

w

**CCV** centrum voor  
criminaliteitspreventie en  
veiligheid

## CCV-Certificatieschema BORG-A

Productcertificaat voor het  
beveiligingsplan

Versie 1.0

Publicatiedatum: 1 september 2023

Ingangsdatum: 1 januari 2024



# Inhoud

<b>1 Inleiding</b>	<b>5</b>
1.1 Algemeen	5
1.1.1 Doel van het certificatieschema	5
1.1.2 Verantwoordelijkheden	6
1.1.3 Leeswijzer	6
1.2 Toepassingsgebied	6
1.3 Relatie met wet- en regelgeving	6
1.4 Relatieschema	7
1.5 Overgangsregeling	7
<b>2 Eisen aan het product</b>	<b>8</b>
2.1 Algemeen	8
2.2 Beoordelingsmethoden, eisen, goed- en afkeur	8
2.2.1 Algemeen	8
2.2.2 Eisen aan het beveiligingsplan	8
<b>3 Voorwaarden voor certificatie</b>	<b>11</b>
3.1 Algemeen	11
3.2 Eisen aan het kwaliteitssysteem	11
3.2.1 Organisatie en verantwoordelijkheden	11
3.2.2 Kwalificaties	11
3.2.3 Uitbesteden	14
3.2.4 Inhuur	14
3.2.5 Inkoop en aanleveren	14
3.2.6 Startinformatie en dossier	14
3.2.7 Documentbeheer, registraties en archivering	15
3.2.8 Klachten	16
3.2.9 Herstel en Corrigerende maatregelen	17
3.2.10 Evaluatie	17
3.3 Voorwaarden bij aanvraag en in standhouden	17
3.3.1 Gegevens bij aanvraag	17
3.3.2 Status gedurende de aanvraag	18
3.3.3 Bezoeken op locatie	18
3.3.4 Planning	18
3.3.5 Wijzigingen	18
<b>4 Uitvoering van certificatie</b>	<b>19</b>
4.1 Eisen aan de certificatie-instelling	19
4.1.1 Algemeen	19
4.1.2 Kwalificaties	19
4.2 Processchema	21
4.3 Behandelen aanvraag	23
4.4 Initiële beoordeling	24
4.4.1 Uitvoering	24
4.4.2 Tijdsbesteding en steekproef	24
4.4.3 Rapportage, beoordeling en besluitvorming	25
4.4.4 Publicatie	25
4.5 Periodieke beoordeling	25

4.5.1	Uitvoering	25
4.5.2	Frequentie, tijdsbesteding en steekproef	26
4.5.3	Rapportage, beoordeling en besluitvorming	27
4.6	Extra beoordeling	27
4.7	Reductie van tijdsbesteding op basis van andere certificaten	27
4.8	Afwijkingen	27
4.8.1	Major – kwaliteitssysteem	28
4.8.2	Major - product	28
4.8.3	Major - consequenties	28
4.8.4	Major - Beoordeling door de certificatie-instelling	28
4.8.5	Minor – kwaliteitssysteem	29
4.8.6	Minor - product	29
4.8.7	Minor - consequenties	29
4.8.8	Minor - Beoordeling door de certificatie-instelling	30
4.9	Schorsing	30
4.9.1	Schorsen	30
4.9.2	Consequenties van schorsing	30
4.9.3	Opheffen van de schorsing	30
4.10	Intrekking	31
4.10.1	Intrekken	31
4.10.2	Consequenties van intrekking	31
4.10.3	Nieuwe aanvraag	31
<b>5 Certificaat en certificatiemerk</b>		<b>32</b>
5.1	Certificatiemerk	32
5.1.1	Woord/Beeldmerk	32
5.1.2	Gebruik van het merk	32
5.2	Productcertificaat	33
5.3	Beveiligingsplan met certificatiemerk	33
<b>6 Verwijzingen</b>		<b>34</b>
6.1	Wet- en regelgeving	34
6.2	Begrippen en afkortingen	34
6.3	Normen en verwijzingen	35
<b>Bijlage 1 - Toelichting beveiligingsplan</b>		<b>37</b>
B1.1	Inleiding	37
B1.2	Projectinformatie en doel	37
B1.3	Omschrijving object en gebruik	39
B1.4	Herkomst uitgangspunten	39
B1.5	Kwaliteitsborging	42

# 1 Inleiding

Het risico bepaalt welke beveiligingsmaatregelen nodig zijn. Doeltreffende beveiliging bestaat uit een combinatie van verschillende beveiligingsmaatregelen die passen bij het risico. Als gebruiker van een object (verder te noemen afnemer), wil je graag dat dit goed gebeurt van ontwerp tot realisatie. Een goed beveiligingsplan is daarbij onmisbaar.

Dit certificatieschema richt zich op het certificeren van het beveiligingsplan. Naast dit schema zijn er ook certificatieschema's voor het leveren van bouwkundige inbraakbeveiliging (BORG-B) en het leveren van alarminstallaties (BORG-E).

## 1.1 Algemeen

### 1.1.1 Doel van het certificatieschema

Doeltreffende beveiliging is gebaseerd op een samenhangend geheel van verschillende beveiligingsmaatregelen die passen bij het risico van het object. Daarvoor is een deskundig opgesteld en goed onderbouwd plan nodig. Bij beveiligingsmaatregelen gaat het om organisatorische, bouwkundige (inclusief compartimentering), elektronische (inclusief alarmering), reactieve en meeneembeperekende maatregelen. De combinatie staat bekend als OBESCAR<sup>1</sup>.

Voor een gebouw of woning wordt op basis van de aard en omvang van het risico en het gekozen doel van de beveiliging een passend en uitvoerbaar beveiligingsplan opgesteld. Doel van het beveiligingsplan is het beschrijven van een samenhangend, bruikbaar en doeltreffend geheel van OBESCAR-maatregelen waarmee het risico wordt teruggebracht tot een voor de betrokken partijen aanvaardbaar niveau.

Het opstellen van een dergelijk beveiligingsplan moet deskundig gebeuren, zodat het in de praktijk leidt tot adequate en effectieve vermindering van het risico. Publieke en private partijen hebben daarom behoefte aan geborgde kwaliteit bij het leveren van beveiligingsplannen. Die borging is mogelijk met productcertificatie van het beveiligingsplan. De eigenschappen van het product en de eisen die hiermee samenhangen staan in hoofdstuk 2.

Het doel van dit certificatieschema is het waarborgen van de kwaliteit van het beveiligingsplan. Het certificatieschema richt zich op het certificeren van het beveiligingsplan.

Doel van het certificeren van het beveiligingsplan is het verminderen van faal- en risicokosten bij afnemers die kunnen optreden als de vermeende kwaliteit niet aanwezig is. Door certificatie kunnen afnemers een gerechtvaardigd vertrouwen hebben dat het geleverde beveiligingsplan, voorzien van het certificatiemerk, voldoet aan de vooraf gestelde eisen en past bij hun risico.

Het vastleggen van de eisen aan een beveiligingsplan en het beschrijven van de uitvoering van certificatie heeft als doel:

- de samenhang tussen de OBESCAR-maatregelen te waarborgen;
- een geharmoniseerde uitvoering;

---

<sup>1</sup> OBESCAR staat voor Organisatorische maatregelen, Bouwkundige maatregelen, Elektronische maatregelen, Signalering, Compartimentering, Alarmering, Reactie.

- het informeren van de markt hoe certificatie van het beveiligingsplan is ingericht en wordt uitgevoerd.

### 1.1.2 Verantwoordelijkheden

De BORG-A adviseur (hierna de Adviseur) is verantwoordelijk:

- voor het opleveren van beveiligingsplannen die aan de in het certificatieschema gestelde eisen voldoen;
- voor het doorlopen van een geborgd proces dat leidt tot het gecertificeerde beveiligingsplan, inclusief verificatie, validatie en controles;
- voor toepassing van het certificatiemerk volgens de bepalingen in paragraaf 5.1 op alle beveiligingsplannen. Het gecertificeerde beveiligingsplan is herkenbaar aan het certificatiemerk.

#### Toelichting

- De opdrachtgever is verantwoordelijk voor de uitvoering van het gecertificeerde beveiligingsplan. De Adviseur adviseert de opdrachtgever over de uitvoering. Bijvoorbeeld door hem te informeren over BORG-B en BORG-E gecertificeerde bedrijven die de beveiligingsmaatregelen kunnen uitvoeren;
- De opdrachtgever is en blijft verantwoordelijk voor de bedrijfsvaardigheid van de beveiligingsmaatregelen. Onderhoud is een middel om in de continue bedrijfsvaardigheid te voorzien. De Adviseur informeert de opdrachtgever over onderhoud en beheer.

NB: adviezen van de Adviseur buiten het beveiligingsplan vallen niet onder het toezicht van de certificatie-instelling.

### 1.1.3 Leeswijzer

Dit certificatieschema bevat:

- eisen waaraan het beveiligingsplan moet voldoen, hoe dit wordt beoordeeld en wanneer er sprake is van goed- en afkeur van het beveiligingsplan (hoofdstuk 2);
- voorwaarden voor de Adviseur voor het verkrijgen en in stand houden van het productcertificaat (hoofdstuk 3);
- geharmoniseerde werkwijzen die de certificatie-instelling hanteert bij de behandeling van een certificatieaanvraag en de instandhouding van het productcertificaat (hoofdstuk 4);
- de beschrijving van het certificaat dat de certificatie-instelling afgeeft aan de Adviseur en het beveiligingsplan met certificatiemerk dat de Adviseur afgeeft aan de opdrachtgever (hoofdstuk 5).

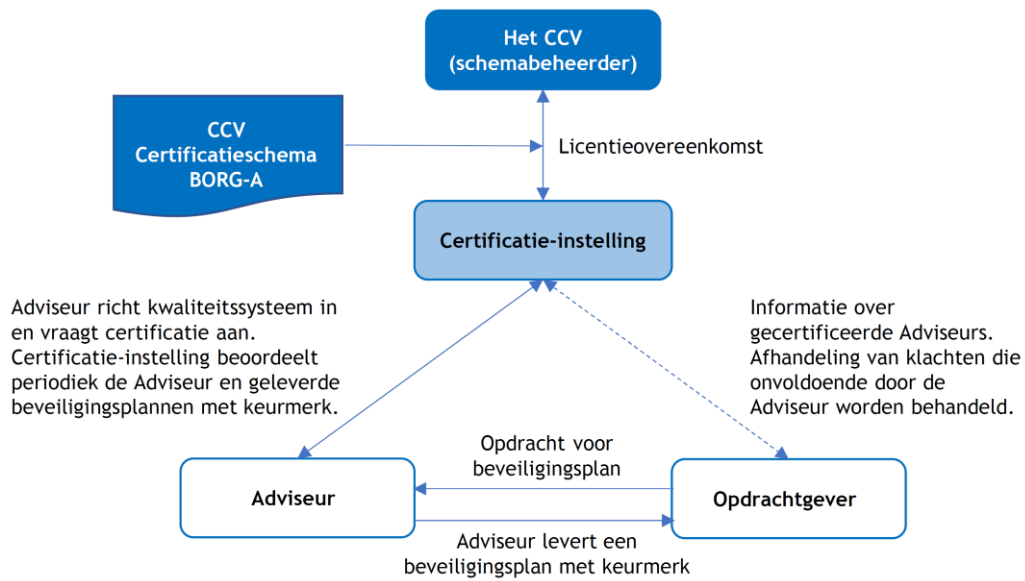
## 1.2 Toepassingsgebied

Het opstellen en leveren van het BORG-A Beveiligingsplan.

## 1.3 Relatie met wet- en regelgeving

Het certificatieschema wordt niet aangestuurd vanuit wet- en regelgeving. Het certificatieschema is privaatrechtelijk en bevat wettelijke eisen.

## 1.4 Relatieschema



Figuur 1 – overzicht van betrokken partijen bij productcertificatie

## 1.5 Overgangsregeling

Er is geen overgangsregeling. Dit certificatieschema is een nieuw schema.

## 2 Eisen aan het product

### 2.1 Algemeen

Alle technische en administratieve eisen waaraan het onder certificaat geleverde beveiligingsplan moet voldoen en de wijze waarop dit wordt beoordeeld, zijn opgenomen in dit hoofdstuk. Als niet aan de eisen in dit hoofdstuk wordt voldaan, is er sprake van afkeur.

### 2.2 Beoordelingsmethoden, eisen, goed- en afkeur

#### 2.2.1 Algemeen

De vorm van het beveiligingsplan conform dit certificatieschema is vrij. Het beveiligingsplan moet aan de in dit hoofdstuk genoemde eisen voldoen.

Voor beoordeling wordt gebruik gemaakt van de verificatiemethoden uit tabel 1.

TABEL 1 – VERIFICATIEMETHODEN	
Methodiek	Omschrijving
Administratief (A)	<ul style="list-style-type: none"> <li>■ A-A: Beoordeling op aanwezigheid</li> <li>■ A-C: Beoordeling op compleetheid</li> <li>■ A-J: Beoordeling op juistheid</li> </ul> <p><u>Noot:</u> als compleetheid (A-C) moet worden getoetst is het document aanwezig (A-A); in dat geval wordt alleen methode A-C vermeld. Als juistheid of conformiteit (A-J) moet worden beoordeeld is het document aanwezig (A-A) en compleetheid (A-C); in dat geval wordt alleen methode A-J vermeld.</p>

#### 2.2.2 Eisen aan het beveiligingsplan

Het beveiligingsplan moet minimaal voldoen aan de eisen in tabel 2.

