberassessmenttool.htm. Deze tool is zeer uitgebreid en met name bedoeld voor de financiële sector. 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 het instrument 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 geen verplicht instrument, maar naar ons inzicht een onmisbaar hulpmiddel 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 belangrijk onderdeel van de belangenafweging en besluitvorming over de informatiebeveiliging- en privacy strategie. 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 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 en privacy wordt gerespecteerd.
3. Het verbeteren van de communicatie over *security*, privacy en de bescherming van vertrouwelijke gegevens.

Wanneer voert u een CSA uit?

In ieder geval éénmaal per jaar voor het te beoordelen object. Dit laatste kan bijvoorbeeld zijn 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.

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 "Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT". Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (definitie NCSC, juni 2012). 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 waarin vormen van criminaliteit worden omvat die betrekking hebben op, of gepleegd worden met, computersystemen, inclusief telecommunicatienetwerken. De criminele activiteiten kunnen hierbij gericht zijn tegen personen, eigendommen en/of organisaties of elektronische telecommunicatienetwerken en computersystemen.

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.

Andere (Cyber) Securityinstrumenten

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

- National Institute of Standards and Technology (NIST)/Cyber Security Framework (CSF)
    - version 1.1
- 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 2019/2020
- Payment Card Industry (PCI)/Data Security Standard (DDS)
    - V4.0
- Critical Security Controls (CIS)

- v8 May 18, 2021

- Cloud Security Alliance (CSA) / Cloud Controls Matrix (CMM)
  - V4.05

Bovenstaande standaarden zijn niet uitputtend en uiteraard hangt de toepasbaarheid sterk af van de omgeving en het gekozen object. Verder leggen de standaarden de nadruk op cybersecurity, dat een geïntegreerd onderdeel uitmaakt van de aanpak van informatiebeveiliging in de breedste zin.

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
7. Reactie

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.

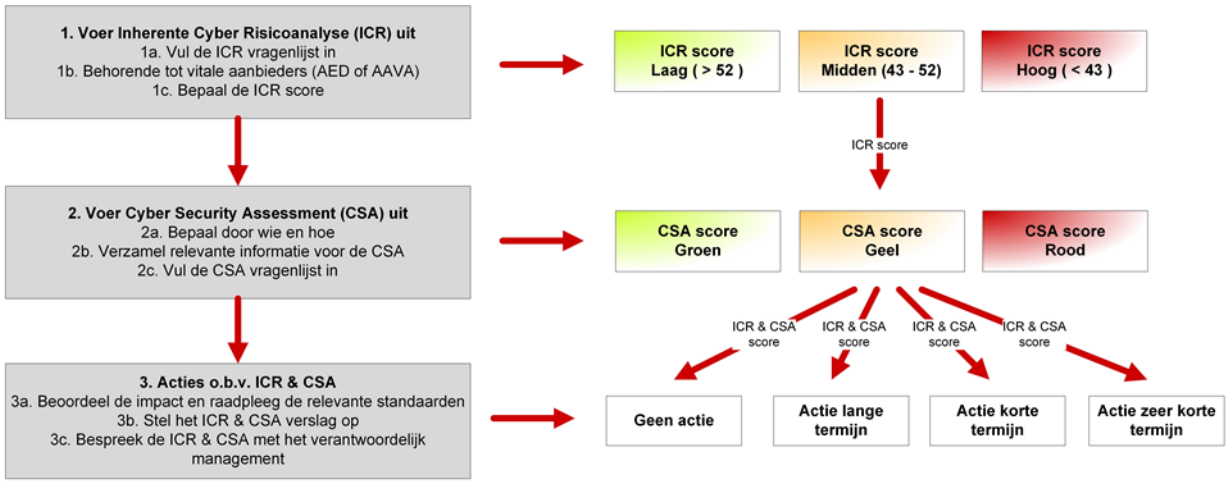
De kennisgroep heeft de ambitie om de CSA uit te breiden met aangepaste, andere en nieuwe standaarden op het gebied van cybersecurity. Voorliggende versie 3 is hiervan een uitwerking.

