EINDTERMEN

HOOG RISICO ADVISEUR / TBV-SPECIALIST

HRA/TBV-S®

LEVEL 3 - SPECIALIST

Versie 1.0

Publicatiedatum	01-05-2026
Ingangsdatum	01-05-2026

Inhoudsopgave

1. Inleiding

1.1 Doelstelling

Dit eindtermendocument gaat over het werkgebied van de Hoog Risico Adviseur. Doel is vast te stellen of de kandidaat kennis en vaardigheden heeft om een goed advies te verstrekken bij een hoog risico object. Het advies gaat primair over security (dus criminele risico's) maar sluit gevolgschades, zoals brandrisico, en reputatieschade, niet geheel uit. Het advies richt zich op "maatwerk" van VRKI-risicoklasse 4 objecten; maar ook op risico's, al dan niet verzekerd of verzekerbaar, die dat risico overstijgen.

Toelichting: Kennisniveau TBV wordt niet getoetst – voor adviseurs niet werkzaam in beveiligingsbranche is een introductiecursus gewenst.
Dit eindtermendocument zegt niets over de basisbeginselen van het beveiligingsvak voor adviseurs, sales-medewerkers en technisch beheerders van beveiligingsbedrijven. Het is geen herhaling of uitbreiding van de TBV-eindtermen maar een voortgezette TBV-opleiding. Het werkveld van de TBV-S® heeft ook niet de VRKI als basis maar maakt wel gebruik van begrippen die o.a. in de VRKI vermeld worden. Deze eindtermen zijn ook bedoeld voor personen die werkzaam zijn als adviseur in de civiele sector; die dus geen TBV-achtergrond hebben. Omdat in de beveiligingsplannen van het examen wel de definities uit deel B van de VRKI mogen worden gebruikt (naast andere normeringen) is het voor cursisten die niet in het bezit zijn van een TBV-diploma gewenst dat zij eerst een introductiecursus volgen waarin basisbeginselen van de VRKI en gebruikte definities worden uitgelegd. Uitgangspunt voor het examen HRA/ TBV-S® is dat de kandidaat kennis en vaardigheden heeft op HBO denk- en werkniveau. Het examen is toegankelijk zonder vereiste verplichte vooropleiding.

1.2 Eindtermen, toetstermen, toetsmatrijs

Dit document heeft de indeling: Eindtermen, toetstermen en toetsmatrijs. In de eindtermen worden de hoofdgroepen weergegeven waarover de kennis getoetst wordt. Bij de toetstermen wordt concreet in steekwoorden benoemd waar de kennis en vaardigheden zich op moeten richten. Dat is voor opleiders van belang om lesstof te ontwikkelen voor de opleiding HRA/ TBV-S®. De toetstermen zijn indicatief en niet absoluut. In de toetsmatrijs (Bijlage 1) wordt weergegeven hoeveel vragen van een bepaald onderdeel tijdens het theoretisch examen gesteld worden.

1.3 Taxonomie

In dit eindtermendocument is geen taxonomie aangegeven. Er is immers sprake van specialistische kennis.

1.4 Examenonderdelen

Het examen bestaat uit vijf onderdelen en wordt afgenomen en wordt afgenomen door examinatoren van CIBV:

1. Theorie-examen
2. Toets beoordelen praktijksituaties
3. Volgen security workshops (deelname van alle 5 security workshops bij leveranciers)
4. Eindscriptie maken
5. Eindscriptie verdedigen

2. Beoordelingscriteria examenonderdelen

2.1 Onderdeel 1: Theorie-examen

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x1

- Kandidaat krijgt 90 minuten de tijd om het theorie-examen te maken.
- Tijdens het examen mag de kandidaat geen naslagwerken of documenten raadplegen.
- De theorie wordt getoetst d.m.v. 50 meerkeuzevragen met 4 antwoordmogelijkheden per vraag. Voor alle correct beantwoorde vragen kunnen samen 50 punten worden behaald.
- De cesuur (de zak-slaaggrens) is bepaald op 17. Dus bij 17 fouten heeft de kandidaat een 6.
- De uitslag van het examen wordt uitgedrukt in een heel cijfer.
- De norm mag niet meer worden gewijzigd door de examinatoren.
- In Bijlage 2 is de cesuur weergegeven.
- De uitslag van dit examen krijgt de kandidaat direct na afloop.
- Voorwaardelijk: Dit examenonderdeel is cruciaal. De kandidaat moet minimaal een 6 scoren voor dit onderdeel.