TABEL 2 – EISEN AAN HET BEVEILIGINGSPLAN			
NR	ONDERWERP	METHODE	EIS
2.1	Locatie en objectbeschrijving	A-C	De locatie en het soort object zijn in voldoende detail beschreven om het beveiligingsplan op te stellen.
2.2	Gebruik	A-C	Het feitelijke/gewenste gebruik van het gebouw/object is in voldoende detail beschreven om het beveiligingsplan op te kunnen stellen.
2.3	Doel van de beveiliging	A-C	De doelstelling van de beveiliging is duidelijk omschreven.
2.4	Uitgangspunten	A-C	De uitgangspunten (bijvoorbeeld wensen van de opdrachtgever, de verzekeraar, etc.) die bij het opstellen van het beveiligingsplan worden aangehouden zijn omschreven.
2.5	Te beveiligen risico	A-C	Het te beveiligen risico is in voldoende detail omschreven om de aard en omvang van de beveiligingsmaatregelen te kunnen kiezen.
2.6	Bepaling van het risico	A-J	De keuze voor de beveiligingsmaatregelen is m.b.v. de VRKI of een andere methodiek bepaald en is gebaseerd op het



TABEL 2 – EISEN AAN HET BEVEILIGINGSPLAN			
NR	ONDERWERP	METHODE	EIS
			<p>geïdentificeerde risico. De bepaling van het risico is op één van genoemde methode in het beveiligingsplan opgenomen:</p> <ul style="list-style-type: none"> <li>■ Volledig of;</li> <li>■ Als bijlage waarnaar in het beveiligingsplan wordt verwezen.</li> </ul> <p>De Adviseur mag een risicoanalyse gebruiken die door een tweede (bijvoorbeeld de opdrachtgever) of derde (bijvoorbeeld de verzekeringsexpert) partij is opgesteld. De Adviseur moet dit in het beveiligingsplan duidelijk vermelden.</p>
2.7	Aard en omvang van de beveiligingsmaatregelen	A-J	<ul style="list-style-type: none"> <li>■ Aard en omvang van de beveiliging zijn vastgelegd, komen overeen met het beoogd gebruik van het object en passen bij de risicoanalyse;</li> <li>■ Van keuzes die gemaakt zijn door derden is getoetst of ze passend, uitvoerbaar en samenhangend zijn bij het beoogde gebruik en kunnen leiden tot een doeltreffende beveiliging;</li> <li>■ Gemaakte keuzes zijn onderbouwd;</li> <li>■ Van gemaakte ontwerpkeuzes die niet zijn aangegeven in de van toepassing zijnde normen/voorschriften/standaarden is voldoende gemotiveerd dat ze leiden tot doeltreffende beveiliging;</li> <li>■ Elke gelijkwaardige oplossing is onderbouwd;</li> <li>■ Van onderwerpen die niet verder zijn uitgewerkt, is de reden daarvan toegelicht;</li> <li>■ De gegevens zijn onderling consistent en er zijn geen conflicterende situaties en/of oplossingen beschreven;</li> <li>■ Aan <u>alle</u> OBESCAR-maatregelen wordt aandacht besteed;</li> <li>■ Alle maatregelen zijn zo uitgewerkt dat de installateur, de aannemer en de opdrachtgever weten wat ze moeten doen. Voorbeeld: van welke grade of weerstandklasse moeten de toegepaste producten zijn en hoe moet de doormelding worden gerealiseerd? Bijvoorbeeld door middel van DP3 of DP4;</li> <li>■ Indien van toepassing: bij het ontwerp van de beveiliging is rekening gehouden met andere brand- en/of beveiligingsvoorzieningen die wederzijds van invloed kunnen zijn;</li> <li>■ Als voor toepassing van de beveiliging organisatorische maatregelen noodzakelijk zijn (bijvoorbeeld protocol in- en uitschakelen, opvolging door hulpdiensten) staat in het plan wie daarvoor verantwoordelijk is.</li> </ul>
2.8	Borging samenhang	A-C	De samenhang van de gekozen maatregelen met het geanalyseerde risico is duidelijk weergegeven.
2.9	Passend bij gebruik	A-J	De gemaakte ontwerpkeuzes m.b.t. de bouwkundige-, installatietechnische- en organisatorische maatregelen in het beveiligde gebied zijn passend voor het beoogd gebruik.
2.10	Kwaliteitsborging	A-A	<ul style="list-style-type: none"> <li>■ Advies over de uitvoering van de maatregelen en de wijze van kwaliteitsborging in de realisatiefase, opleverfase en gebruiksfase (beheer en onderhoud) is in het beveiligingsplan opgenomen.</li> </ul>

TABEL 2 – EISEN AAN HET BEVEILIGINGSPLAN			
NR	ONDERWERP	METHODE	EIS
			<ul style="list-style-type: none"> <li>■ Informatie over beheer en onderhoud is in het beveiligingsplan opgenomen.</li> </ul>
2.11	Geschiktheid en actualiteit van normen en voorschriften	A-J	<ul style="list-style-type: none"> <li>■ De van toepassing verklaarde (delen van) normen/voorschriften zijn geschikt om doeltreffende beveiliging te realiseren.</li> <li>■ In het beveiligingsplan staat duidelijk welke versie van normen, voorschriften en standaarden van toepassing zijn.</li> </ul>
2.12	Verwijzing	A-J	De verwijzing naar andere documenten is consistent en volledig.
2.13	Volledigheid gegevens en identificatie	A-A	<ul style="list-style-type: none"> <li>■ Alle personen en organisaties die betrokken zijn bij het opstellen van het beveiligingsplan staan vermeld;</li> <li>■ Het beveiligingsplan is voorzien van een unieke identificatie, inclusief versienummer en status zoals concept of definitief.</li> </ul>

## 3 Voorwaarden voor certificatie

In dit hoofdstuk staan de voorwaarden waaraan de Adviseur moet voldoen om een gecertificeerd beveiligingsplan te leveren.

### 3.1 Algemeen

De Adviseur moet continu aan de certificatie-instelling kunnen aantonen dat voldaan wordt aan de eisen van kwaliteitsborging (paragraaf 3.2) en aan de voorwaarden bij aanvraag en in stand houden van de certificering (paragraaf 3.3).

De Adviseur voorziet de certificatie-instelling van alle opgevraagde informatie en gegevens. Het niet nakomen hiervan kan leiden tot sancties zoals beschreven in paragraaf 4.9 (schorsing) en 4.10 (intrekking).

### 3.2 Eisen aan het kwaliteitssysteem

Bij productcertificatie gaat het primair om het voldoen aan de eisen zoals beschreven in hoofdstuk 2. Het kwaliteitssysteem<sup>2</sup> heeft hierbij een ondersteunend karakter, gericht op het continu borgen van de kwaliteit van het onder certificaat geleverde beveiligingsplan. In de volgende paragrafen zijn de eisen aan het kwaliteitssysteem verder uitgewerkt.

#### 3.2.1 Organisatie en verantwoordelijkheden

De Adviseur beschikt over een overzicht van de medewerkers<sup>3</sup> van wie het werk van invloed is op de kwaliteit van het te leveren beveiligingsplan.

Indien de organisatie van de Adviseur bestaat uit meer dan één medewerker zijn taken, verantwoordelijkheden en bevoegdheden van deze medewerkers en hiërarchische verbanden vastgelegd. De medewerkers zijn op de hoogte van het kwaliteitssysteem, werken volgens het kwaliteitssysteem en worden geïnformeerd over wijzigingen.

#### 3.2.2 Kwalificaties

##### Algemeen

De kwaliteit van het geleverde werk is sterk afhankelijk van de vakbekwaamheid van het personeel: de juiste mensen moeten het juiste werk doen.

Voor kwalificatie van medewerkers moet de Adviseur een procedure of werkinstructie hebben, en ten minste één medewerker aanwijzen. De medewerker moet voldoen aan de volgende eisen:

---

<sup>2</sup> Inrichting en omvang van het kwaliteitssysteem zijn sterk afhankelijk van o.a. het product of dienst en de omvang van de organisatie. In het algemeen geldt: zo licht als mogelijk en zo zwaar als nodig.

<sup>3</sup> Met medewerkers wordt hier ook ingehuurd personeel bedoeld (zie ook paragraaf 3.2.4).

VERANTWOORDELIJKE VOOR KWALIFICATIE VAN MEDEWERKERS	
Kwalificatie	Door of namens de directie
Niveau	Indien namens de directie: HBO-werk- en denkniveau
Kennis van en kunnen werken met	Dit certificatieschema

De Adviseur stelt van alle medewerkers die betrokken zijn bij taken aangegeven in het certificatieschema vast dat zij aan de kwalificatie-eisen voldoen. Voor het opstellen van beveiligingsplannen wordt uitsluitend gekwalificeerd personeel ingezet.

Kwalificaties worden bijgehouden en geregistreerd. Jaarlijks wordt geëvalueerd of de medewerkers nog steeds aan beschikken over de vereiste kwalificaties. Dit kan bijvoorbeeld op basis van eigen waarnemingen, functioneringsgesprekken, beoordelingsgesprekken, geleverd werk.

### BORG-A adviseur

De Adviseur heeft minimaal één medewerker in vast dienstverband die voldoet aan de kwalificatie-eisen in deze paragraaf.

BORG-A ADVISEUR	
Kwalificatie	Door de verantwoordelijke voor het kwalificeren van medewerkers
Taken	<ul style="list-style-type: none"> <li>■ Het verzamelen van de benodigde informatie over het risico op gerichte inbraak en de omstandigheden waarvoor de beveiliging doeltreffend moet zijn;</li> <li>■ Mondeling en schriftelijk adequaat informeren van de opdrachtgever over (de samenhang van) alle maatregelen in relatie tot het geanalyseerde risico en de consequenties van eventuele keuzes;</li> <li>■ Het opstellen van het beveiligingsplan.</li> <li>■ Het verifiëren of de in het beveiligingsplan beschreven maatregelen ook zijn uitgevoerd.</li> </ul>
Opleiding	TBV (diploma)
Ervaring	<ul style="list-style-type: none"> <li>■ HBO werk- en denkniveau (diploma of assessment);</li> <li>■ Drie jaar relevante werkervaring in het opstellen van beveiligingsplannen.</li> </ul>
Kennis van en kunnen werken met	<ul style="list-style-type: none"> <li>■ Dit certificatieschema</li> <li>■ De Verbeterde Risicoklassenindeling (VRKI)</li> </ul>

De Adviseur moet kunnen aantonen dat medewerkers aan de vereiste kwalificaties voldoen. Voor het aantonen van kwalificaties met behulp van diploma's is de CCV-richtlijn Verificatie diploma's van toepassing.

### Toelichting

De certificatie-instelling gebruikt de CCV-richtlijn Verificatie diploma's om de kwalificatieprocedure van de Adviseur te verifiëren.

Gelijkwaardig aan een diploma TBV is een erkenning van beroepskwalificatie zoals bedoeld in artikel 5 van de Algemene wet erkenning EG beroepskwalificaties, voor werkzaamheden als alarminstallateur. (Zie wijzigingen Regeling particuliere beveiligingsorganisaties en recherchebureaus, 19 juli 2008 Stcrt 5 augustus nr. 149). [wettelijke eis]

### Betrouwbaarheid

Alle medewerkers betrokken bij het ontwerp en de realisatie van een beveiligingsplan zijn in het bezit van een geldige "Verklaring Van Betrouwbaarheid" (VVB) zoals bedoeld in de Wet particuliere beveiligingsorganisaties en recherchebureaus, artikel 10, eerste lid, niet ouder dan drie jaar [wettelijke eis].

Alle overige medewerkers die betrokken zijn bij het BORG-A-proces en/of over de informatie kunnen beschikken (vast of ingehuurd) zijn in het bezit van een geldige 'verklaring omtrent het gedrag' (VOG) zoals bedoeld in de Wet justitiële en strafvorderlijke gegevens, artikel 28. De te toetsen functieaspecten op de VOG zijn passend op de uit te voeren werkzaamheden, maar bevatten minimaal de algemene screeningsprofielen 12, 13 en 41.

#### Toelichting: Algemene screeningsprofielen

- 12 – Met gevoelige/vertrouwelijke informatie omgaan;
- 13 – Kennis dragen van veiligheidssystemen, controlemechanismen en verificatieprocessen;
- 41 – Het verlenen van diensten (advies, beveiliging, schoonmaak, catering, onderhoud etc.)

De VOG wordt afgegeven binnen drie maanden na indiensttreding en mag niet ouder zijn dan drie jaar.

### Werken onder toezicht

Medewerkers in opleiding werken onder toezicht van een medewerker, die voor de betreffende werkzaamheden is gekwalificeerd. De gekwalificeerde medewerker is verantwoordelijk voor de correcte uitvoering van de werkzaamheden.

### Op peil houden van kennis

De Adviseur heeft een aantoonbaar beleid om de kennis van de gekwalificeerde medewerkers over de van toepassing zijnde regelingen en/of methodieken actueel en op peil te houden.