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 (> 52)	ICR Midden (43 - 52)	ICR Hoog (< 43)
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

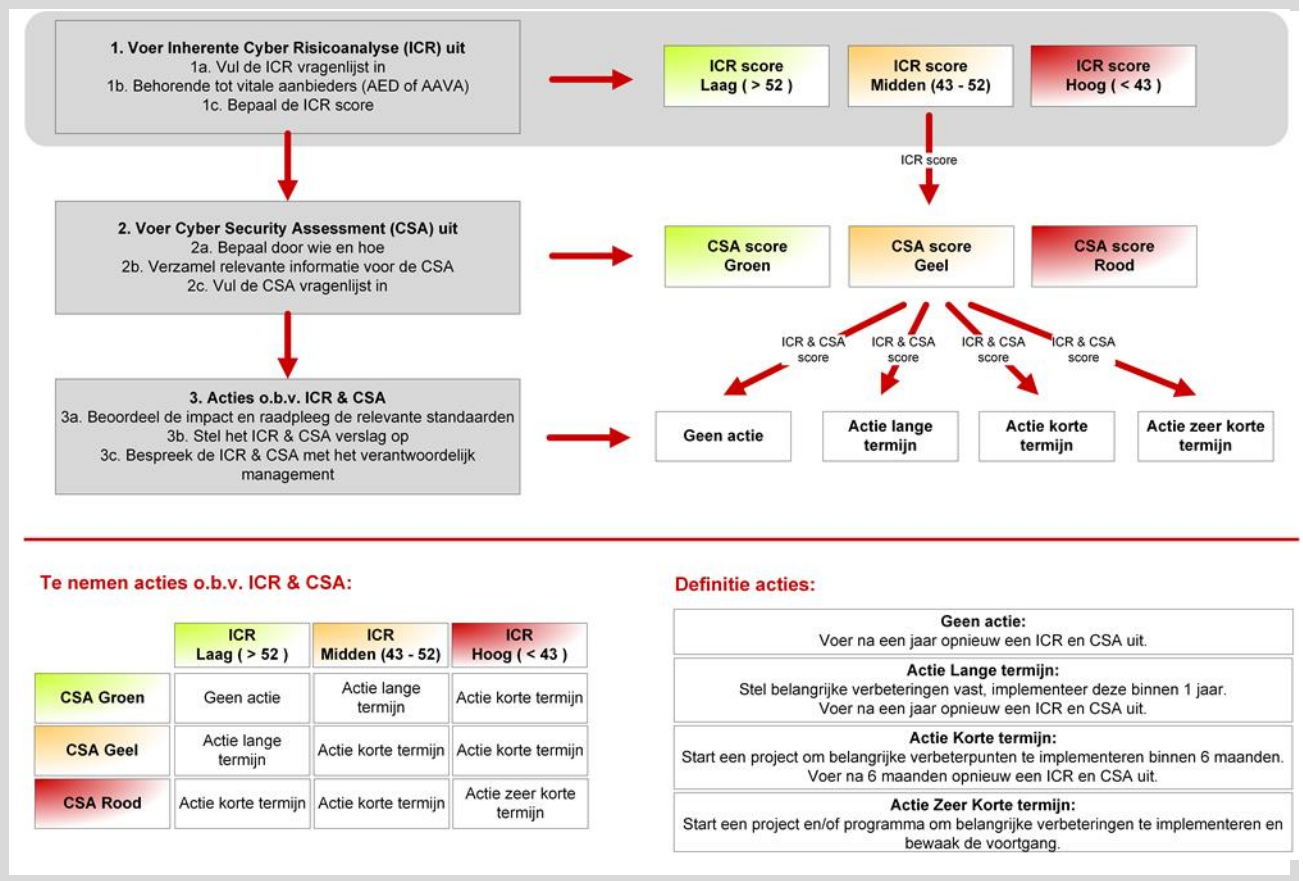
Definitie acties:

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.

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 voorgenoemd figuur.



1a. Vul de ICR vragenlijst in

De vragenlijst is opgenomen in een aparte bijlage (4a). De vragenlijst bestaat uit 24 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?
- **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 14: 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.

Nr.	Categorie	Vraag	1 = Hoog	2 = Midden	3 = Laag	Risico inschatting
14	Technologie & derde partijen	Hebben derde partijen toegang tot de interne ICT systemen van uw organisatie?	1 of meer derde partijen met toegang tot interne systemen	NVT	Geen derde partijen, individuen met toegang tot interne systemen	3

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.