Noot: een kandidaat krijgt binnen de periode van 3 jaar maximaal 3 herkansingen

2.2 Onderdeel 2: Toets beoordelen praktijksituaties

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x1

- De kandidaat krijgt 90 minuten de tijd om het examen “Beoordelen praktijksituaties” te maken.
- Tijdens het examen mag de kandidaat schriftelijke naslagwerken of documenten raadplegen.
- Het gebruik van digitale en andere hulpmiddelen is niet toegestaan.
- Het examen bestaat uit beantwoorden van open vragen a.d.h.v. 5 praktijkincidenten uit de media.
- Per case moet de kandidaat een antwoord geven op:
    - Wat is er beveiligings-technisch fout gegaan in het voorbeeld uit de media?
    - Beschrijf hoe op die locatie de schillentheorie toegepast zou kunnen worden.
    - Benoem criminele risico’s waarmee u, als u een beveiligingsplan voor dit object zou moeten maken, rekening zou houden.
- Het examen wordt door twee examinatoren nagekeken. De kandidaat krijgt de uitslag binnen 4 weken van CIBV.
- De uitslag van het examen wordt uitgedrukt in een heel cijfer. Het eindcijfer is het gemiddelde van alle resultaten uitgedrukt in een heel cijfer (afronding van < 0,4 naar beneden en > 0,5 naar boven).

Examenonderdeel 1 en 2 mogen op dezelfde dag worden afgenomen.

2.3 Onderdeel 3: Volgen security workshops

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x1

- De kandidaat moet alle workshops bijwonen.
- In geval van ziekte, overmacht, etc. is de kandidaat zelf verantwoordelijk dat hij de gemiste workshop inhaalt op een later tijdstip. In dit geval mag hij wel deelnemen aan de andere examenonderdelen. De gemiste workshop moet de kandidaat binnen 3 jaar halen. Het diploma wordt pas verstrekt na het behalen van alle onderdelen.

- Voor een gemiste workshop mag één “Vrijstelling workshop” worden aangevraagd. Onder de volgende voorwaarden:
    - De vrijstelling wordt slechts éénmaal tijdens de opleiding verleend.
    - Een “vrijstelling workshop” is geen automatisch recht; het wordt slechts in zeer uitzonderlijke gevallen verleend.
    - De aanvraag dient met redenen omkleed worden ingediend.
    - De kandidaat moet aantonen dat de inhoud/kennis van de workshop op een andere maar gelijkwaardige wijze is verkregen.
    - De aanvraag wordt door twee examinatoren beoordeeld.
    - Een afwijzing van de aanvraag is niet vatbaar voor beroep.
    - Aan de beoordeling van de aanvraag “vrijstelling workshop” zijn administratieve kosten verbonden.
- Na het volgen van de workshop maakt de kandidaat een “Rapport van deelname” op dat binnen 5 werkdagen na het volgen van de workshop per mail wordt ingeleverd bij CIBV.
- CIBV mailt rapport van deelname naar twee leden van de CIBV Examencommissie.
- Ieder Rapport van deelname kan maximaal 2 punten opleveren. De maximale score voor dit onderdeel is dus 10 punten.
- De uitslag van dit examenonderdeel wordt uitgedrukt in een heel cijfer.
- In Bijlage 3 is een voorbeeld “Rapport van Deelname” opgenomen.

2.4 Onderdeel 4: Eindscriptie maken

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x3
De kandidaat maakt een eindscriptie die moet voldoen aan de onderstaande voorwaarden:

- CIBV verstrekt geen examenopdracht; de kandidaat kiest zelf het te beveiligen object (zie uitleg hieronder).
- Als de kandidaat een keuze van zijn afstudeer object heeft bepaald, biedt hij een beschrijving met toelichting en plattegrond van dat object aan met eventuele foto’s (dus niet de uitwerking met complete uitwerking) bij CIBV.
- De EC bepaalt binnen vier weken of het object voldoet aan de criteria zoals hieronder is gesteld.
- CIBV accepteert ingeleverde werkstukken pas:
    - Als aan betalingsverplichting is voldaan
    - Voorwaardelijk: Kandidaat geslaagd is voor examenonderdeel 1, 2 en 3 met minimaal een cijfer 6
- Voor het afronden van de eindscriptie heeft de kandidaat één jaar de tijd gerekend vanaf de datum dat de EC heeft bepaald dat het object geschikt is als afstudeerobject.
- Bij het maken van het werkstuk is raadplegen van alle lectuur toegestaan.
- Deskundigen mogen geraadpleegd worden.
- Citaten uit onderzoeken of normen moeten met bronvermelding.

Afstudeer object
De kandidaat heeft de keuze uit:

- Een bestaand hoog risico object
- Een fictief object

Toelichting keuze object eindscriptie:
De kandidaat is zelf verantwoordelijk voor de keuze van het object van zijn eindscriptie. In veel gevallen staan hoog risicobedrijven niet te springen om hun risico’s te delen met derden. Onbekenden te laten kijken in hun keuken. Daarom is het toegestaan dat de kandidaat een

fictief bedrijf gebruikt voor zijn eindscriptie. In beide gevallen moet het object wel aan onderstaande voorwaarden voldoen.