De Adviseur zorgt dat gekwalificeerde medewerkers minimaal één keer in de drie jaar een opfriscursus/training van twee dagdelen volgen om de kennis op peil te houden. Het onderwerp van de opfriscursus/training moet betrekking hebben op de VRKI en ten minste één van de aspecten van het normatief kader OBESCAR. Van de opfriscursus/training moet een bewijs van deelname beschikbaar zijn waarop ten minste zijn vermeld:

- Naam van de organisatie die de verklaring verstrekt;
- Naam van de deelnemer aan de opfriscursus/training;
- Plaats en datum opfriscursus/training of opleiding;
- Het onderwerp waarop de opfriscursus/training betrekking heeft;
- De leerdoelen van de opfriscursus/training;
- De kennisaspecten die behandeld zijn.

### 3.2.3 Uitbesteden

De Adviseur mag werkzaamheden uitbesteden aan een onderaannemer. Hierbij geldt:

- De Adviseur beoordeelt vooraf aan de hand van de eisen in paragraaf 3.2 en de eisen in hoofdstuk 2 of de onderaannemer geschikt is voor het uitvoeren van het specifieke uit te besteden werk.
- Bij positieve conclusie op de beoordeling is en blijft de Adviseur zelf verantwoordelijk voor de kwaliteit van het uitbestede werk en voor het door hem geleverde gecertificeerde beveiligingsplan.
- Indien de onderaannemer de werkzaamheden onder geldige productcertificatie conform het CCV-certificatieschema BORG-A, BORG-B of BORG-E uitvoert, mag de Adviseur aannemen dat de onderaannemer geschikt is voor het uitvoeren van het werk. De omvang en diepgang van het onderzoek van de geschiktheid van de onderaannemer door de Adviseur beperkt zich in dat geval tot verificatie van het productcertificaat van de onderaannemer.
- Personeel dat betrokken is bij het ontwerp van inbraakbeveiliging is in het bezit van een 'verklaring van betrouwbaarheid' (VVB) en/of 'verklaring omtrent het gedrag' (VOG).

### 3.2.4 Inhuur

De Adviseur mag personeel inhuren om de werkzaamheden te verrichten. Hierbij zijn de eisen uit paragraaf 3.2.2 van toepassing.

### 3.2.5 Inkoop en aanleveren

De organisatie maakt aantoonbaar dat in te kopen diensten volgens inkoopspecificatie worden besteld en bij levering tegen inkoopspecificatie worden gecontroleerd. Bij levering of in gebruik nemen van ingekochte of door de afnemer toegeleverde diensten moet de organisatie controleren dat deze voldoen aan de gestelde eisen.

### 3.2.6 Startinformatie en dossier

Voordat de Adviseur kan beginnen met uitvoering van de opdracht moet hij nagaan of hij beschikt over voldoende informatie over het te beveiligen object. Bij aanvang van de werkzaamheden moeten ten minste de volgende gegevens beschikbaar zijn:

- (beoogd) gebruik van het te beveiligen gebouw;
- Specifieke omstandigheden in het gebouw of in het gebruik/leefgewoonten;
- Doel van de beveiliging;
- Gewenste niveau van beveiliging;
- Gewenste beveiligingsmaatregelen en -voorzieningen;
- Indien van toepassing: overige brand- en/of beveiligingsvoorzieningen.

Indien al een risicoanalyse beschikbaar is hoeft de Adviseur deze niet zelf te maken (zie 2.6 in tabel 2 in 2.2.2). De Adviseur moet beoordelen of de risicoanalyse van de tweede of derde partij bruikbaar is voor de opdracht en of andere belanghebbenden daarover zijn geïnformeerd.

Van elke opdracht voor het maken van een beveiligingsplan is een dossier aanwezig. De organisatie is vrij in de wijze waarop het dossier ingericht wordt.

Het dossier moet informatie geven over de volgende onderwerpen:

- Offerte en opdracht;
- Wijzigingen in het proces;
- Gegevens voor het beveiligingsplan en de verificatie hiervan;
- De onderbouwing van keuzes;
- Gelijkwaardige oplossingen en de validatie hiervan;
- Wie eraan gewerkt heeft en wie de eindverantwoordelijkheid heeft.

### Toelichting

Het beveiligingsplan is onderdeel van het dossier. Bovengenoemde onderwerpen kunnen herleidbaar zijn vanuit het beveiligingsplan.

#### 3.2.7 Documentbeheer, registraties en archivering

De Adviseur zorgt voor overzichtelijke archivering van alle gegevens en documenten die betrekking hebben op de eisen zoals gesteld in het certificatieschema. De Adviseur moet toegang hebben tot:

- de documenten genoemd in paragraaf 6.3;
- de schriftelijke procedures en werkinstructies volgend uit het certificatieschema.

De Adviseur houdt deze documenten actueel en informeert zijn medewerkers hierover.

De Adviseur beschikt over de volgende registraties:

- Overzicht van medewerkers<sup>4</sup>, taken, bevoegdheden en verantwoordelijkheden, hiërarchische verbanden (paragraaf 3.2.1);
- Kwalificaties van het personeel (paragraaf 3.2.2);
- Uitbestede werk (paragraaf 3.2.3);
- Klachten (paragraaf 3.2.8);
- Correcties en corrigerende maatregelen (paragraaf 3.2.9);
- Evaluaties (paragraaf 3.2.10);
- Documenten waarin de opdrachten aan de Adviseur zijn vastgelegd (bijvoorbeeld contract, opdrachtbevestiging, eigen registratie van een mondelinge opdracht, e-mail).

De gegevens worden voor een periode van minimaal 5 jaar<sup>5</sup> bewaard. Voor niet meer bestaande objecten is archivering niet langer van toepassing.

De Adviseur zorgt ervoor dat de toegang tot vertrouwelijke (project)gegevens<sup>6</sup> wordt beperkt en beheerd. De gegevens zijn alleen toegankelijk voor eigen personeel die vanuit hun functie toegang tot deze dossiers nodig hebben.

---

<sup>4</sup> Waarmee ook ingehuurd personeel wordt bedoeld (zie paragraaf 3.2.5) en personeel dat de verificatie uitvoert (paragraaf 3.2.10)

<sup>5</sup> In verband met wetgeving kunnen voor bepaalde documenten langere of kortere bewaartermijnen gelden.

<sup>6</sup> Bedoeld wordt gegevens die betrekking hebben op de beveiliging bij de opdrachtgever, zowel in fysieke vorm als digitaal.

### 3.2.7.1 Papieren dossiers

Bij gebruik van papieren dossiers zorgt de Adviseur voor de volgende maatregelen:

- Een inbraakwerende kast of safe klasse CEN 0, conform uitgave Vereniging Geld- en Waardeberging; of
- Een inbraakwerende kast of safe die daaraan gelijkwaardig is; of
- CO<sub>3</sub> of ME<sub>3</sub> conform de VRKI deel B, inclusief bijbehorende EL-maatregelen; of
- Een maatregel: bereikbare buitenschil BK2 inclusief EL3 en CO2.

Externe toegang wordt zoveel mogelijk beperkt.

### 3.2.7.2 Digitale dossiers (opslag op eigen server)

Als dossiers op een eigen server worden opgeslagen, moet de beveiliging voldoen aan dezelfde eisen zoals benoemd bij papieren dossiers (3.2.7.1).

Externe toegang (bijvoorbeeld digitaal onderhoud aan server) wordt uitgevoerd met een beveiligde verbinding met encryptie. Een schriftelijke geheimhouding wordt opgesteld en ondertekend door de externe leverancier.

### 3.2.7.3 Digitale dossiers (opslag in datacenter)

Als dossiers of delen ervan zijn opgeslagen bij een datacenter, dan voldoet het datacenter – middels een geldig certificaat uitgegeven onder accreditatie - aantoonbaar aan ISO27001. Het datacenter is gevestigd:

- Binnen Nederland; of
- Buiten Nederland, maar binnen de Europese Unie en/of Noorwegen, IJsland, Liechtenstein.

#### **Toelichting: Datacenter buiten Nederland, maar binnen EU en/of Noorwegen, IJsland, Liechtenstein**

Het is belangrijk dat de opgeslagen data in het datacenter veilig is. Providers hebben daarin rechten, maar ook plichten. Je wilt niet het risico lopen dat je opgeslagen data in beslag wordt genomen door een buitenlandse regering. Binnen de EU, Noorwegen, IJsland en Liechtenstein is dit gelijkwaardig geregeld en zijn hierover afspraken gemaakt. Buiten de EU is dit niet het geval.

Let op! Het Verenigd Koninkrijk is geen lid van de EU en valt niet binnen de tweede bullet.

Als de externe toegang door de externe leverancier (ICT-bedrijf) wordt ingericht kunnen zij ook bij de digitale dossiers. De Adviseur maakt hierover afspraken (bijvoorbeeld over waar gegevens staan, geheimhouding) met de ICT-leverancier en legt deze schriftelijk vast.

### 3.2.8 Klachten

De Adviseur heeft een schriftelijke procedure voor klachten, klachtanalyse en het nemen van corrigerende maatregelen om herhaling te voorkomen.

De Adviseur bevestigt de ontvangst van een klacht binnen maximaal twee weken schriftelijk aan de klagende partij. De Adviseur handelt de klacht binnen maximaal twee maanden af en stuurt hiervan een schriftelijk bericht aan de klagende partij. In het schriftelijke bericht vermeldt de Adviseur of de klacht terecht is, zo nee waarom niet en zo ja, welke maatregelen de Adviseur heeft genomen of gaat nemen.



### 3.2.9 Herstel en Corrigerende maatregelen

De Adviseur heeft een schriftelijke procedure voor herstel en corrigerende maatregelen. Bij geconstateerde fouten en afwijkingen zorgt de Adviseur naast herstel ook voor corrigerende maatregelen. Corrigerende maatregelen zijn gericht op het voorkomen van het opnieuw optreden van de fout.

### 3.2.10 Evaluatie

De Adviseur kan aantonen dat blijvend aan alle voorwaarden genoemd in dit hoofdstuk (voorwaarden voor certificatie) en hoofdstuk 2 (eisen aan product) wordt voldaan. Daartoe maakt de Adviseur jaarlijks een analyse van:

- De ontvangen klachten en de wijze van afhandeling;
- Het periodiek toetsen van werkzaamheden van uitvoerende medewerkers tegen de voorgeschreven werkwijzen;
- Het periodiek toetsen van het kwaliteitssysteem op een effectieve implementatie (interne audit).

#### Toelichting

Het advies is om voor analyse en evaluatie van de eigen cyberveiligheid gebruik te maken van de Risicoklassenindeling Digitale Veiligheid (RKIDV) van het Digital Trust Center.

#### Toelichting

Een voorbeeld van het periodiek toetsen van het kwaliteitssysteem op een effectieve implementatie is het beoordelen van een of enkele dossiers. Tegelijk kan beoordeling plaatsvinden van kwalificatie van de medewerkers die volgens het dossier aan het project hebben gewerkt.

Bij een Adviseur met slechts één personeelslid en die geen gebruik maakt van ingehuurd personeel mag voor evaluatie bij uitzondering de audit van de certificatie-instelling worden gebruikt.

## 3.3 Voorwaarden bij aanvraag en in standhouden

### 3.3.1 Gegevens bij aanvraag

De Adviseur biedt de certificatie-instelling bij aanvraag de volgende gegevens aan:

- Een bewijs van wettelijke registratie (uittreksel Kamer van Koophandel);
- Een verklaring van een hiertoe bevoegd persoon dat de Adviseur zich zal houden aan de in het certificatieschema genoemde eisen, voorwaarden en verplichtingen;
- De eventuele aanwezigheid van meerdere vestigingen voor het leveren van de inbraakbeveiliging.

De Adviseur voorziet verder de certificatie-instelling op diens verzoek van alle nodige informatie en gegevens (zie paragraaf 4.3).

### 3.3.2 Status gedurende de aanvraag

Tot het moment dat de initiële beoordeling is afgesloten met een positief besluit (zie paragraaf 4.4), is het niet toegestaan enige verwijzing te publiceren naar de aanvraag voor certificatie. In individuele contacten en contracten mag hier wel naar worden verwezen.

### 3.3.3 Bezoeken op locatie

[nog niet van toepassing in dit schema]

### 3.3.4 Planning

De Adviseur voorziet de certificatie-instelling van gegevens over op te stellen beveiligingsplannen en/of opgestelde beveiligingsplannen, zodat de certificatie-instelling haar eigen activiteiten kan inplannen. De mate van detaillering vindt plaats in onderling overleg.

Alle beveiligingsplannen vallen onder toezicht van de certificatie-instelling.

### 3.3.5 Wijzigingen

De Adviseur meldt relevante veranderingen in de organisatie tijdig bij de certificatie-instelling. Het gaat om veranderingen als:

- Fusies en overnames;
- Wijzigingen van de organisatie;
- Wijzigingen in het kwaliteitssysteem, die van invloed zijn op de:
  - kwaliteit van de beveiligingsplannen;
  - borging van de kwaliteit van de beveiligingsplannen;
  - uitvoering van het certificatieschema;
  - Wijzigingen in de inhoud en de status van andere certificaten (voor zover van invloed op uitvoering van het certificatieschema).

# 4 Uitvoering van certificatie

## 4.1 Eisen aan de certificatie-instelling

### 4.1.1 Algemeen

Certificatie-instellingen kunnen certificatiecontracten sluiten met een BORG-A adviseur als zij voor het certificatieschema een licentieovereenkomst<sup>7</sup> hebben met het CCV.