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

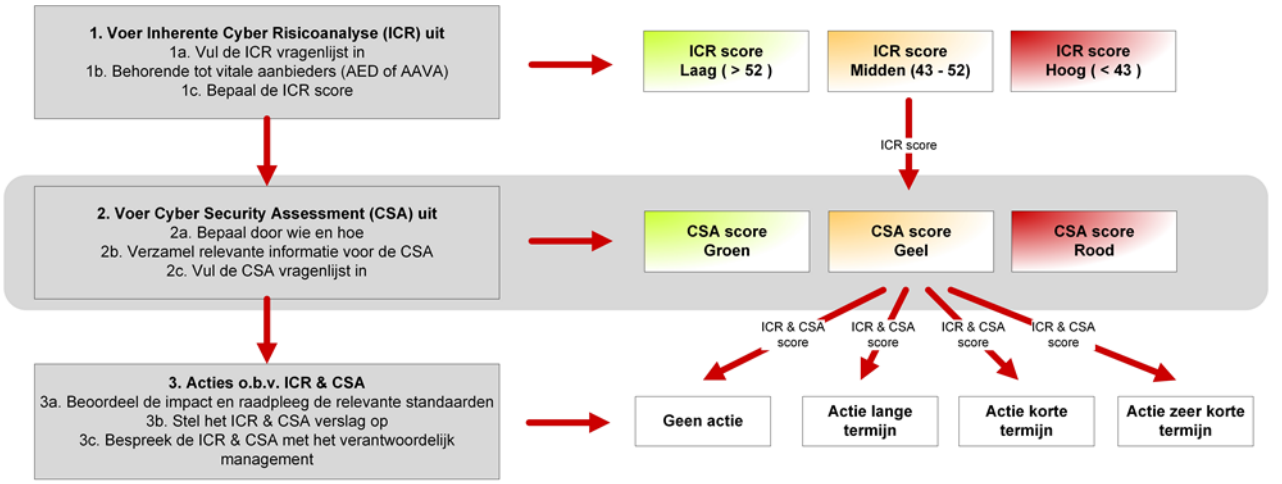
1c. Bepaal de ICR score

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

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 (> 52)	ICR Midden (43 - 52)	ICR Hoog (< 43)
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.

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 auditor 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.

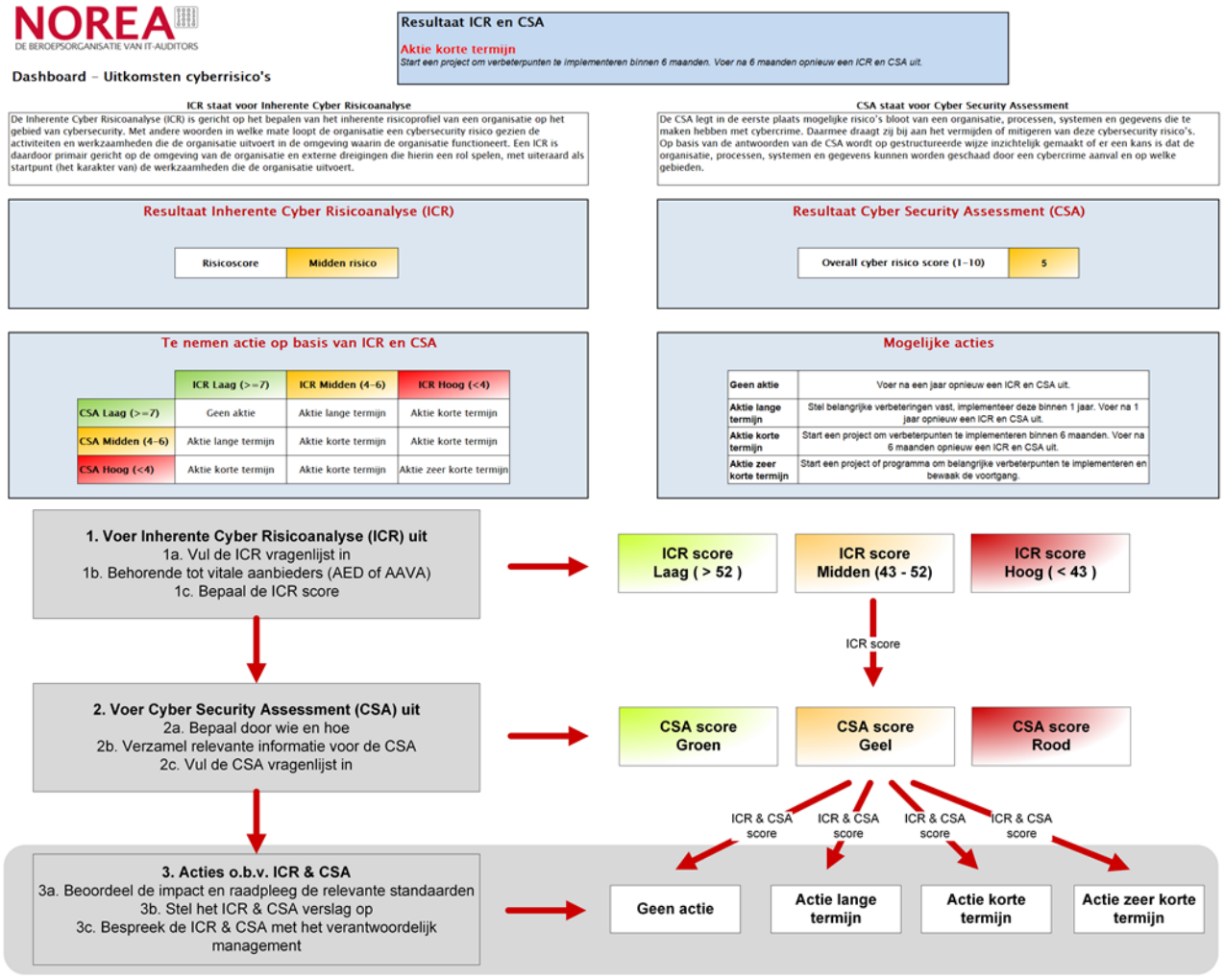
2c. Vul de CSA vragenlijst in

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

Stap:	Actie
1	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.