- Het object moet voldoen aan VRKI-risicoklasse 4 of gelijkwaardig
- Moet voldoende omvang hebben. Het object moet zich lenen om de 12 onderdelen van examenonderdeel 4 toe te passen.
    1. Stappenplan
    2. Kleurenmethode
    3. Risicoanalyse & Risicomanagement (inclusief spionage)
    4. Schillentheorie (w.o. Toegangsbeheer & Toegangscontrole)
    5. Cyber Security
    6. Bouwkundig- mechanische beveiliging
    7. Inbraaksignaleringssystemen (w.o. noodstroom, in- en uitschakeltechnieken, lokale alarmering)
    8. Brandpreventieve maatregelen (w.o. brandsignalering – detectie – blusmiddelen – vluchtwegsignalering)
    9. Waardeberging, compartimentering en meeneembeperkende maatregelen (w.o. Mistgeneratoren)
    10. Alarmtransmissie & Alarmcentrales
    11. Alarmafhandeling en preventief toezicht (w.o. technische toezicht)
    12. CCTV/ VSS/ drones
- Het object mag iets zijn waar de kandidaat eerder bij betrokken is geweest. Hij mag ook een fictief object gebruiken. Ook met behulp van AI.
- Een object dat ooit eerder is ingeleverd door andere kandidaat is toegestaan mits de attractiviteit, bedrijfscultuur, functie per ruime, eisende partij, criminele risico's en omgevingsrisico's totaal anders zijn.

De opbouw en vorm van eindscriptie

- Het werkstuk wordt aangeleverd als pdf-bestand. Alle pagina's zijn genummerd.
- Het voorblad bevat de volgende gegevens:
    - Het CIBV-kandidaat nummer (wordt verstrekt na inschrijving voor het examen);
    - Naam, voornaam, geboortedatum van de kandidaat;
    - Emailadres en telefoonnummer;
    - Titel van het object waarvoor het plan gemaakt is (bedrijfsactiviteit).
- Verplichte volgorde:
    1. Beschrijving van het object:
        a. Bedrijfssoort;
        b. Ligging en omgeving;
        c. Schadehistorie;
        d. Bouwaard;
        e. Huidig beveiligingsniveau;
        f. Aanleiding hoe kandidaat bij zijn object is betrokken.
    2. Beveiligingsplan:
        a. De hoofdgroepen moeten verwerkt worden;
        b. De onderdelen moeten voorzien worden van een titel (kop)
        c. De thema's van de workshops moeten verwerkt zijn in het beveiligingsplan.

De beoordeling van de eindscriptie

- Wordt gedaan door 2 examencommissie-leden

- Door elke examinator wordt proces-verbaal van beoordeling opgemaakt. Het toegekend cijfer wordt schriftelijk gemotiveerd. Het proces-verbaal wordt ingestuurd naar CIBV.
- De kandidaat ontvangt daarvan geen afschrift. Inzage bij CIBV is tegen vergoeding mogelijk.
- De beheerders van deze eindtermen hebben op verzoek wel inzage maar document wordt niet verstrekt.
- Voor dit onderdeel moet de kandidaat minimaal een 6 halen.

De uitslag

Voldoende

Als uitslag voldoende is wordt de kandidaat ingepland voor onderdeel 5: de verdediging.

Onvoldoende

Als de kandidaat voor dit onderdeel zakt:

- Vindt er een bespreking plaats met de examencommissie.
- De toelichting van de examencommissie duurt maximaal 1,5 uur.
- De kandidaat krijgt de gelegenheid om éénmaal zijn werkstuk te herstellen en te voldoen aan de eisen. Als de kandidaat na herbeoordeling slaagt gaat hij door naar examenonderdeel 5.
- Als de kandidaat opnieuw zakt stopt het examenonderdeel 4. Hij kan zich bij CIBV opnieuw inschrijven voor een examenonderdeel 4. De geldigheid van examenonderdeel 1 (Tussentijdse toets), 2 (theorie-examen) en 3 (volgen workshops) is drie jaar.