Dit certificatieschema gaat uit van geharmoniseerde uitvoering onder NEN-EN-ISO/IEC 17065. Hierbij geldt dat vanuit de accreditatieorganisatie hieraan verbonden documenten en interpretaties op nationaal en internationaal niveau van toepassing zijn.

Bij de uitvoering van dit certificatieschema hanteert de certificatie-instelling NEN-EN-ISO/IEC 17065 en implementeert deze volledig, aangevuld met de bepalingen uit dit certificatieschema. Waar dit schema geen detaillering geeft, moet de certificatie-instelling zelf de noodzakelijk detaillering implementeren. De certificatie-instelling stelt de schemabeheerder hiervan in kennis door het onderwerp voor harmonisatie in te dienen. Met de schemabeheerder overeengekomen certificatieafspraken moeten worden gevolgd.

Certificatie-instellingen kunnen, voor zover niet strijdig met dit certificatieschema, hun eigen reglementen en procedures voor productcertificatie toepassen. Indien er strijdigheid is met bepalingen uit dit certificatieschema, is dit certificatieschema bindend. In die situatie waarbij er strijdigheid is op uitvoering maar hetzelfde doel wordt nagestreefd is het certificatieschema niet bindend. Voorwaarde hierbij is dat dit schriftelijk tussen het CCV en de certificatie-instelling wordt vastgelegd.

Dit certificatieschema wordt buiten accreditatie uitgevoerd.

### 4.1.2 Kwalificaties

#### 4.1.2.1 Algemeen

Het personeel van de certificatie-instelling wordt gekwalificeerd op basis van de vereiste competenties. Competenties zijn gebaseerd op aantoonbaar “kennen” en “kunnen”.

De certificatie-instelling kan voor het kwalificeren van het personeel betrokken bij de uitvoering van dit certificatieschema aanvullende eisen stellen met betrekking tot diploma's, opleiding, werkervaring om hiermee meer zekerheid te krijgen dat aan de vereiste competenties kan worden voldaan. Het ontslaat de certificatie-instelling niet van de verplichting om op basis van eigen waarnemingen (o.a. waarnemen in het veld, interviews, beoordeling rapporten, collegiale toets) zelf het beeld te vormen dat aan de gestelde competenties wordt voldaan.

De certificatie-instelling stelt voor nieuw te kwalificeren certificatiepersoneel een opleidingsprogramma vast, gericht op het voldoen aan de gestelde competenties.

De certificatie-instelling stelt voor iedere gekwalificeerde medewerker een programma vast voor het monitoren en evalueren van de gestelde competenties. Dit programma wordt actueel gehouden.

---

<sup>7</sup> De modelovereenkomst voor certificatie-instellingen is gepubliceerd op de website van het CCV: [www.hetccv.nl](http://www.hetccv.nl)

Certificatiepersoneel dat direct betrokken is bij certificatiebeoordelingen (auditoren, inspecteurs) wordt minimaal eenmaal per drie jaar gemonitord.

In het certificatieschema zijn de algemene competenties vastgelegd voor auditoren en inspecteurs. De certificatie-instelling moet de competenties in voldoende mate detailleren, passend bij de eigen organisatie om aan de eisen van NEN-EN-ISO/IEC 17065 te voldoen. Dit geldt niet alleen voor de betrokken auditoren, inspecteurs en eventuele vakdeskundigen. Het betreft al het certificatiepersoneel, dat betrokken is bij het certificatieproces. Met het certificatieproces wordt onder meer bedoeld (maar niet beperkt tot):

- behandelen van de aanvraag, offerte;
- kwalificeren van het certificatiepersoneel;
- monitoren van het certificatiepersoneel;
- review van auditrapporten;
- beslissing;
- administratieve verwerking van certificaten;
- behandelen van klachten.

De certificatie-instelling legt het voldoen aan de vereiste competenties van het betrokken personeel vast, inclusief de onderbouwing hiervan.

De certificatie-instelling stelt per betrokken medewerker vast voor welke activiteiten de medewerker ingezet kan worden.

#### 4.1.2.2 Competenties voor uitvoeren van de audit

Voor het uitvoeren van:

- de beoordeling op een effectieve implementatie van het kwaliteitsborgingsysteem (audit);
- de beoordeling van de procedures voor gebruik van het certificatiemerk;

zijn minimaal de volgende kwalificatie-eisen en competenties van toepassing:

- De eisen volgens NEN-EN-ISO/IEC 17021-1 annex A (table of knowledge and skills);
- De eindtermen conform Document 09-220 Technicus Beveiligingsinstallatie – TBV, vigerende versie (*zie hiervoor de desbetreffende functie in paragraaf 3.2.2*);
- Het in bezit zijn van een geldige ‘verklaring van betrouwbaarheid’ (VVB) of Verklaring omtrent Gedrag (VOG), niet ouder dan drie jaar, voor de algemene screeningsprofielen 12, 13 en 41;
- Het kunnen beoordelen en wegen wat de mogelijke effecten van een geconstateerde afwijking zijn;
- Bevindingen en afwijkingen kunnen toelichten en communiceren met de Adviseur;
- De bevindingen en afwijkingen en de weging hiervan eenduidig schriftelijke rapporteren;
- Kennis hebben en het kunnen werken met het certificatieschema.

#### 4.1.2.3 Competenties voor uitvoering van de productgerichte beoordeling

Voor het uitvoeren van:

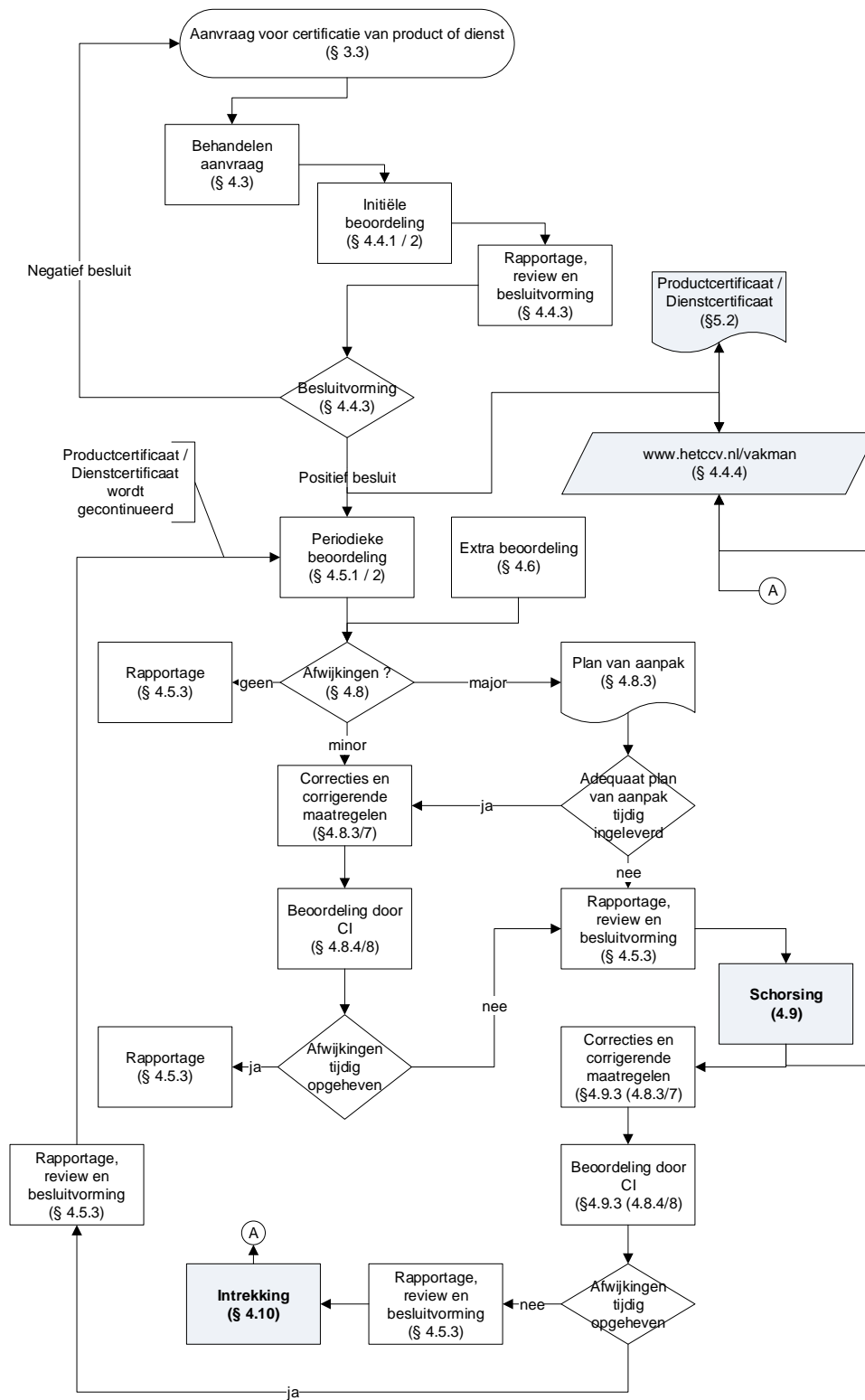
- beoordeling van het opgestelde beveiligingsplan;
- verificatie van projectdossiers;

zijn minimaal de volgende kwalificatie-eisen en competenties van toepassing:

- De eindtermen volgens Document 09-220 Technicus Beveiligingsinstallatie – TBV, vigerende versie (*zie hiervoor de desbetreffende functie in paragraaf 3.2.2*);
- Het in bezit zijn van een geldige 'verklaring van betrouwbaarheid' (VVB) of Verklaring omtrent Gedrag (VOG) niet ouder dan drie jaar voor de algemene screeningsprofielen 12, 13 en 41;
- Het kunnen beoordelen van de opgestelde beveiligingsplannen tegen de eisen gesteld in hoofdstuk 2 van het certificatieschema;
- Het kunnen beoordelen en wegen wat de mogelijke effecten van een geconstateerde afwijking zijn;
- Bevindingen en afwijkingen kunnen toelichten en communiceren met de Adviseur;
- De bevindingen en afwijkingen en de weging hiervan eenduidig schriftelijk kunnen rapporteren;
- Kennis hebben van en kunnen werken met het certificatieschema.

## 4.2 Processchema

Zie schema op volgende pagina.



Figuur 2 – Processchema productcertificatie NEN-EN-ISO/IEC 17065

### 4.3 Behandelen aanvraag

De certificatie-instelling neemt elke aanvraag in behandeling en controleert of alle gegevens bij aanvraag compleet en juist zijn.

De certificatie-instelling vraagt aanvullende gegevens op die nodig zijn voor het behandelen van de aanvraag en het opstellen van een begroting en planning, zoals:

- Gegevens gevraagd in paragraaf 3.3.1;
- Gegevens gevraagd in paragraaf 3.3.4;
- Beschrijving hoe het kwaliteitssysteem ingericht is;
- Gegevens die mogelijk tot een reductie kunnen leiden in de omvang en diepgang van de initiële beoordeling, zoals andere aanwezige certificaten en beschikbare beoordelingsrapporten. De certificatie-instelling beoordeelt in welke mate aanwezige rapporten en certificaten bruikbaar zijn;
- Gegevens voor het correct kunnen beoordelen van een Adviseur met meerdere vestigingen. Een Adviseur met meerdere vestigingen kan zich op twee manieren laten beoordelen:
  - Elke vestiging apart, hierbij wordt elke vestiging als een apart Adviseur gezien met één productcertificaat per vestiging;
  - Als één Adviseur met meerdere locaties/vestigingen. Hierbij is er sprake van één organisatie met één certificatiecontract en één productcertificaat (multi-site beoordeling). De voorwaarden voor multi-site certificatie zijn:
    - De Adviseur heeft een hoofdkantoor en decentrale locaties die alle hetzelfde kwaliteitssysteem toepassen dat vanuit het hoofdkantoor wordt beheerd;
    - Vanuit het hoofdkantoor worden de decentrale locaties hiërarchisch aangestuurd (het is niet nodig dat alle locaties onder dezelfde juridische entiteit vallen);
    - De processen op alle locaties zijn substantieel vergelijkbaar en dezelfde methoden en procedures worden toegepast;
    - Het hoofdkantoor behandelt klachten (zie paragraaf 3.2.8);
    - Het hoofdkantoor ziet erop toe dat corrigerende maatregelen (zie paragraaf 3.2.9) ook worden geïmplementeerd op alle decentrale locaties, waar van toepassing;
    - Het hoofdkantoor betreft bij het uitvoeren van evaluaties (zie paragraaf 3.2.10) ook de decentrale locaties.
- Mogelijk aanwezige schorsing (zie paragraaf 4.9) of intrekking (zie paragraaf 4.10).

De certificatie-instelling behandelt de aanvraag van een certificaathouder met een certificatie-overeenkomst met een andere certificatie-instelling volgens het CCV-reglement Beoordelen overstappende certificaathouder.

Aan de hand van de gedocumenteerde aanvraag voor certificatie stelt de certificatie-instelling een begroting en planning op voor het uitvoeren van de initiële beoordeling en voor het uitvoeren van periodieke beoordelingen. De certificatie-instelling hanteert hierbij de bepalingen in paragrafen 4.4.2 en 4.5.2. De berekende tijden zijn exclusief reis- en rapportagetijd en exclusief de benodigde tijd voor de beoordeling van tekortkomingen.

