NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Cyber Security Assessment (NOREA-CSA)

Introductie, handreiking en vragenlijst

Augustus 2015

Over deze handreiking Cyber Security Assessment (NOREA-CSA)

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:
http://www.norea.nl

De CSA zal worden geëvalueerd en in de toekomst worden verbeterd. Het is de bedoeling de CSA op basis van ervaring en evaluatie als de NOREA-handreiking (conform artikel 15 Reglement Beroepsbeoefening) vast te stellen. Dit document heeft tot dat moment de formele status van studierapport (conform artikel 18 Reglement Beroepsbeoefening).

Inhoud

Voorwoord

Onze samenleving is exponentieel aan het digitaliseren. Wie kan zich nog herinneren dat de eerste smartphone pas in 2007 zijn intrede deed? En dat er slechts een klein groepje “nerds” als *early adopters* enthousiast mee aan de slag ging? Eind 2014 heeft inmiddels driekwart 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 verder gaande 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 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 lijkt niet af te zwakken, 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 een publiek beschikbaar hulpmiddel als de *Cyber Security Assessment* (NOREA-CSA) bijdraagt om op hoofdlijnen de risico’s rondom cybercrime in kaart te brengen en daarmee aan de beheersing van deze risico’s binnen de risicomanagement cyclus.

De NOREA-kennisgroep CyberSecurity wenst u veel succes met het gebruik van dit hulpmiddel. 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, verwachten we ook uw bijdrage in het verder ontwikkelen van de NOREA-CSA.

De NOREA-kennisgroep CyberSecurity.

Leeswijzer

De CSA is primair bedoeld als middel voor IT-Auditors in hun werkzaamheden voor directies en senior management van organisaties. Daarnaast kan de CSA gebruikt worden door de actoren binnen de risicomanagementcyclus, zoals *Internal Audit, security management* en *risk management*, ondersteund door een IT-Auditor.

De CSA bestaat uit de volgende delen:

Deel 1: Introductie: over het instrument CSA

In dit eerste deel wordt ingegaan op de achtergrond en het belang van de CSA. U krijgt antwoord op vragen als *Wat is een CSA? Wat is het belang van een CSA? Wat levert het uitvoeren van een CSA op? Hoe verhoudt de CSA zich tot andere informatiebeveiligings-instrumenten?*

Deel 2: Handreiking voor het CSA proces

Dit deel bevat een handreiking voor het effectief en efficiënt uitvoeren van een CSA. U krijgt antwoorden op vragen als *Uit welke stappen bestaat het CSA proces? Wie kan ik betrekken bij de CSA? Wat zijn succes- en faalfactoren?*

Deel 3: CSA-vragenlijst

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

- *Wat zijn voor mijn organisatie de belangrijkste cybercrime risico's van de verwerking en beheersing van gegevens?*
- *Hoe kan mijn organisatie deze risico's mitigeren?*

Deel 1: 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 is het belang van een CSA? Wat levert het uitvoeren van een CSA op? Hoe verhoudt de CSA zich tot andere informatiebeveiligingsinstrumenten?

Beschrijving van het instrument CSA

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 te maken hebben met cybercrime. Daarmee draagt zij bij aan het vermijden of mitigeren van deze *Cyber Security* risico's. De CSA kan als zelfstandig *assessment* worden uitgevoerd of als onderdeel van bijvoorbeeld 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 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 *Cyber Security* risico's inzichtelijk te maken. 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.

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.

Voor wie is het instrument CSA bedoeld?

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. In het algemeen kan worden gezegd dat het zinvol is een CSA minimaal éénmaal per jaar uit te voeren.

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 *Cyber Security* mee te nemen bij het verdere ontwerp van een systeem. 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 *Cyber Security* 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 *Cyber Security*;
- 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 CSA 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?

Cyber Security 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 *Cyber Security* steeds belangrijker.

Wij hanteren voor de definitie van het begrip *"Cyber Security"* de formulering van het NCSC, te weten "*Cyber Security* 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). *Cyber Security* is daarmee direct gelieerd aan begrippen als Cybercrime, Datalekken, Privacy bescherming, DDoS 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, keten-verantwoordelijkheden (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) Security instrumenten

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

- *Information Security Forum (ISF):*
  - *Standard of Good Practice (SoGP)*
  - *Cyber Resilience Framework (CRF)*
- *SANS Institute (SANS)*
  - *Critical Controls for Effective Cyber Defense (CCfECD)*
- *Information Systems Audit and Control Association (ISACA)*
  - *Cybercrime Audit/Assurance Program*
- *British Standards Institute (BSI)*
  - *PAS 555 Cyber security risk. Governance and management.*
- *National Institute of Standards and Technology (NIST)*
  - *Cyber Security Framework*
- *International Standards Organisation (ISO)*
  - *ISO27032 Guidelines for cybersecurity*

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 *Cyber Security*, dat een geïntegreerd onderdeel uit maakt 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. In de toekomst is de ambitie om de CSA uit te breiden met aangepaste, andere en nieuwe standaarden op het gebied van Cyber Security.