2.5 Onderdeel 5: Eindscriptie verdedigen

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x4

- De verdediging wordt afgenomen door 2 examinatoren van de vaste CIBV EC Crimi; als de kandidaat dat wenst mag er één door hem aangedragen toezichthouder aanwezig zijn. Een medecursist mag geen toezichthouder zijn.
- De toezichthouder heeft geen inspraak en maakt geen deel uit van de beoordeling.
- Het examen duurt maximaal 90 minuten.
- De uitslag van de verdediging wordt door de commissie met redenen omkleed vastgelegd in een proces-verbaal.
- De kandidaat krijgt de uitslag direct mondeling meegedeeld.
- Voor kandidaten in het bezit van het TBV-diploma en slagen voor examen TBV-S®:
    - Op verzoek van de kandidaat kan kandidaat in vakbekwaamheid register van CIBV geregistreerd worden als TBV-er level 3 (specialist)
    - Een geslaagde kandidaat krijgt een diploma en mag titel en logo “TBV Hoog Risico Adviseur” gebruiken.
    - Kandidaat mag BORG-A gecertificeerde beveiligingsplannen maken mits certificaathouder is bij CIBV.
- Indien gewenst wordt de kandidaat geregistreerd in het vakbekwaamheidsregister van CIBV op level 3 (specialist - HRA – nieuw onderdeel). Deze registratie is 5 jaar geldig. Verlenging is mogelijk en staat geregeld in het register vakbekwaamheid.
- Voor kandidaten die niet in het bezit zijn van het TBV-diploma:
    - Op verzoek van de kandidaat kan kandidaat in vakbekwaamheid register van CIBV geregistreerd worden als Hoog Risico Adviseur (apart register)
    - Een geslaagde kandidaat krijgt een diploma en mag titel en logo “Hoog Risico Adviseur” gebruiken.

3. Beoordeling examen

Dit eindtermendocument gaat over het werkgebied van de Hoog Risico Adviseur. Doel is vast te stellen of de kandidaat kennis en vaardigheden heeft om een goed advies te verstrekken bij een hoog risico object. Het advies gaat primair over security (dus criminele risico's) maar sluit gevolgschades, zoals brandrisico, en reputatieschade, niet geheel uit. Het advies richt zich op "maatwerk" van VRKI-risicoklasse 4 objecten; maar ook op risico's, al dan niet verzekerd of verzekerbaar, die dat risico overstijgen.

1	Theorie-examen	Cijfer x1	Max. 10 punten	Min. cijfer 6 (6 punten)
2	Praktijksituatie	Cijfer x1	Max. 10 punten	Min. cijfer 6 (6 punten)
3	Workshops	Cijfer x1	Max. 10 punten	Min. cijfer 6 (6 punten)
4	Eindscriptie	Cijfer x3	Max. 30 punten	Min. cijfer 6 (18 punten)
5	Verdediging	Cijfer x4	Max. 40 punten	Min. cijfer 6 (24 punten)
	Maximale score		100 punten	100 punten is eindcijfer 10

Als de kandidaat voor onderdeel 5 zakt kan éénmaal her-verdediging plaatsvinden.

Bijlagen:
1. Toetsmatrijs
2. Cesuur theorie-examen
3. Model Rapport van deelname van bijwonen workshops

Eindtermen

Theoriekennis

Toetstermen

Toetskennis

De genoemde toetstermen zijn richtinggevend, niet absoluut.

1	Stappenplan Hoog Risico Methodiek (HRM)	3 – 6 vragen
1.1	De adviseur verstrekt uitleg en instrueert opdrachtgever en medewerkers die bij de beveiliging een sleutelrol vervullen.	De werkwijze van de adviseur (HRA), het doorlopen van het stappenplan met behulp van de HRM, wordt met opdrachtgever doorlopen. - Het stappenplan bevat tussentijdse “beslismomenten” - Opdrachtgever bevestigt schriftelijk dat hij akkoord gaat met stappenplan.
1.2	De kandidaat toont aan dat verkregen informatie en documenten karakter heeft van geheimhouding en vertrouwelijkheid.	Verklaring van betrouwbaarheid- verklaring omtrent gedrag – geheimhoudingsverklaring – wie mag wat hebben – opslag bij adviseur van vertrouwelijke gegevens.
1.3	De kandidaat beheerst het stappenplan hoog risico methodiek.	Kandidaat kan stappenplan (12 stappen) van HRM aan klant uitleggen – kandidaat kan werken met beslisdocument van stappenplan.
1.4	Stap 1: Oriëntatie van het beveiligingsobject	Vastleggen fysieke situatie te beveiligen object – luchtfoto’s – plattegronden – deel-plattegronden-afdelingen – hoe zien huidige beveiligingsmaatregelen er uit - is security vastgelegd in beleid – is er een security-officer? – wie zijn huidige partners/partijen van de beveiliging?
1.5	Stap 2: Aanleiding/ start beveiligingsonderzoek	Er bestaat altijd een reden waarom de adviseur bij dit project betrokken wordt. Onderzoek naar incident – eisen verzekeraar – klanten van opdrachtgever – overheid.
1.6	Stap 3: Oriëntatie/voorbereiding opstellen PvE Verkenning wens klant.	Wordt de OR betrokken bij het Beveiligingsplan Hoog Risico (BHR)? - Krijgt adviseur (HRA) toestemming om kleurenmethode met medewerkers op te stellen? - Zijn er onderdelen van het bedrijf die taboe (geheim) zijn? - Is er budget begroot voor de beveiligingsmaatregelen? - Wie is beslissingsbevoegd? - Wie mag kennisnemen van BHR? - Bestaan er contracten met huidige beveiliging? - Zijn er partijen (beveiligingsbedrijven) die klant per sé wil inschakelen?
1.7	Stap 4: Stappenplan Hoog Risico Methodiek (HRM) De adviseur verstrekt uitleg en instrueert opdrachtgever en medewerkers die bij de beveiliging een sleutelrol vervullen.	De werkwijze van de adviseur (HRA), het doorlopen van het stappenplan met behulp van de HRM, wordt met opdrachtgever doorlopen. - Het stappenplan bevat tussentijdse “beslismomenten” - Opdrachtgever bevestigt schriftelijk dat hij akkoord gaat met stappenplan.
1.8	Juridisch kader	AVG – aansprakelijkheid BW – WPBR – VEB4 – BORG.