Variabelen in de berekening van de begroting kunnen zijn: de organisatievorm van de Adviseur, het aantal medewerkers, geografische spreiding, variaties in projecten. De begroting wordt vastgelegd en geaccordeerd, inclusief de onderbouwing hiervan.

De certificatie-instelling informeert de Adviseur over ten minste:

- een begroting van kosten en tijd;

- de eisen en voorwaarden uit dit schema;
- de contractuele/reglementaire voorwaarden van de certificatie-instelling zelf (waaronder het reglement certificatiemerk).

## 4.4 Initiële beoordeling

### 4.4.1 Uitvoering

De initiële beoordeling bestaat uit de volgende onderdelen:

- Verificatie van de gegevens verstrekt bij de aanvraag;
- Verificatie op geldigheid en reikwijdte van andere certificaten (indien relevant);
- Beoordeling op een effectieve implementatie van het kwaliteitssysteem, zie paragraaf 3.2 met de hierin genoemde onderwerpen, inclusief verificatie van kwalificatie van medewerkers aan de hand van de CCV-richtlijn Verificatie diploma's (audit);
- Beoordeling van het voldoen aan de voorwaarden van het certificatieschema, waaronder gebruik van het certificatiemerk;
- Beoordeling van technische voorzieningen (inspectie, indien van toepassing);
- Beoordeling van het opgestelde beveiligingsplan tegen de eisen geformuleerd in paragraaf 2.2.2;
- Beoordeling van corrigerende maatregelen en aantoonbaarheid hiervan (indien van toepassing).

### 4.4.2 Tijdsbesteding en steekproef

#### A. INITIËLE BEOORDELING - AUDIT

Beoordeling kwaliteitssysteem	<p>De certificatie-instelling maakt op basis van de beschikbare gegevens een auditplan(ning) en een auditprogramma voor alle in paragraaf 3.2 genoemde elementen van het kwaliteitssysteem. Als startpunt geldt hierbij de mandagentabel IAF-MD5 voor het uitvoeren van audits, of de eigen mandagentabel voor vergelijkbare bedrijven.</p> <p>De certificatie-instelling kan hierbij kortingen en toeslagen berekenen op basis van (maar niet beperkt tot):</p> <ul style="list-style-type: none"> <li>■ Elementen uit ISO 9001 die niet in het schema voorkomen;</li> <li>■ De aanwezigheid van een ISO 9001 certificaat of andere certificaten en het uitvoeren van de verificatie;</li> <li>■ Het gecombineerd uitvoeren van audits voor andere schema's (ISO 9001, andere CCV schema's, schema's van andere schemabeheerders);</li> <li>■ De organisatievorm;</li> <li>■ De mate waarin en de wijze waarop het kwaliteitssysteem is gedocumenteerd;</li> <li>■ De ervaringen bij het specifieke bedrijf;</li> <li>■ Wel/geen uitbesteding;</li> <li>■ De wijze waarop de controleprocessen (proces – eindcontrole) zijn georganiseerd;</li> <li>■ Interne/externe kalibratie;</li> <li>■ Meerdere vestigingen;</li> <li>■ Geografische spreiding;</li> <li>■ Het aantal medewerkers in dezelfde functie.</li> </ul> <p>De certificatie-instelling zorgt na afloop van de audit voor een evaluatie van de tijdsbesteding ten opzichte van het gestelde doel en stelt waar nodig de</p>
----------------------------------	--



	<p>auditplanning, het auditprogramma en de tijdsbesteding bij, inclusief (indien nodig) een aanvulling op de uitgevoerde audit.</p> <p>De certificatie-instelling zorgt voor een volledige gedocumenteerde onderbouwing van de auditplanning, het auditprogramma, de tijdsbesteding en de aanpassingen hierop ten behoeve van harmonisatieonderzoek door het CCV.</p>
--	---

B. INITIËLE BEOORDELING – PRODUCTGERICHTE BEOORDELING (PER VESTIGING)	
Beveiligingsplan	<p>Twee beveiligingsplannen worden beoordeeld tegen de eisen uit paragraaf 2.2.2.</p> <p>In geval van multi-sitebeoordeling geldt voor de hoofdvestiging twee projecten en één project per nevenvestiging.</p>
Dossier	<p>Van de beoordeelde projecten (zie hierboven) wordt het projectdossier beoordeeld, zodat een compleet en representatief beeld ontstaat over het gehele proces (Beveiligingsplan, procedures, documentatie).</p>

#### 4.4.3 Rapportage, beoordeling en besluitvorming

Elke initiële beoordeling wordt voorzien van een rapportage met alle bevindingen op de punten genoemd in paragraaf 4.4.1.

De certificatie-instelling beoordeelt de rapportage op in ieder geval de compleetheid van de beoordeling, de uitvoering door gekwalificeerd certificatiepersoneel en een correcte procesafloop.

Op basis van deze beoordeling maakt de certificatie-instelling een schriftelijk advies ten behoeve van de besluitvorming door de certificatie-instelling. Alle afwijkingen, geconstateerd tijdens de initiële beoordeling, moeten aantoonbaar zijn opgeheven voordat de certificatie-instelling een positief besluit kan nemen.

#### 4.4.4 Publicatie

Na een positief besluit publiceert de certificatie-instelling de gegevens van de Adviseur bij het betreffende certificatieschema op [www.hetccv.nl/keurmerken/vakman](http://www.hetccv.nl/keurmerken/vakman). Deze website is eigendom van en wordt beheerd door het CCV.

## 4.5 Periodieke beoordeling

### 4.5.1 Uitvoering

De periodieke beoordeling bestaat uit de volgende onderdelen:

- Beoordeling op een effectieve implementatie van het kwaliteitssysteem, zie paragraaf 3.2 met de hierin genoemde onderwerpen, inclusief verificatie van kwalificatie van medewerkers aan de hand van de CCV-richtlijn Verificatie diploma's (audit);
- Beoordeling van het blijvend voldoen aan de voorwaarden van dit certificatieschema, waaronder gebruik van het certificatiemerk;
- Beoordeling primaire processen;
- Beoordeling van technische voorzieningen (inspectie, indien van toepassing);
- Beoordeling van het opgestelde beveiligingsplan tegen de eisen zoals geformuleerd in paragraaf 2.3;

- Beoordeling van corrigerende maatregelen en aantoonbaarheid hiervan (indien van toepassing).

#### 4.5.2 Frequentie, tijdsbesteding en steekproef

De periodieke beoordeling wordt minimaal eenmaal per jaar uitgevoerd. Audits en inspectie(s) kunnen gecombineerd, maar ook gescheiden worden uitgevoerd. De steekproef moet bij voorkeur worden verdeeld over de gehele periode tot de volgende periodieke audit.

##### A. PERIODIEKE BEOORDELING - AUDIT

Beoordeling kwaliteitssysteem	<p>De certificatie-instelling voert de audit uit conform het opgestelde en bijgestelde auditplan(ning) en auditprogramma, zie paragraaf 4.4.2.</p> <p>De certificatie-instelling zorgt na afloop van de audit voor een evaluatie van de tijdsbesteding ten opzichte van het gestelde doel en stelt waar nodig de auditplanning, het auditprogramma en de tijdsbesteding bij, inclusief (indien nodig) een aanvulling op de uitgevoerde audit.</p> <p>De certificatie-instelling zorgt voor een volledige gedocumenteerde onderbouwing van de auditplanning, het auditprogramma, de tijdsbesteding en de aanpassingen hierop ten behoeve van het harmonisatieonderzoek door het CCV.</p> <p>In geval van multi-sitebeoordeling geldt hoofdkantoor ieder jaar en overige locaties minimaal 1 keer per 3 jaar.</p>
-------------------------------	---

##### B. PERIODIEKE BEOORDELING – PRODUCTGERICHTE BEOORDELING (PER VESTIGING)

Beveiligingsplan	<p>Het aantal te beoordelen beveiligingsplannen, tegen alle relevante eisen uit hoofdstuk 2, worden bepaald volgens tabel 1.</p> <table border="1" data-bbox="539 1281 1273 1630"> <thead> <tr> <th colspan="2">TABEL 1</th> </tr> <tr> <th>Aantal beveiligingsplannen</th> <th>Aantal controles</th> </tr> </thead> <tbody> <tr> <td>Tot 3</td> <td>1</td> </tr> <tr> <td>4 t/m 10</td> <td>2</td> </tr> <tr> <td>11 t/m 45</td> <td>3</td> </tr> <tr> <td>46 en meer</td> <td>4</td> </tr> </tbody> </table> <p><i>Tabel controlefrequentie onder certificaat opgestelde beveiligingsplannen</i></p> <p>De certificatie-instelling bepaalt de steekproef. Er zal naar gestreefd worden om de hoogst omschreven beveiligingsklasse te beoordelen.</p> <p>Indien per auditjaar minder dan één beveiligingsplan wordt opgesteld, moet de certificatie-instelling nadere afspraken maken met de Adviseur onder welke voorwaarde het door de certificatie-instelling afgegeven productcertificaat zijn geldigheid blijft behouden. Als de Adviseur maximaal 2 auditjaren achtereen geen gecertificeerd werk levert volgens dit certificatieschema, moet de certificatie-instelling het certificaat intrekken.</p>	TABEL 1		Aantal beveiligingsplannen	Aantal controles	Tot 3	1	4 t/m 10	2	11 t/m 45	3	46 en meer	4
TABEL 1													
Aantal beveiligingsplannen	Aantal controles												
Tot 3	1												
4 t/m 10	2												
11 t/m 45	3												
46 en meer	4												

Dossier (tijdens audit)	Van de beoordeelde projecten (zie hierboven) wordt het projectdossier beoordeeld, zodat een representatief beeld ontstaat over het gehele proces (ontwerp, procedures, documentatie).
-------------------------	---

#### 4.5.3 Rapportage, beoordeling en besluitvorming

De rapportage van een periodieke beoordeling of een extra beoordeling bevatten alle bevindingen van de beoordeling, inclusief de beoordeling van de corrigerende maatregelen voor geconstateerde tekortkomingen. Als de tekortkomingen binnen de hiervoor gestelde termijnen worden opgeheven, moet het rapport een positieve conclusie bevatten over de geconstateerde conformiteit zodat de gecertificeerde status, zonder besluitvorming, gehandhaafd kan blijven.

Wanneer tekortkomingen niet binnen de hiervoor gestelde termijnen worden opgeheven, wordt een tussentijdse rapportage opgesteld met hierin advies voor schorsing van (een deel) van de scope.

Het rapport met advies tot schorsing wordt beoordeeld op onder andere volledigheid van de beoordeling, uitvoering door gekwalificeerd certificatiepersoneel en correcte procesafloop.

## 4.6 Extra beoordeling

De certificatie-instelling kan extra beoordelingen uitvoeren als hiertoe aanleiding is. Aanleidingen kunnen zijn:

- De resultaten van andere beoordelingen;
- Klachten dat het beveiligingsplan waarbij het certificatiemerk is toegepast niet aan de gestelde eisen voldoet;
- Klachten over misleidend of foutief gebruik van het certificatiemerk;
- Publicaties;
- Eigen waarnemingen door de certificatie-instelling;
- Informatie van belanghebbende partijen, zoals de overheid en/of verzekeraars.

Voor de uitvoering, rapportage, beoordeling, besluitvorming en eventuele sancties gelden de bepalingen zoals bij de periodieke beoordeling.

## 4.7 Reductie van tijdsbesteding op basis van andere certificaten

Zie tabel A in paragraaf 4.4.2 respectievelijk paragraaf 4.5.2.

## 4.8 Afwijkingen

Een situatie die niet in overeenstemming is met de eisen wordt beschouwd als een afwijking. Afwijkingen kunnen betrekking hebben op de onder certificaat opgestelde beveiligingsplan en/of op het kwaliteitssysteem. Afwijkingen kunnen worden geclassificeerd als major of minor.

De certificatie-instelling communiceert afwijkingen aan de Adviseur bij het afsluiten van de audit of inspectie.

Bij een Adviseur met meerdere vestigingen die kiest voor multi-site beoordeling (zie paragraaf 4.3) hebben afwijkingen en de consequenties hiervan betrekking op de gehele organisatie.

#### 4.8.1 Major – kwaliteitssysteem

- Eén of meerdere eisen uit het certificatieschema zijn niet geïmplementeerd, of er is sprake van een situatie die, gebaseerd op objectieve waarnemingen, significante twijfel doet rijzen of het kwaliteitssysteem voldoende ondersteuning biedt aan de Adviseur, of
- Bij de laatste beoordeling was dezelfde afwijking vastgesteld, of
- Het niet registreren van klachten en/of het niet opvolgen van klachten, of
- Misbruik van het certificatiemerk, of
- Fraude, misleiding van de certificatie-instelling of het bewust verstrekken van foutieve of onvolledige informatie aan de certificatie-instelling.

#### 4.8.2 Major - product

Het onder certificaat opgestelde beveiligingsplan voldoet niet aan de gestelde eisen waardoor:

- Het beveiligingsplan niet de noodzakelijke informatie beschrijft, of
- Gevaarlijke of onveilige situaties (kunnen) ontstaan.

