EINDTERMEN

HOOG RISICO ADVISEUR/TBV-SPECIALIST

HRA/TBV-S® 2026

LEVEL 3 - SPECIALIST

Versie 2.0

Versie 2.0

Publicatiedatum 01-06-2026

Ingangsdatum 01-06-2026

Het beheer wordt uitgevoerd door CIBV, Maas-Opleidingen en Van Dusseldorp Training.

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 vervolg daarop. 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. Bij de eindtermen wordt tevens weergegeven hoeveel vragen van een bepaald onderdeel tijdens het theoretisch examen gesteld worden (toetsmatrijs).

1.3 Taxonomie

In dit eindtermendocument is geen taxonomie aangegeven. Er is immers sprake van specialistische kennis (dit geldt voor de pilotperiode. Na evaluatie wordt taxonomie opgenomen).

1.4 Examenonderdelen

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

1. Theorie-examen met toets beoordelen praktijksituaties.
2. Eindscriptie maken met bijlage over gevolgde security workshops (deelname van alle 5 security workshops bij leveranciers).
3. 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 50 meerkeuzevragen van het examen bestaan uit twee onderdelen: 40 vragen over algemene kennis en 10 meerkeuzevragen aan de hand van een of meerdere krantberichten.
- 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 1 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: Eindscriptie maken

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x 4

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 examencommissie 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 met minimaal een cijfer 6.
- Voor het afronden van de eindscriptie heeft de kandidaat één jaar de tijd gerekend vanaf de datum dat de examencommissie 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 één pdf-bestand. Hele grote plattegronden (met b.v. projectering) mogen als bijlagen bijgevoegd worden.
    - Alle pagina's zijn genummerd.
    - Heeft een index.
    - Heeft een aanbiedingsbrief voor de klant.
    - Moet voor de klant leesbaar en begrijpbaar zijn.
    - Opsomming van allerlei technische mogelijkheden (om de examinator te overtuigen van kennis) moet worden vermeden. Als de technische mogelijkheden functioneel zijn en dienen om de klant een keuze te geven, is het toegestaan.
- 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 (na voorblad – index – aanbiedingsbrief) :
  - ***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.
  - ***Beveiligingsplan:***
    a. De hoofdgroepen moeten overzichtelijk verwerkt worden; iedere nieuwe hoofdgroep begint op een nieuwe pagina.
    b. De onderdelen moeten voorzien worden van een titel (kop)
    c. De thema's van de workshops moeten verwerkt zijn in het beveiligingsplan
  - ***Projectering inbraaksignaleringssysteem:***
    - Een projecteringstekening is verplicht. Een plattegrond met symbolen volstaat; motivatie en toelichting van soort detector en wijze van projecteren (zoals bij de TBV eindtermen) is niet noodzakelijk
    - Deelnemers zonder TBV achtergrond mogen hulp inroepen van elke TBV adviseur (bij de beoordeling van het werkstuk wel graag vermelding van externe hulp op dit onderdeel).
  - ***Organigram of blokkenschema van schillen***
    In het advies moet een organigram of blokkenschema zijn opgenomen zodat snel inzichtelijk wordt hoe de schillen zijn opgebouwd. Een handige tip is om de blokken te nummeren en onder het schema de blokken te beschrijven.
  - ***Uitwerking kleurenmethode***
    De kleurenmethode moet worden toegepast met kleuring van volledige vlakken en geen dunne lijn en tekst die kleur aangeeft.
  - ***Rapport van deelname workshops***
    a. In geval van ziekte, overmacht, etc. is de kandidaat zelf verantwoordelijk dat hij de gemiste workshop inhaalt op een later tijdstip.
    b. Van elke gevolgde workshop maakt de kandidaat een rapport van deelname op waaruit zijn kennis over die bepaalde workshop blijkt. In Bijlage 2 is een voorbeeld "Rapport van Deelname" opgenomen.

De beoordeling van de eindscriptie

- Wordt gedaan door 2 leden van de examencommissie.
- 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 *(Maas Opleidingen en Van Dusseldorp Trainingen)* 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 3: 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 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 3.
- Als de kandidaat opnieuw zakt stopt het examenonderdeel 2 Hij kan zich bij CIBV opnieuw inschrijven voor een examenonderdeel 2. De geldigheid van examenonderdeel 1 is drie jaar.

2.3 Onderdeel 3: Eindscriptie verdedigen

Waardering maximaal 10 punten – cijfer tussen 0 en 10 x 5

- De verdediging wordt afgenomen door 2 CIBV-HRA-examinatoren; 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 60 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	Eindscriptie	Cijfer x4	Max. 40 punten	Min. cijfer 6 (24 punten)
3	Verdediging	Cijfer x5	Max. 50 punten	Min. cijfer 6 (30 punten)
	Maximale score		100 punten	100 punten is eindcijfer 10

Als de kandidaat voor onderdeel 3 zakt kan éénmaal her-verdediging plaatsvinden.