2	Stap 5: Kleurenmethode	1 – 2 vragen
2.1	Systeem en methodiek Kleurenmethode	De HRA is vaardig met toepassing van de kleurenmethode en weet dat instrument naast optische verduidelijking, zwaartepunt en toegankelijkheid belangrijk is voor acceptatie en effectiviteit.
2.2	Zwaartepunt	Weet zwaartepunt van object te bepalen. Naast attractiviteit ook de kwetsbaarheid van organisatie en inzicht in gevolgschaden.
2.3	Uitleg effect Kleurenmethode	HRA is in staat voorlichting en een presentatie te geven aan afdelingshoofden. Weet naar organisatie vertaling te geven van E = K x A.
2.4	Juridisch kader	AVG – WPBR – OR.

3	Stap 6: Risicoanalyse & Risicomanagement (Beoordelen objecten)	6 – 10 vragen
3.1	Risico-weging	HRA doet met opdrachtgever in bijzijn sleutelpersonen beveiliging onderzoek naar risico-weging – R=K x S = inventarisatie van accepteerbare en niet-accepteerbare schades – met de criminele delict afweging wordt in elk geval rekening gehouden met; Cybercriminaliteit, Diefstal, inbraak, overval, verduistering, Brandstichting, Spionage, Oplichting, Geweld, Ontvoering (Terrorisme?) Openbare ordeverstoring (Klimaatactivisten ed.) Maar ook risico's als b.v. uitbraak bij gevangenissen, moeten gewogen worden.
3.2	Schadehistorie	Dit is een heel gevoelig onderdeel. Hoog risico-objecten willen deze info vaak niet delen. - Reputatieschade kan enorme gevolgen hebben. - De adviseur (HRA) moet dan via mondelinge gesprekken een inzicht krijgen. - Hij probeert antwoord te krijgen op: Heeft er al eens een cyber-aanval plaatsgevonden? Hoeveel schade heeft bedrijf geleden onder criminaliteit? Zijn er medewerkers bij betrokken geweest? Wat is het beleid? Wordt er aangifte gedaan? Hoe is er gereageerd op criminele schades?
3.3	Huidige beveiligingsmaatregelen	Is er een bestaand beveiligingsplan? Welke maatregelen zijn er al genomen? Hoe zijn de ervaringen met bestaande maatregelen? Is er een onderhoudsplan? Worden de beveiligingsmaatregelen structureel op effectiviteit getest?
3.4	Bedrijfscultuur en beveiliging	Wat is het huidig beleid m.b.t. security? Wie is er binnen het bedrijf verantwoordelijk voor security? Is beleid vastgelegd in bedrijfshuishoudelijk reglement/ arbeidscontract/ kenbaar gemaakt aan medewerkers/ maakt het deel uit van werkoverleg? Is security begroot binnen het financieel jaarplan?

		Wordt securitybeleid visueel uitgedragen naar de medewerkers.
3.5	Rapportage - PvE	Wat is het zwaartepunt van de beveiliging? Is het risico verzekerbaar en onder welke voorwaarden? Wat is voor eisende partij een acceptabel risico? R = K x S - Is de uitkomst van de Kleurenmethode verwerkt in PvE? Zijn de eisen van security-beleid opgenomen in PvE?
3.6	Juridisch kader	AVG – WvStr. – BW – WPBR.