#### 4.8.3 Major - consequenties

Bij major afwijkingen presenteert de Adviseur een plan van aanpak binnen een door de certificatie-instelling vast te stellen periode van maximaal 7 werkdagen. Gemaakte fouten worden onmiddellijk hersteld. Het plan van aanpak bestaat ten minste uit:

- Een analyse gericht op de grondoorzaak en/of grondoorzaken van de afwijking. In deze analyse komen in elk geval (niet limitatief) de mogelijke oorzaken in het voortbrengingsproces van het beveiligingsplan en de mogelijke oorzaken in het falen van controleprocessen naar voren;
- De te nemen acties die onmiddellijk noodzakelijk zijn om te voorkomen dat meer beveiligingsplannen die niet aan de eisen voldoen met certificatiemerk worden geleverd;
- Een analyse gericht op de geleverde beveiligingsplan sinds de laatste beoordeling door de certificatie-instelling die mogelijk niet aan de gestelde eisen voldoet en op de mate waarin de geanalyseerde grondoorzaken geleid hebben tot (niet eerder) geconstateerde afwijkingen;
- Te nemen acties voor het herstellen of repareren van alle geleverde beveiligingsplannen die niet aan de eisen voldoen;
- Oplossingen gericht op het voorkomen van herhaling en het borgen hiervan;
- De beoordeling van de doeltreffendheid van de implementatie van deze oplossingen (bijvoorbeeld met een interne audit).

De Adviseur documenteert de volgens het plan van aanpak uit te voeren corrigerende maatregelen volledig, zodat deze door de certificatie-instelling verifieerbaar zijn. De termijn voor het uitvoeren van het plan van aanpak bedraagt maximaal drie maanden.

#### 4.8.4 Major - Beoordeling door de certificatie-instelling

De certificatie-instelling beoordeelt binnen een periode van ten hoogste 7 werkdagen na de afgesproken datum van ontvangst het plan van aanpak op doelmatigheid en doeltreffendheid in relatie tot de geconstateerde afwijking.

De certificatie-instelling beoordeelt binnen vier maanden na vaststelling van de afwijking de uitvoering van de correcties en de implementatie van de corrigerende maatregelen<sup>8</sup> om vast te stellen dat de afwijking is opgeheven. De wijze van beoordelen is afhankelijk van de aard van de afwijkingen, en is gebaseerd op de onderdelen genoemd in paragraaf 4.5.1. Zo nodig wordt een extra beoordeling uitgevoerd ter verificatie.

De certificatie-instelling kan eenmalig, met onderbouwing hiervan, de termijn voor correcties en corrigerende maatregelen verlengen met een periode van drie maanden.

#### 4.8.5 Minor – kwaliteitssysteem

- Een situatie die, gebaseerd op objectieve waarnemingen, twijfel doet rijzen over de borging van de kwaliteit van het gecertificeerde beveiligingsplan, of
- Het ontbreken van, het niet hebben geïmplementeerd of niet in stand hebben gehouden van één van de eisen uit het certificatieschema, hetgeen niet heeft geleid tot een major afwijking, of
- Het niet in stand hebben gehouden van één of meerdere voorwaarden uit dit certificatieschema (waaronder financiële verplichtingen en het reglement voor gebruik van het certificatiemerk).

#### 4.8.6 Minor - product

- De onder certificaat geleverde beveiligingsplan voldoet niet aan de gestelde eisen, hetgeen niet heeft geleid tot een major afwijking, of
- Een situatie die, gebaseerd op objectieve waarnemingen twijfel doet rijzen over de kwaliteit van de onder certificaat geleverde beveiligingsplan

#### 4.8.7 Minor - consequenties

De Adviseur krijgt drie maanden de tijd om corrigerende maatregelen te nemen. De corrigerende maatregelen moeten ten minste bestaan uit:

- Een analyse gericht op de grondoorzaak en/of grondoorzaken van de afwijking. In deze analyse komen in elk geval (niet limitatief) de mogelijke oorzaken in het voortbrengingsproces van het beveiligingsplan en de mogelijke oorzaken in het falen van controleprocessen naar voren;
- Een analyse gericht op de omvang van de geleverde beveiligingsplan sinds de laatste beoordeling door de certificatie-instelling die mogelijk niet aan de gestelde eisen voldoen, en de mate waarin de geanalyseerde grondoorzaken geleid hebben tot (niet eerder) geconstateerde afwijkingen;
- Te nemen actie voor het herstellen en/of repareren van alle geleverde beveiligingsplannen die niet aan de eisen voldoen;
- Oplossingen gericht op het voorkomen van herhaling en het borgen hiervan;
- De beoordeling van de doeltreffendheid van de implementatie van deze oplossingen (bijvoorbeeld met een interne audit).

De Adviseur documenteert de uit te voeren corrigerende maatregelen volledig, zodat deze door de certificatie-instelling verifieerbaar zijn.

---

<sup>8</sup> Deze termijn van drie maanden is hetzelfde bij major afwijkingen als bij minor afwijkingen (zie paragraaf 4.8.6).

Indien er sprake is van een schorsing is het aan te bevelen de beoordeling niet gelijktijdig uit te voeren maar te splitsen zodat de schorsing zo snel mogelijk opgeheven kan worden.

#### 4.8.8 Minor - Beoordeling door de certificatie-instelling

Om vast te stellen dat de afwijking is opgeheven, beoordeelt de certificatie-instelling binnen vier maanden na vaststellen van de afwijking de uitvoering van de correcties en de implementatie van de corrigerende maatregelen. De wijze van beoordelen is afhankelijk van de aard van de afwijkingen en is gebaseerd op de onderdelen genoemd in paragraaf 4.5.1. Zo nodig wordt een extra beoordeling uitgevoerd ter verificatie.

De certificatie-instelling kan eenmalig, met onderbouwing hiervan, de termijn voor correcties en corrigerende maatregelen verlengen met een periode van drie maanden.

## 4.9 Schorsing

### 4.9.1 Schorsen

De Adviseur wordt geschorst:

- Bij het niet tijdig aanleveren van een plan van aanpak bij het vaststellen van een major afwijking (zie paragraaf 4.8.3), of
- Bij een plan van aanpak dat onvoldoende borgt dat correcties worden uitgevoerd en/of dat onvoldoende borging biedt voor de uitvoering van de oorzaakanalyse en implementatie van corrigerende maatregelen (zie paragrafen 4.8.3 en 4.8.7), of
- Als de corrigerende maatregelen voor zowel major als minor afwijkingen binnen de gestelde (verlengde) termijn niet hebben geleid tot het opheffen van de afwijking(en) (zie paragrafen 4.8.3 en 4.8.7), of
- Bij het niet voldoen aan de voorwaarden voor certificatie (waaronder de financiële verplichtingen en verplichtingen inzake het gebruik van het certificatiemerk) (zie paragraaf 3.1);
- Als de Adviseur over een periode van maximaal twee jaar geen beveiligingsplannen heeft geleverd;
- Als de Adviseur de belangen en het imago van het certificatieschema, de certificatie-instelling en of het CCV schaadt.

De certificatie-instelling documenteert het advies van de beoordelaar, de beoordeling en besluitvorming en de beslissing volledig, inclusief de onderbouwing.

De certificatie-instelling informeert de Adviseur over de schorsing per aangetekend schrijven of per e-mail met ontvangstbevestiging.

### 4.9.2 Consequenties van schorsing

De certificatie-instelling publiceert de schorsing op [www.hetccv.nl/keurmerken/vakman](http://www.hetccv.nl/keurmerken/vakman).

Vanaf het moment van schorsing mag de Adviseur het certificatiemerk niet gebruiken. Ook mag de Adviseur niet verwijzen naar de gecertificeerde status van het te leveren beveiligingsplan.

De Adviseur blijft bij een schorsing verantwoordelijk voor het verhelpen van gebreken aan het beveiligingsplan waarbij het certificatiemerk is toegepast.

### 4.9.3 Opheffen van de schorsing

Als de certificatie-instelling vaststelt dat alle geconstateerde afwijkingen opgeheven zijn, wordt de schorsing opgeheven. De certificatie-instelling stelt de Adviseur hiervan schriftelijk op de hoogte en maakt de publicatie over schorsing ongedaan.

Vanaf de datum die door de certificatie-instelling schriftelijk is vermeld, is het gebruik van het certificatiemerk weer toegestaan. Een schorsing duurt maximaal zes maanden.

## 4.10 Intrekking

### 4.10.1 Intrekken

Het certificaat wordt ingetrokken indien de Adviseur niet in staat is de geconstateerde afwijkingen binnen de periode van schorsing op te heffen.

De certificatie-instelling informeert de Adviseur over de intrekking per aangetekend schrijven, of per e-mail met ontvangstbevestiging.

### 4.10.2 Consequenties van intrekking

Vanaf het moment van intrekking mag de Adviseur het certificatiemerk niet gebruiken, of verwijzen naar de gecertificeerde status van het te leveren beveiligingsplan. De certificatie-instelling verwijdert de gegevens van de Adviseur bij het betreffende certificatieschema op [www.hetccv.nl/keurmerken/vakman](http://www.hetccv.nl/keurmerken/vakman).

De Adviseur blijft bij intrekking verantwoordelijk voor het verhelpen van gebreken aan het beveiligingsplan waarbij het certificatiemerk is toegepast.

De certificatie-instelling heeft de bevoegdheid om – indien de Adviseur hierin nalatig is – correctieve maatregelen te nemen, zoals het informeren van afnemers. De kosten hiervan kunnen bij de Adviseur waarvan het productcertificaat is ingetrokken in rekening worden gebracht.

### 4.10.3 Nieuwe aanvraag

Een Adviseur waarvan het certificaat is ingetrokken, kan zich weer aanmelden voor een initiële beoordeling volgens het certificatieschema (zie paragraaf 4.4).

# 5 Certificaat en certificatiemerk

## 5.1 Certificatiemerk

Het certificatiemerk, verder te noemen 'het merk', is het bewijs voor afnemers dat de certificatie-instelling een gerechtvaardigd vertrouwen heeft dat de Adviseur een beveiligingsplan levert dat voldoet aan de gestelde eisen in het certificatieschema (zoals beschreven in hoofdstuk 2) en waarbij aan de contractuele en reglementaire voorwaarden is voldaan. Het merk is uitgevoerd als woord/beeldmerk, zie paragraaf 5.1.1.

Uitsluitend het gebruik van het merk beschreven in het certificatieschema is toegestaan.

### 5.1.1 Woord/Beeldmerk

Aan dit certificatieschema is onderstaand afgebeeld beeldmerk verbonden.



Het merk aangebracht op het beveiligingsplan duidt aan dat het vertrouwen gerechtvaardigd is dat op basis van het beveiligingsplan doeltreffende inbraakbeveiliging kan worden gerealiseerd.

### 5.1.2 Gebruik van het merk

De belangrijkste voorwaarden voor het gebruik zijn:

- De certificatie-instelling heeft een geldige licentie bij het CCV;
- De Adviseur heeft een geldig certificatiecontract en is niet geschorst;
- De Adviseur heeft zich ervan vergewist dat het product aan de gestelde eisen voldoet;
- Het illustratief gebruik op briefpapier, website, folders en andere publiciteitsuitingen bij verwijzingen naar het certificatieschema, door de certificatie-instelling is toegestaan onder voorwaarden, zoals aangegeven in het reglement;
- Het illustratief gebruik op briefpapier, website, folders en andere publiciteitsuitingen bij verwijzingen naar het certificatieschema, door de Adviseur is toegestaan onder voorwaarden, zoals aangegeven in het reglement.

De wijze waarop het merk op beveiligingsplannen wordt gebruikt, wordt van tevoren met de certificatie-instelling afgestemd. Het gebruik van het merk is verplicht, zie ook paragraaf 1.1.2.



## 5.2 Productcertificaat

Het productcertificaat wordt opgesteld in de huisstijl van de certificatie-instelling. De Adviseur mag zich profileren als "BORG-A adviseur". Het productcertificaat bevat minimaal de volgende gegevens:

- NAW gegevens van de certificatie-instelling;
- NAW gegevens van de certificaathouder (correspondentieadres);
- De teksten en certificatiemerk:

*"<certificatie-instelling> verklaart dat op grond van beoordelingen door <certificatie-instelling> het vertrouwen gerechtvaardigd is dat een door [naam Adviseur] geleverde beveiligingsplan voldoet aan de eisen gesteld in het CCV-certificatieschema BORG-A, versie <nummer>."*

*"<certificatie-instelling> geeft het hier afgebeelde certificatiemerk in licentie aan <Adviseur> voor de onder certificaat geleverde beveiligingsplannen."*



- Datum van uitgifte / vervanging;
- Eventueel de oorspronkelijke uitgiftedatum;
- (Digitale) handtekening (met naam en functie);

### Toelichting: Digitale handtekening

Een digitale handtekening is een elektronische variant van een handgeschreven handtekening. Een digitale handtekening bestaat uit elektronische gegevens die zijn vastgehecht aan een digitaal document.

- Het bedrijfslogo van de certificatie-instelling;
- Een uniek certificatienummer;
- De tekst:

*"Afnemers van beveiligingsplannen en derden kunnen de status van een geldig productcertificaat nagaan bij <certificatie-instelling> of op [www.hetccv.nl/keurmerken/vakman](http://www.hetccv.nl/keurmerken/vakman). Dit certificaat blijft eigendom van <certificatie-instelling>."*

## 5.3 Beveiligingsplan met certificatiemerk

Gebruik van het merk is verplicht (zie onder paragraaf 1.1.2).