De kennisgroep heeft de ambitie om de CSA uit te breiden met aangepaste, andere en nieuwe standaarden op het gebied van *Cyber Security*.

De NOREA leden en andere gebruikers van de CSA worden nadrukkelijk uitgenodigd hieraan een bijdrage te leveren.

Positionering Cyber Security Assessment in GBRE

De NOREA kent een kwaliteitsraamwerk van Gedrags- en Beroepsregels voor Register EDP-Auditors (GBRE). De CSA is hierbinnen gepositioneerd in aandachtsgebied D als assessment dat gebruikt kan worden door IT-Auditors. Het kwaliteitsraamwerk is hieronder weergegeven. Middels deze positionering kan de CSA tevens als onderdeel van een audit worden uitgevoerd.

A1 Statuten

B1 Reglement Gedragscode

B2 Reglement Beroepsbeoefening

B3 Reglement Kwaliteitsbeheersing NOREA

B4 Reglement KwaliteitsOnderzoek NOREA

- A2 Huishoudelijk reglement
- A3 Reglement van toelating
- A4 Reglement van beroepsethiek
- A5 Reglement van Tucht
- A6 Reglement van beroep
- A7 Richtlijn Permanente Educatie
- A8 Regeling Overstappers en herintreders

- C1 Raamwerk Assurance-opdrachten
- C1 Richtlijn Assurance-opdrachten

D Audit
Assessment
Review
Quick Scan
Beoordeling
Analyse

E Advies

Invulling in ontwikkeling

F Niet Actief zoals in business of gepensioneerd

(geen invulling b2 en b3 n.v.t.)

G Uitvoeringsrichtlijnen

Opdrachtaanvaarding (210) en documentatie (230)

H Handreikingen (ZekeRE Business en ZekeRE Zorg DBC en AWBZ, Studierapporten, Handboek en de 'EDP-Auditor'

Deel 2: Handreiking voor het CSA proces

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

Wat zijn de stappen in een CSA proces?

De uitvoering van een CSA bestaat uit de volgende stappen:

1. Bepaal wie de CSA gaat uitvoeren en hoe dit moet gebeuren.
2. Verzamel relevante informatie voor de CSA.
3. Vul de CSA vragenlijst in.
4. Beoordeel de impact en raadpleeg de relevante standaarden.
5. Stel het CSA verslag op.
6. Bespreek de CSA met het verantwoordelijke management.

Deze stappen worden hierna kort toegelicht.

1 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.

2 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.

3 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
2	Na beantwoording van alle vragen verschijnt in het dashboard de totale risicoscore (1 - 10).
3	Bepaal de relevante standaard(en) die u wenst in te zetten om het risicogebied te beheersen.

4 Schat de impact in en raadpleeg de relevante standaarden

Op basis van het overzicht van de risicogebieden waar de Cyber Security mogelijk wordt geschaad kan de organisatie, ondersteund door de IT-Auditor, een inschatting maken van de impact 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.

Impact bepaling

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, 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 beoor-delen object, de organisatie en stakeholders moeten hierbij tegen elkaar worden afgewogen.

Het vermijden of mitigeren van risico's houdt overigens niet altijd in dat de doelen moeten worden bijgesteld. Naarmate de inschatting van de impact hoger wordt, is het raadzamer 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.

5 Stel het CSA verslag op

De resultaten van de CSA kunnen in een verslag worden vastgelegd. Op basis van dit verslag kan de gebruiker van de resultaten van de CSA eventueel noodzakelijke beslissingen nemen. Let op dat een dergelijk verslag zeer vertrouwelijk is en beperkt op detailniveau beschikbaar wordt gesteld.

De Cyber Security risicogebieden volgen uit de ingevulde 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 CSA verslag.

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

6 Bespreek de CSA met het verantwoordelijke management

Tot slot is het raadzaam dat u het verslag met de uitkomsten van de 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 CSA toe te lichten en veranderingen 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 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:

1. Interpretatie en inschatting van de (rest)risico's.
2. 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 CSA zal wellicht beperkt gebruik gemaakt worden van deze mogelijkheid en vooral afhangen van de ervaring van het verantwoordelijke management met risico's van cybercrime.

Deel 3: BIJLAGE – CSA vragenlijst

Deze is in een aparte Excel bijlage beschikbaar

Leden NOREA Kennisgroep CyberSecurity

drs. ir. M.P.P. Baveco RE CISA CISSP CRISC

drs. R.P. M. van Beusekom RE RO

drs. R.R. Bouman RE RA

ing. J.G.M. Hofhuis RI EMITA RE

drs. A.L. Hristova RE CISA

ing. T.P. Inia RE

ing. R.H.J. Kok RE

ing. M. van der Krift RE CISSP

M.J.B. van Leeuwen RE

R.J. Mora RE CISSP

ing. M.H.L. van Rooijen RE CISA

mr. W. B. van der Vegt RE CISSP CIPP/E

ing. M.S. Woltjes RE

R. Zwartjes RE