4	**Stap 7: Schillentheorie (Beveiligingsplan Hoog Risico - BHR)**	**15 – 25 vragen**
4.1	Kenmerken en soorten Schillenmethode	Bulls-Eye-methode, Uien-methode, the 3 lines of defence, Hazard-barrier-target model, Zwitsers gatenkaas model, LOPA-model, defence in depth-model, Haagse methodiek, TAPA-analyse, Handreiking buitenterreinen – mobiliteitsbedrijven, handreiking transport & logistieke bedrijven, Handreiking explosieve voor civiel gebruik.
4.2	Verplichte inhoud beveiligingsplan	Uitgangspunt is kwetsbaarheid/ attractiviteit - Van daar uit schillen aanbrengen - Organisatie en O-maatregelen borgen - Alarmopvolging borgen - Alarmopvolging politie □prio 1 - Onderhoud borgen - Jaarlijkse herijking risico borgen in specifieke audit HR-object.
4,3	Maatregelen buitenterrein	Hekwerk - Sloten/gracht – Roadbarrier – CCTV - Parkeerbeleid-personeel - Uitgangscontrole/ ingangscontrole – Buitendetectie – schrikdraaddetectie – Ramkraakbeveiliging – (w.o. autovangrail – afgekeurde heipalen) – Verlichting Verhoogde grondwal. Natuurlijke elementen als beveiliging toepassen.
4.4	Maatregelen m.b.t. buitenschil	Bewegwijzering gebouwen - Herkenning object (“vlaggen” attractiviteit) - Inkijk in het pand – bezoekersregistratie - Staat gevelelementen – Toegangscontrole – CCTV - Sluisfunctie – tourniquet - Vrijwillige visitatie – inleveren GSM – lockers – Goederenscan.
4.5	Maatregelen m.b.t. waardeberging (zie ook Onderdeel 9)	Inbraakwerende kast – afstortmogelijkheid –tijdslot – openingsvertragingsslot – elektronisch codeslot – verankering – VGW - Bouwen compartiment – VSP – staalmat constructies – oud zeecontainer – eigen constructie – toegang met sluis – beperkte openstand – Mistgeneratoren.
4.6	Maatregelen m.b.t. kwetsbaar onderdeel bedrijf/bedrijfsvoering	Dit onderdeel gaat over niet criminele attractiviteit (buit) – wel over kwetsbaarheid bedrijf (uitval/sabotage machine) – kwetsbaarheid door chantage van sabotage onderdeel – voorbeeld zijn bv ook examens.
4.7	Maatregelen CCTV/VSS	ANPR-camera’s - Motion detectie - Thermische camera’s – Verlichting – Beeldopslag - Controle/ handelen CCTV-beelden – Verlichting - Wettelijke

		eisen – toezichtcentrale – live view Drone mogelijkheden.
4.8	Cybersecurity (zie ook onderdeel 5)	Firewall - Patchruimte beveiliging – Virusscanners - Beleid thuiswerken - Dataopslag cloud & fysiek - High security USB's - Data lekken.
4.9	Geweld en ontvoeringsmaatregelen	Strongroom – Digitale life-lijn systeem onafhankelijk naar buiten
4.10	Alarmoverdracht – alarmopvolging – preventie toezicht – persoonscontrole (zie ook onderdeel 12)	Alarm- en dataverbindingen – monitoring signalering & ME4 – preventief toezicht (BD) – vrijwillige visitatie – protocol overval – life view – poortcontrole.
4.11	Stap 8: Bereiken overeenstemming over beveiligingsmaatregelen	Klant + eisende partij - Gaat opdrachtgever/ klant akkoord met uw voorstel? - Gaat eisende partij akkoord met uw voorstel? - Gaat inspectie-instelling akkoord met uw voorstel? Dit is een beslismoment voor opdrachtgever. Opdrachtgever en eisende partijen gaan akkoord met voorstel van maatregelen.
4.12	Stap 9: Implementeren & uitvoeren beveiligingsmaatregelen Alle beveiligingsmaatregelen worden uitgevoerd en high security-producten geïnstalleerd	Aanbrengen van technische high security producten- Opnemen security beleid - Trainen/voorlichting personeel - Security-manager betrekken bij uitvoeren van de technische maatregelen - Alarmopvolging regelen.
4.13	Stap 10: Test maatregelen & Opleveren	Alle maatregelen worden op goede werking getest – maatregelen worden in onderlinge samenhang getest – alle maatregelen waarbij externe partners betrokken zijn worden getest Opdrachtgever tekent voor oplevering en gaat akkoord met maatregelen – heeft persoonlijk gecontroleerd of alle maatregelen naar wens werken - Eisende partij gaat akkoord met de maatregelen - Onafhankelijke en door CIBV erkend inspectie-instelling gaat akkoord met de maatregelen.
4.14	Stap 11 (interne audit) Elk jaar voert opdrachtgever samen met de HRA een interne audit uit.	De HRA maakt voor opdrachtgever een passende checklijst voor het herijken van het risico en testen van de maatregelen op functionaliteit.
4.15	Stap 12 (externe inspectie) Een door CIBV aangewezen inspecteur voert audit/inspectie uit. TBV is onvoldoende. - BORG-A gecertificeerd is onvoldoende. - Minimaal werk-denkniveau TBV-level 3. (TBV-S)	De HRA kan werkdocument opstellen voor inspectie door externe inspecteur. – HRA kan bevindingen uit inspectierapport verwerken in beveiligingsplan en omzetten in oplossingen.
4.16	Juridisch kader	AVG – WvStr. – BW – WPBR – APV – NEN – VEB/BORG.