De Adviseur plaatst het merk op elke versie van het beveiligingsplan. De status van elke versie (concept, definitief) moet duidelijk herkenbaar zijn. De opmaak van het document is zodanig dat het duidelijk is dat het een beveiligingsplan betreft.

## 6 Verwijzingen

### 6.1 Wet- en regelgeving

- Wet particuliere beveiligingsorganisaties en recherchebureaus (Staatsblad 1997, 500) (**Wpbr**);
- Regeling particuliere beveiligingsorganisaties en recherchebureaus met Bijlagen (**Rpbr**);
- Toelichtingen op de regeling particuliere beveiligingsorganisaties en recherchebureaus zoals opgenomen in de Staatscourant of op [wetten.overheid.nl](http://wetten.overheid.nl).

### 6.2 Begrippen en afkortingen

Adviseur	Organisatie die het beveiligingsplan levert (BORG-A adviseur).
Afnemer	Persoon of organisatie die het beveiligingsplan afneemt en de Adviseur opdracht geeft voor het opleveren van het beveiligingsplan.
Audit	Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijs en het objectief beoordelen daarvan om vast te stellen in welke mate aan overeengekomen auditcriteria is voldaan.
Beoordeling	Uitvoering van dit certificatieschema door de certificatie-instelling bij de Adviseur.
Beveiligingsplan	In het beveiligingsplan legt de BORG-A adviseur de voorgenomen beveiligingsmaatregelen en de voor beveiliging relevante informatie vast.
CCV	Centrum voor Criminaliteitspreventie en Veiligheid.
Certificatiemerk	Woord- of beeldmerk dat wordt gebruikt om conformiteit met de gestelde eisen aan te geven.
Certificatieschema	Stelsel van regels, procedures en beheeraspecten voor het uitvoeren van certificatie beoordelingen.
Commissie van Belanghebbenden (CvB)	De commissie binnen het CCV waar het draagvlak voor het schema wordt bepaald en die het CCV adviseert over (wijzigingen in) het certificatieschema. In deze commissie zijn belanghebbende en betrokken partijen vertegenwoordigd.
Eisende partij	Partij die een beveiligingsplan met BORG-A-keurmerk vereist. Denk hierbij aan verzekeraar, opdrachtgever, eigenaar/gebruiker.
EN	Europese Norm, uitgegeven door CEN of CENELEC (European Committee for (Electrotechnical) Standardization).
Initiële beoordeling	Beoordeling die leidt tot besluitvorming over afgifte van het productcertificaat.

ISO	International Organization for Standardization, dit is een Internationale norm die wordt uitgegeven door ISO.
NAW-gegevens	Gegevens die betrekking hebben op naam, adres en woonplaats.
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut. Het NEN geeft normen uit.
Norm	Document waarin door betrokken partijen afspraken zijn vastgelegd met het doel zich daaraan te houden.
OBESCAR	Organisatorische maatregelen, Bouwkundige maatregelen, Elektronische maatregelen, Signalering, Compartimentering, Alarmering, Reactie.
Periodieke beoordeling	Beoordeling gericht op bevestiging dat nog steeds aan de eisen en voorwaarden wordt voldaan.
Productgerichte beoordeling	Beoordeling door de certificatie-instelling van het geleverde beveiligingsplan.
Productcertificaat	Document dat de certificatie-instelling opstelt, en waarop de Adviseur wordt vermeld als leverancier van het gecertificeerde beveiligingsplan.
Risico	Een mogelijke gebeurtenis die schade of verlies kan toebrengen. Risico wordt bepaald op basis van de waarschijnlijkheid van een bedreiging, de kwetsbaarheid voor die bedreiging, en de impact indien de bedreiging zich voordoet.
TBV	Technicus Beveiligingsinstallaties.
VOG	Verklaring Omtrent Gedrag.
VRKI	Verbeterde Risico Klasse Indeling.  Een instrument om op basis van attractiviteit bij diefstal na inbraak een samenhangend pakket aan beveiligingsmaatregelen te bepalen (deel A) en een beschrijving hoe deze beveiligingsmaatregelen uitgevoerd moeten worden (deel B).
VVB	Verklaring Van Betrouwbaarheid.

### 6.3 Normen en verwijzingen

De normen en documenten in onderstaande tabel zijn van toepassing voor dit certificatieschema. Het versienummer is bindend (statische verwijzing). Bij een dynamische verwijzing is de versie van toepassing, met de overgangstermijnen, zoals die door de beheerder van het document wordt aangegeven.

Deze normen en documenten zijn normatief, tenzij in dit schema aangegeven is dat het indicatieve verwijzing betreft. Er kan ook normatief of indicatief naar delen van een norm of document worden verwezen, waarbij dan de overige delen van deze norm of dit document voor dit schema geen betekenis hebben. In deze normen en documenten genoemde andere normen of documenten zijn van toepassing, zoals hierin aangegeven.

Een certificatie-instelling beschikt over alle normatieve normen en documenten. De Adviseur beschikt tenminste over de normen en documenten die met een \* zijn gemarkeerd.

NEN-NORMEN		
NEN-EN-ISO/IEC 17065	Conformiteitsbeoordeling – Eisen voor certificatie-instellingen die certificaten toekennen aan producten, processen en diensten	NEN, Delft
NEN-EN-ISO 17021-1	Conformiteitbeoordeling - Eisen voor instellingen die audits en certificatie van managementsystemen uitvoeren	NEN, Delft

REGLEMENTEN		
Merkgebruik	Handleiding gebruik beeldmerk BORG	* Website CCV
Overstappen als certificaathouder	Reglement beoordelen overstappende certificaathouder	Website CCV
Verificatie Diploma's	Richtlijn Verificatie Diploma's	Website CCV

DOCUMENTEN EN RICHTLIJNEN		
VRKI(vigerende versie)	<ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> VRKI deel A</li> <li><span style="color: #0070C0;">■</span> VRKI deel B</li> <li><span style="color: #0070C0;">■</span> VRKI Samenvatting</li> </ul>	* Website CCV

# Bijlage 1 - Toelichting beveiligingsplan

## B1.1 Inleiding

Deze bijlage geeft een toelichting op de onderwerpen die moeten worden behandeld in het beveiligingsplan. Het beveiligingsplan bevat minimaal alle onderwerpen die in paragraaf 2.2.2 zijn vermeld. De wijze waarop dit is ingevuld en de mate van detaillering is afhankelijk van de situatie. De vorm van het beveiligingsplan is vrij. De hierna gegeven volgorde van onderwerpen is niet verplicht maar kan als richtinggevend dienst doen. Daarnaast kan een beveiligingsplan uit één of meerdere documenten bestaan.

De toelichting is ingericht op de meest complexe situatie. Afhankelijk van de situatie is het niet altijd nodig elk onderdeel volledig uit te werken en/of op te nemen in het beveiligingsplan. Uit het beveiligingsplan blijkt middels een onderbouwing, waarom er geen nadere invulling aan de onderwerpen gegeven wordt.

Keuzes die in een eerder stadium gemaakt zijn kunnen worden overgenomen. Hierbij moet worden nagegaan of deze passend en uitvoerbaar zijn bij het geconstateerde risico. Uit het beveiligingsplan blijkt dat risico's zijn geïdentificeerd en dat hiervoor passende en uitvoerbare maatregelen genomen zijn, waarmee voldaan wordt aan de eisen van de opdrachtgevers en kader stellende partijen.

## B1.2 Projectinformatie en doel

De gegevens in dit hoofdstuk hebben betrekking op het document zelf. Hierin worden geen objectgegevens opgenomen.

### B1.2.1 Aanleiding van het beveiligingsplan

Wat is de aanleiding om het beveiligingsplan op te stellen? Zijn er achtergronden die belangrijk zijn om te vermelden?

#### Bijvoorbeeld

- geef een korte introductie van de opdrachtgever;
- realisatie nieuw bouwwerk of gewijzigd gebruik van een bouwwerk;
- nieuwe polis verzekering.

### B1.2.2 Betrokken partijen

Welke relevante partijen, (organisatie en contactpersonen), zijn betrokken bij de totstandkoming van het document? In welke rol zijn zij betrokken?

De betrokken partijen kunnen onder andere bestaan uit:

- Opdrachtgever;
- Gebouweigenaar, gebruiker van een pand;
- Projectontwikkelaar of architect;
- Verzekeraar;
- Opsteller van het beveiligingsplan;

- BORG B/E bedrijf.

Er moet worden aangegeven welke partijen betrokken zijn en wat hun rol en belang in het proces is. Als borging van de uitgangspunten moet het beveiligingsplan worden ondertekend door de opdrachtgever, eisende partij(en) en de Adviseur.

Het beveiligingsplan is een opdracht tussen opdrachtgever en de BORG-A adviseur. De Adviseur maakt op basis van de analyse een plan. Het is aan de opdrachtgever om aan de Adviseur eventuele eisen (bijvoorbeeld van een verzekeraar) door te geven. Als het beveiligingsplan klaar is kan de verzekeraar beoordelen of hij, als het plan wordt uitgevoerd, het risico wil verzekeren.

Het is geen taak van de Adviseur (maar van de opdrachtgever) om te zorgen dat de verzekeraar hierbij betrokken wordt.

### B1.2.3 Doel van het beveiligingsplan

In deze paragraaf wordt de doelstelling van het beveiligingsplan beschreven. Je beschrijft wat er in het rapport wordt uitgewerkt. Wat is de adviesvraag? Waar wordt het beveiligingsplan voor gebruikt? Is het een document voor een verzekeraar? Of voor de opdrachtgever, is het de basis voor certificering? Of een combinatie?

### B1.2.4 Uitgangspunten van het beveiligingsplan

In deze paragraaf worden de uitgangspunten van het beveiligingsplan vastgelegd. Denk hierbij aan:

- Afspraken tussen eigenaar/gebruiker/verzekeraar;
- Certificering;
- Wensen van de opdrachtgever;
- Gegevens, zoals tekeningen, gespreksverslagen, rapporten, lijsten, etc. die zijn gebruikt;
- (On)mogelijkheden van maatregelen (bijvoorbeeld vanuit beperkingen vanuit de Algemene Plaatselijke Verordening (APV)).

#### Opmerking

- Let op: de APV kan bepalingen bevatten over de toepassing van bijvoorbeeld rolluiken;
- Let op: leg hier de concrete eisen, aangegeven door de opdrachtgever, die de verzekeraar heeft gesteld vast.

### B1.2.5 Versiebeheer

Zorg dat het document actueel wordt gehouden en dat betrokken partijen op de hoogte blijven van gewenste of noodzakelijke wijzigingen in het document. De volgende punten worden minimaal in het document vastgelegd:

- Versienummer en datum;
- Wie heeft het plan gewijzigd;
- Waar gaat de wijziging over (geef een korte beschrijving).

Neem een overzicht op van de verschillende versies met wijzigingen in hoofdlijnen.

### B1.2.6 Geldigheid van het document

Omschrijf in deze paragraaf dat het beveiligingsplan een momentopname is. Het is opgesteld voor het op dat moment geconstateerde risico. Wijzigingen in bijvoorbeeld risicofactoren - (waarde, attractieve goederen, gebouwgebruik) - kunnen gevolgen hebben voor de genomen maatregelen.

### B1.2.7 Leeswijzer

Hoe is het document opgebouwd? Hoe moet het worden gelezen? Voor wie is het document bestemd.

## B1.3 Omschrijving object en gebruik

Dit hoofdstuk beschrijft het object. Neem hier minimaal de gegevens m.b.t. paragraaf B1.3.1 t/m B1.3.4 in op.

### B1.3.1 Locatie

Het gaat om de naam van het object, adres, kadastrale ligging, etc. Tevens wordt beschreven hoe het object is gelegen ten opzichte van zijn omgeving. Welke omgevingsfactoren kunnen van invloed zijn op het object? Er zijn omgevingsfactoren, die van invloed kunnen zijn op het te beveiligen object, maar waar je geen invloed op kan uitoefenen (bijvoorbeeld zaken in de openbare ruimte zoals verlichting, parkeergelegenheid, andere risicovolle objecten etc.). Het is belangrijk dat deze omgevingsfactoren wel in het beveiligingsplan worden benoemd.

### B1.3.2 Omschrijving soort object

Deze paragraaf wordt gebruikt voor een algemene beschrijving van het object. Het gaat hier met name om gegevens, zoals:

- Soort bedrijf
- Indeling
- Aantal verdiepingen
- Afmetingen: (gebruiks)oppervlakten, hoogte
- Materialisatie
- Bijzondere kenmerken

### B1.3.3 Gebruik object

Welk gebruik kent het object? Welke goederen zijn er aanwezig?

Specificeer het gebruik. Dit moet per bouwdeel of bouwlaag gebeuren indien er meerdere soorten gebruik plaatsvinden. Welke vorm van productie of opslag vindt plaats? Beschrijf in welke delen van een object welke productie of opslag plaatsvindt. Neem de relevante gegevens op.

### B1.3.4 Omschrijving attractieve en/of risicovolle zaken

Omschrijving van welke attractieve en/of risicovolle zaken er zijn die van invloed (kunnen) zijn op het uiteindelijke beveiligingsniveau. Benoem de attractieve en/of risicovolle zaken (door klant te specificeren en aan te leveren). Vanuit de VRKI wordt uitgegaan van attractief in de zin van aantrekkelijk voor diefstal en na inbraak, verhandelbaar en makkelijk mee te nemen. In dit geval is attractief risicovol. Echter vanuit de totale beveiligingsfilosofie is risicovol niet altijd attractief. Denk hierbij aan een productiemachine. Deze is niet eenvoudig mee te nemen, maar kan wel worden gesaboteerd waardoor een productieproces voor langere tijd stil ligt.