	 **Reactie** — Selecteer score (Ja of Nee) 1 Kan de organisatie snel acteren richting de diverse stakeholders in geval van een cyberdreiging? — Nee 2 Is een specifiek proces ingericht voor de afhandeling van cybersecurity incidenten? Denk hierbij bijvoorbeeld aan Ransomware, Phishing, CEO fraude, etc.) — Nee 3 Is een (cyber)Security Incident Response Team of vergelijkbaar orgaan ingericht en staat deze ook in verbinding met de Business Continuity Management (BCM) organisatie? — Ja 4 Heeft u een actueel BCM-draaiboek voor het geval dat uw organisatie getroffen wordt door een cybersecurityaanval? — Nee 5 Maakt de organisatie voor de afhandeling van incidenten onderscheid o.b.v. bijvoorbeeld impact van een incident? Business Impact Assessment (BIA). — Nee 6 Vinden periodiek red/bleu-teaming trainingen / testen plaats om cybersecurity incidenten effectief af te handelen? — Ja 7 Zijn uw kritische leveranciers en afnemers (contractueel) onderdeel van het responseproces en zijn zij daar ook van op de hoogte/aansprakelijk? — Ja 8 Zijn uw kritische leveranciers en afnemers betrokken bij uw trainingen / testen voor cyberincidenten? — Nee **Totaal score** 4
2	Na beantwoording van alle vragen verschijnt in het dashboard de totale risicoscore (1 - 10).  Detectie — 5 — U lijkt uw risico's t.a.v. detectie niet volledig te kennen en te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, DNB controls, PCI/DSS, CIS controls en CCM bieden hier handvatten voor. Reactie — 4 — U lijkt uw risico's t.a.v. reactie niet volledig te kennen en te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, PCI/DSS en CIS controls bieden hier handvatten voor. **Overall cyber risico score (1-10)** — 5
3	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 volledig te kennen en te beheersen. De normen van NIST CSF, ISO/IEC 27002, ISACA COBIT, DNB controls, PCI/DSS, CIS controls en CCM bieden hier handvatten voor.

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



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

	ICR Laag (> 52)	ICR Midden (43 - 52)	ICR Hoog (< 43)
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.

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 moet u zelf vaststellen. Deze wordt onder andere beïnvloed door de branche waarin u zich begeeft en het belang dat uw klanten en ketenpartners aan security en privacy 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 worden vastgelegd. Op basis van dit verslag kan de gebruiker van de resultaten van de ICR & CSA eventueel noodzakelijke beslissingen nemen. Let op dat een dergelijk verslag zeer vertrouwelijk is en beperkt op detailniveau beschikbaar wordt 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 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.

Deel 4a: BIJLAGE – ICR vragenlijst

Deze is als onderdeel van de MS-Excel bijlage beschikbaar

Zie https://www.norea.nl/organisatie/kennis-en-werkgroepen/kennisgroep-cybersecurity

Deel 4b: BIJLAGE – CSA vragenlijst

Deze is als onderdeel van de MS-Excel bijlage beschikbaar

Zie https://www.norea.nl/organisatie/kennis-en-werkgroepen/kennisgroep-cybersecurity

Leden NOREA Kennisgroep CyberSecurity

- drs. Hanifi Akçay RE
- drs. ir. Marcel Baveco RE CISA CRISC CISSP
- drs. Rob Bouman RE RA
- Jalal Bani Hashemi MSc RE CISSP CCSP CISA
- drs. Dennis van Heijst RE
- ing. Johan Hofhuis RI EMITA RE
- dr. ing. Jürgen van Grinsven RE
- ing. Richard Kok RE CISSP
- ir. Peter Kornelisse, RE CISA CIPP/e
- Christopher Nield MSc CISA CISSP
- Amer Ramkoeber MSc RE CISSP CISM CGEIT
- ing. Danny Schmidt, RE MSc CISSP CISM
- mr. Wouter Bas van der Vegt RE (voorzitter)
- Tom Verharen, RE MSc CISA CISSP CD
- drs. Marc Welters RE RA (linking-pin bestuur)
- ing. Marcel Woltjes RE
- ing. Jean Zweers RE CISA CISSP