5	Cyber Security	1 – 2 vragen
5.1	Cyberbeleid	Beleidsmaatregelen – bedrijfscultuur – beleid cyber security – de rol van de medewerker.
5.2	Uitvoering maatregelen	Firewall - Patchruimte beveiliging – Virusscanners - Beleid thuiswerken - Dataopslag cloud & fysiek - High security USB's - Data lekken.
5.3	Cyberspionage	Hoe weet je of je Pegasus hebt? Wie twijfelt of zijn smartphone gehackt is en besmet met Pegasus, de spionagesoftware van de Israëlische NSO Group, kan dit controleren met een tool. De zogeheten Mobile Verification Toolkit (MVT) is ontwikkeld door de onderzoekers van Amnesty International die de malware Pegasus grondig hebben onderzocht en onthuld.
5.4	Juridisch kader	AVG – WvStr – BW – Wet uitbreiding strafbaarheid spionageactiviteiten.

6	Bouwkundig- en mechanische beveiliging (vertraging)	4 – 8 vragen
6.1	B-voorzieningen omgeving	Sloten, grachten, vangrail, heipalen, rampalen, hekken, etc. Hekwerk - Roadbarrier - Parkeerbeleid-personeel –– Ramkraakbeveiliging – (w.o. autovangrail – afgekeurde heipalen) – Verlichting Verhoogde grondwal. Natuurlijke elementen als beveiliging toepassen.
6.2	Afscherming gevelopeningen	Rolluiken (+ matrix), weet dat rolluiken ook vallen onder de NEN 5096, slagwerende kunststoffen – gelaagd glas – slagwerend – kogelwerend – explosiewerend.
6.3	Verstevigde gevels	Security panel – braakvertragende bouwwerken – strekmetaal, etc.
6.4	Inbraakwerende deuren	Geattesteerde inbraakwerende deuren.
6.5	Toegangsverlening	Kaartlezers -elektronische sloten – biometrische toegangsverlening -etc. Bewegwijzering gebouwen - Herkenning object ("vlaggen" attractiviteit) - Inkijk in het pand – bezoekersregistratie - Staat gevelelementen – Toegangscontrole – CCTV - Sluisfunctie – tourniquet - Vrijwillige visitatie – inleveren GSM – lockers – goederenscan. - Uitgangscontrole/ ingangscontrole
6.6	Deur- en raamsloten	Hang- en sluitwerklijst PKVW, insteek- en oplegsloten, haakschoten, overval, klaviersloten, sluitkom, sluitkast, inbraakwerend bouwbeslag, blindbeslag, rozet, Veiligheidsklaviersloten.
6.7	Juridisch kader	Wetten – Normen – Richtlijnen – verordeningen – besluiten.

7	**Electrische signalering (w.o. Alarmsystemen/VSS, CCTV, buitendetectie, schrikdraaddetectie, noodstroom – in- en uitschakeltechnieken**	**5 – 10 vragen**
7.1	Centrale van inbraakalarmsysteem	Kenmerken van CCS geschikt voor hoge risico's.
7.2	Detectoren	Grade > 3, geschikt voor hoge risico's, soorten en toepassingen, detectoren zonder Grade.
7.3	Bediening (in- en uitschakelsystemen)	Codebediendeel, biometrische, kaartlezen, draadloos, apps, camera's.
7.4	Noodstroomvoorziening	Accu's, UPS, noodstroomaggregaat, stroomgroep verdeling.
7.5	Projectering	Zones, groepen, deelschakelingen, zichtbaar/ onzichtbaar, test en verslaglegging.
7.6	Installatie	Bevoegdheden en eisen aan installateur/monteur.
7.7	Onderhoud inbraaksignaleringssysteem	
7.8	CCTV/VSS –-	
7.9	Buitendetectie	schrikdraaddetectie
7.10	Juridisch kader	Wetten – Normen – Richtlijnen – verordeningen – besluiten.

8	**Brandpreventieve maatregelen**	**2 – 5 vragen**
8.1	Branddetectie via CCS	Soorten detectoren, niet draadloos.
8.2	Branddetectie op basis van NEN 2535	Kenmerken/eisen NEN 2535, verslaglegging.
8.3	Brandpreventie	
8.4	Brand ontruiming	
8.5	Vluchtwegsignalering	
8.6	Brandbestrijding (blussing)	Blusmiddelen.
8.7	Installatie	Bevoegdheden en eisen aan installateur/monteur.
8.8	Onderhoud brandmeld- en ontruimingsinstallaties	
8.9	Juridisch kader	REOB