## B1.4 Herkomst uitgangspunten

In dit hoofdstuk wordt weergegeven waar uitgangspunten vandaan komen. Hierin wordt ten minste aandacht besteed aan risicoanalyse en evaluatie van de risicoanalyse.

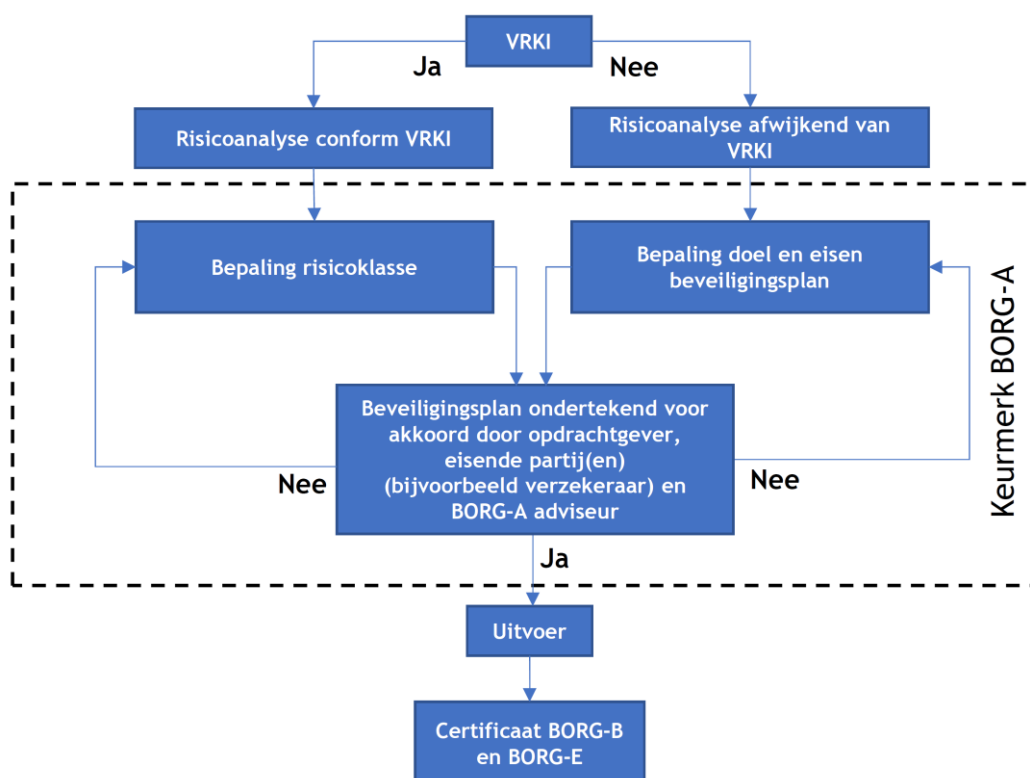
### B1.4.1 Algemeen

Uitgangspunten bestaan uit door diverse betrokken partijen geformuleerde eisen. De gehanteerde methode voor het bepalen van de herkomst van de eisen moet benoemd worden. Aangegeven moet worden wat het toetsingskader is.

Het toetsingskader kan bestaan uit:

- Risicoanalyse conform VRKI en/of;
- Risicoanalyse afwijkend van de VRKI.

Een schematisch beslismodel over het toe te passen toetsingskader ziet er als volgt uit.



Figuur B1 – Schematisch overzicht BORG-A

### B1.4.2 Risicoanalyse conform VRKI

Uiteenzetting in welke risicoklasse het object conform de VRKI ingeschaald wordt. Het zwaartepunt van de beveiliging wordt hierbij bepaald. Indien het object wordt gesplitst in meerdere deelobjecten met ieder zijn eigen risicoklasse, (partiele beveiliging), dit hier duidelijk uiteenzetten (indien nodig plattgrond toevoegen of naar verwijzen). Het kan zijn dat de beveiligingsmaatregelen conform de geconstateerde risicoklasse niet passen bij het object, waardoor er afgeweken gaat worden van de VRKI. Zie figuur B1. Er moet dan worden gekozen voor de route afwijkend VRKI zie paragraaf B1.4.3.

#### B1.4.2.1 Combinaties van niveau beveiligingsmaatregelen

De Adviseur beschrijft welke combinatie van beveiligingsmaatregelen het best van toepassing is (met motivatie). De combinatie moet zo gekozen worden dat het totaal aan beveiligingsmaatregelen overeenkomt met de geconstateerde risicoklasse en moet passend en uitvoerbaar zijn voor het object.



- Combinaties met BK2 zijn de basis voor elk te beveiligen object aan de buitenschil. Daar waar BK2 niet haalbaar is kan worden uitgeweken naar BK1, dit is op een eenduidige manier omschreven;
- Combinaties met BK3 en BK4 zijn niet of nauwelijks haalbaar en zijn primair bedoeld voor compartimenten. Als wel gekozen wordt voor deze combinaties moet rekening worden gehouden met de haalbaarheid hiervan en moet men zich realiseren dat er geattesteerde gevelelementen en bijvoorbeeld P5A glas geplaatst moet worden.

#### B1.4.2.2 Risicoklasse 4 en maatwerk.

Indien met goedkeuring van partijen voor een deel van de beveiliging wordt afgeweken van de standaard beveiligingsmaatregelen voor risicoklasse 4, omdat dit praktisch en/of economisch niet mogelijk is, dient hier gemotiveerd de afwijking beschreven te worden. Ook dient aangegeven te worden hoe dit met de eisende partij en de klant is overeengekomen. Gemotiveerd moet worden dat de impact van de afwijking verantwoord is (eventueel in samenspraak met de eisende partij). Uitgangspunt blijft de VRKI maar voor één onderdeel van de beveiligingsmaatregelen is dit niet mogelijk. De VRKI biedt oplossingen hiervoor. Er wordt dus afgeweken van de zwaarte van de maatregel. Dit mag alleen toegepast worden binnen de mogelijkheden van de VRKI en voor slechts één onderdeel van de maatregelenmix. Zijn het er meer, dan moet er worden gekozen voor de route afwijkend VRKI, paragraaf B1.4.3. Het is dus geen “gelijkwaardigheids-issue”, maar een echte “afwijking”.

#### B1.4.3 Risicoanalyse afwijkend van de VRKI

Zodra er een methodiek wordt toegepast anders dan de VRKI of op het moment dat er meerdere beveiligingsmaatregelen niet passen bij het object kan het toetsingskader waarop de risicoanalyse is gebaseerd uit de volgende punten bestaan:

- Wet- en regelgeving: Te denken valt aan de Wpbr, archiefwet en andere regelingen. Van belang is te vermelden welke voorschriften (datum/versie) van toepassingen zijn en op welke wijze deze zijn toegepast bij het opstellen van het document (toetsingskader).
- Vergunningen en meldingen: Zijn er meldingen gedaan voor het object waaraan voorwaarden zijn verbonden of zijn er geldende voorschriften uit een (eerdere) vergunning? Deze documenten en de hierin relevante beperkingen moeten worden opgenomen in deze paragraaf.
- Normen en overige voorschriften: Bij de totstandkoming van het document zal veelvuldig worden verwezen naar relevante normen en overige voorschriften. Deze moeten worden opgenomen in het document. Belangrijk hierbij is welke versie hiervan is toegepast en welke onderdelen van het normatief voorschrift wel/niet van toepassing zijn.
- Richtlijnen en handreikingen: Dit kunnen voorschriften zijn die worden opgelegd vanuit een betrokken/eisende partij of bijvoorbeeld van toepassing zijn verklaard in een vergunning of op voorwaarde verzekeraar.
- Overeenkomsten (contracten, verzekeringspolis).
- Overig (Bijvoorbeeld: eisen voortvloeiend uit omgeving).

De Adviseur beschrijft welke (combinatie van) risicoanalyse methodiek(en) wordt toegepast, mits deze is uitgevoerd door de Adviseur.

#### B1.4.3.1 Beschrijving van de beveiligingsmaatregelen

De Adviseur moet de relevante beveiligingsmaatregelen OBESCAR uitwerken en voldoende detailleren.

Daarbij let de Adviseur op het volgende:

- De uitwerking en detaillering is op een niveau waarbij het BORG-B- en/of het BORG-E-bedrijf en/of een aannemer een detailontwerp van de maatregelen kan maken. Detailontwerp is de projectie, ontwerp van de constructie, keuze van materialen en/of componenten e.d.;
- De opdrachtgever en de verzekeraar moeten zich een beeld kunnen vormen van de te realiseren maatregelen;
- Aspecten waarbij verwacht kan worden dat misverstanden of fouten kunnen ontstaan door verschil in interpretaties en/of ontbrekende kennis moeten in de uitwerking door de Adviseur nadrukkelijk zijn vermeld, waar nodig en/of nuttig met een relevante oplossingsrichting.

### Opmerkingen

- Over het algemeen is de opdrachtgever een leek en de deskundigheid van de verzekeraar kan variëren (b.v. functie als tussenpersoon of risk engineer). Beiden moeten een goed beeld hebben van de beveiligingsmaatregelen. Een omschrijving met slechts de aanduidingen uit de VRKI (zoals EL2, BK3 etc.) is onvoldoende. De Adviseur moet per ruimte, gevelement, wand en evt. vloer en plafond aangeven welke beveiliging moet worden toegepast. Waar zinvol, mag dit ook gedaan worden per groep ruimten, gevelementen, etc. Het doel is dat ook iemand zonder inhoudelijke (detail)kennis van de VRKI zich een juist beeld van de omvang van beveiliging en aard van werkzaamheden moet kunnen vormen. Met name voor de BK-, CO- en ME-maatregelen speelt dit een rol (bijvoorbeeld vervangen van glas, verstevigen van muren, bouwen van compartimenten). Hoewel verwijzingen naar normen en vaktermen nooit volledig kunnen worden voorkomen.
- De ME-maatregelen anders dan de mistgenerator (ME1, ME2 en ME3) zijn in de VRKI vrij summier beschreven. De Adviseur moet in het advies aangeven hoe de verwachte vertraging wordt bereikt en waar nodig welke materialen moeten worden toegepast.
- Detaillering van de O-maatregelen moet worden gedaan in overleg met de opdrachtgever.
- Het is in principe niet de bedoeling dat de Adviseur een projectie- of constructietekening van de voorzieningen maakt. Waar zinvol, maakt de Adviseur gebruik van een tekening of schets om de situatie te verduidelijken. De bereikbaarheid van gevelementen volgens de NEN5087 bijvoorbeeld kan goed worden aangegeven met een gevel- of doorsnedetekening.

#### B1.4.4 Restrisico (facultatief)

Hier wordt ingegaan op het risico dat overblijft indien de beschreven risico's op de beschreven wijze worden beveiligd. Het moet voor de opdrachtgever duidelijk zijn voor welke risico's het beveiligingsplan **geen** beveiliging biedt.

## B1.5 Kwaliteitsborging

In het beveiligingsplan staat wat er moet worden gedaan en gecontroleerd. Het is een document tussen opdrachtgever en Adviseur. Kwaliteitsborging is daarmee dus geen direct onderdeel van BORG-A. Wel moet de Adviseur de opdrachtgever hierover adviseren. De Adviseur moet vermelden hoe er wordt omgegaan met de kwaliteitsborging van de opgeleverde beveiliging. Bijvoorbeeld:

- Afgifte BORG-B en/of BORG-E certificaat;
- Controle na oplevering door.....;
- Beheer van de beveiliging en onderhoud van het aangebrachte beveiligingssysteem.

Aandacht voor het beheer en het beveiligen van de instellingen van digitale componenten (beveiliging van Operationele Technologie, internetcommunicatie tussen verschillende onderdelen van het beveiligingssysteem) kan een nuttige toevoeging zijn.



## Centrum voor Criminaliteitspreventie en Veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid is het centrum dat samenhangende instrumenten ontwikkelt en implementeert om de maatschappelijke veiligheid te vergroten. Het CCV stimuleert samenwerking tussen publieke en private organisaties om criminaliteit integraal terug te dringen en vormt een schakel tussen beleid en praktijk.

Van deze door het CCV ontwikkelde instrumenten, door andere partijen ontwikkelde instrumenten, of op marktniveau al aanwezige (technische) instrumenten kan de behoefte aanwezig zijn dat de kwaliteit van de gehaalde prestatie aantoonbaar gemaakt wordt.

Het CCV heeft hiervoor conformiteitschema's in beheer, waarvoor een structuur met inspraak van belanghebbende partijen ingericht is.

Het Centrum voor Criminaliteitspreventie en Veiligheid is gehuisvest te Utrecht:  
Churchillaan 11  
3527 GV Utrecht  
Postbus 14069  
3508 SC Utrecht  
T (030) 751 6700  
F (030) 751 6701



De stichting Centrum voor Criminaliteitspreventie en Veiligheid is een initiatief van het Ministerie van Veiligheid en Justitie, het Ministerie van Binnenlandse Zaken en Koninkrijksrelatie, het Verbond van Verzekeraars, werkgeversorganisatie VNO-NCW, de Vereniging van Nederlandse Gemeenten en de Raad van Korpschefs.