9	Spionage- en afluistertechnieken	1 – 3 vragen
9.1	Medewerkers	Monitoren gebruikersactiviteiten medewerkers.
9.2	Afluisterapparatuur & verborgen camera's	
9.3	Spy tools	Spyware is software die is geïnstalleerd zonder toestemming (kan in computer, applicatie, webbrowser of app mobiele telefoon) die vertrouwelijke gegevens naar aanvaller doorstuurt.
9.4	Sweepen (afluisterapparatuur opsporen)	Radio frequentie-onderzoek en analoog zenderonderzoek o.a. GSM (inclusief 5G), Bluetooth, Electronic Spectrum Analyzer. Elektronisch veiligheidsonderzoek van voertuigen, kantoor- of woningruimtes naar microfoons, recorders en zendapparatuur (wanden, muren, vloeren, meubilair en voorwerpen). Non Linear Junction Detection detectie van geschakelde (opname)apparaten die meeliften met het aan- of uitschakelen van elektronische apparaten. Fysiek onderzoek van uw pand (airconditioningsystemen, muren, warmtebuizen, ventilatiesystemen etc.). Onderzoek naar uw fysieke beveiligingspersoneel voor ongeoorloofd toegang om zelf af te luisteren of om apparatuur te plaatsen Observatiewerkzaamheden om verdachte personen in de gaten te houden. Onderzoek met draadloze camera, warmtebeeld en UV licht Doormeten van interne kabelsystemen (lichtnet, telefoonlijn etc.). Onderzoek naar wifi en vaste telefoonlijnen. Onderzoek naar malware en spyware op mobiele telefoons, tablets, laptops etc.
9.5	Apps	
9.6	Juridisch kader	Wie mag er Sweepen? Machtigingen?

10	Waardeberging en Compartimentering	5 – 10 vragen
10.1	Inbraakwerende kasten	
10.2	Brandwerende kasten	
10.3	Kluizen	
10.4	Datasafes	
10.5	Compartimenten	
10.6	Tralie – hekwerken afscherming waardeberging	
10.7	Juridisch kader	

11	Alarmtransmissie en alarmcentrales	5 – 10 vragen
11.1	Alarmtransmissie mogelijkheden	
11.2	Sabotage en uitval alarmtransmissie	
11.3	Soorten alarmcentrales	
11.4	Ontvangst- en verwerkingsmogelijkheden alarmcentrales	
	Juridisch kader	

12	Alarmafhandeling en preventief toezicht	5 – 10 vragen
12.1	Soorten alarmafhandeling	
12.2	Kwaliteit alarmafhandeling	
12.3	Particuliere beveiliging	
12.4	Bedrijfsbeveiliging	
12.5	PPP	
12.6	Collectieve beveiliging	
12.7	Keurmerk en brancheorganisaties	
12.8	Receptionist (portier-manbewaker)	
12.9	Uitgangscontrole	
12.10	Juridisch kader	

4. Bijlage 1: Toetsmatrijs (Theorie-examen HRA)

Stap		Aantal vragen		
-	Geheimhouding vertrouwelijke informatie & stappenplan hoog risico methodiek (HRM)	1 - 2 vragen		
1	Beschrijving object	1 - 2 vragen		
2	Aanleiding/ start beveiligingsonderzoek en plan	1 - 2 vragen		
3	Verkenning wens klant	1 - 2 vragen		
4	Stappenplan Hoog Risico Methodiek (HRM)	1 - 2 vragen		
5	Risicoanalyse	6 - 10 vragen		
6	Risicoanalyse	6 - 10 vragen		
7	Beveiligingsplan Hoog Risico – Schillenmethode	15 - 25 vragen		
8	Confirmeren	1 - 2 vragen		
9	Implementeren & uitvoeren beveiligingsmaatregelen	3 - 5 vragen		
10	Opleveren	3 - 5 vragen		
11	Interne audit	1 - 3 vragen		
12	Externe inspectie	1 - 3 vragen		

5. Bijlage 2: Cesuur theorie-examen (50 meerkeuze vragen)

Aantal fouten	Cijfer
38 t/m 50	1
33 t/m 37	2
28 t/m 32	3
23 t/m 27	4
18 t/m 22	5
14 t/m 17	6
10 t/m 13	7
6 t/m 9	8
2 t/m 5	9
0 t/m 1	10

6. Bijlage 3: Rapport van deelname workshops (voorbeeld)

Dit is een model, vormvrij. De inhoud is verplicht.

Rapport van deelname gevolgde workshop

CIBV examennummer	:	
Naam kandidaat	:	
Emailadres kandidaat	:	
Telefoonnr. Kandidaat	:	
Naam workshop	:	
Korte beschrijving workshop	:	
Datum workshop	:	
Locatie en naam bedrijf	:	
Naam en contactpersoon presentator workshop	:	
Wat was uw leerdoel?	:	
Is uw leerdoel gehaald? Motiveer uw antwoord.	:	
Welke, voor hoog risico's bruikbare onderdelen, had de workshop?	:	
Heeft u uw getuigschrift, verklaring van deelname of diploma bijgevoegd?	:	