Bijlagen:
1. Cesuur theorie-examen
2. 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 – W.v.Str.. – 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 – W.v.Str.. – 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 – W.v.Str. – 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	Naast standaard eisen van onderhoud ook bekend zijn met eisen specialistische detectieapparatuur.
7.8	CCTV/VSS –-	Kenmerken en functies camerasystemen, specialistische systemen voor hoge risico's, alarmafhandeling voor hoge risico's
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	NEN 2535 op hoofdlijnen. Inspectiecertificering.
8.3	Brandpreventie	Ontruimingsplan – ontruimingsprocedures – alarmeringsprocedure – BHV
8.4	Brand ontruiming	NEN2575 op hoofdlijnen. Type ontruimingsalarminstallaties. Inspectiecertificering
8.5	Vluchtwegsignalering	Vluchtwegsignalering – Noodverlichtingsinstallaties.
8.6	Brandbestrijding (blussing)	Type blusmiddelen. Projectering op basis van NEN 4001 op hoofdlijnen.
8.7	Installatie	Bevoegdheden en eisen aan installateur/monteur.
8.8	Onderhoud brandmeld- en ontruimingsinstallaties	Onderhoud brandmeldinstallatie (NEN 2654-1) op hoofdlijnen. Onderhoud ontruimingsalarminstallatie (NEN 2654-2) op hoofdlijnen.
8.9	Juridisch kader	BBL.

9	Spionage- en afluistertechnieken	1 – 3 vragen
9.1	Medewerkers	Monitoren gebruikersactiviteiten medewerkers.
9.2	Afluisterapparatuur & verborgen camera's	Technische hulpmiddelen.
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	Bestaan weten van diverse appas: Ear Spy, mSpy, Snoopza & Hoverwatch, deviceOwl, FindSpy, etc.
9.6	Juridisch kader	Wie mag er Sweepen? Machtigingen? Wetboek van Strafrecht, AVG,

10	Waardeberging en Compartimentering	5 – 10 vragen
10.1	Inbraakwerende kasten	Kennen van Grades, kluizen zonder documentatie(niet gecertificeerd) en liefst onder maaiveld.
10.2	Brandwerende kasten	Welke weerstandsklassen zijn er en voor welke materialen en tijden. Welke temperatuur-drempels zijn er ingebouwd?
10.3	Kluizen	Zie compartiment, daar in deze risicoklassen het uit zal draaien op een goed gebouwd compartiment(inbraak- en Brandwerend)
10.4	Datasafes	Staat in kluis is vaak in ons geval server ruimte Een echte data safe gebruiken we niet, zie ook weer compartiment
10.5	Compartimenten	Hoe bouw je een goed compartiment op met welke materialen kun je wat tegenhouden. Strekmetaal Armourcour, Metalfoil. Hoe word een muur opgeplust en hoe worden deuren gemodificeerd voor sterkere

		weerstand? Uiteraard ook kijken naar brandwerendheid.
10.6	Tralie – hekwerken afscherming waardeberging	Rolluiken. Welke materialen kunnen erin gebruikt worden. Hoe voorkom je optil mogelijkheden, hekwerken bieden weinig tot geen weerstand tegen manier van aanvallen
10.7	Juridisch kader	Weten dat in enkele gevallen eisen zijn m.b.t. opslag en compartimentering. Te denken valt aan opslag blanco paspoorten, vuurwerkdepot, wapenhandel en privé, etc.

11	Alarmtransmissie en alarmcentrales	5 – 10 vragen
11.1	Alarmtransmissie mogelijkheden	DP4. En dedicated lines Daaronder hoeven we niet eens te kijken VOP . begrippen rolling encryptie
11.2	Sabotage en uitval alarmtransmissie	Backup verbinding (Zit al in DP4) eisen aan uitvaldetectie. Verschil in providers
11.3	Soorten alarmcentrales	Benoemen het verschil in PAC/BAC en VTCs Onder welke NEN normering vallen ze (50518) (BAC niet)
11.4	Ontvangst- en verwerkingsmogelijkheden alarmcentrales	Snelheidseisen oppakken, diverse alarmen zoals overval brand en inbraak. Sneller dan NEN 50518?
11.5	Juridisch kader	Hoofdlijnen van de NEN 50518

12	**Alarmafhandeling en preventief toezicht**	**5 – 10 vragen**
12.1	Soorten alarmafhandeling	Weten wat de procedures zijn m.b.t. reactie bij overval, inbraak en brand. Afhandeling bij inzet Mistgeneratoren.
12.2	Kwaliteit alarmafhandeling	Welke bev bedrijf neem je in de armen Hoeveel beveiligers sturen ze en hoe lang doen ze erover op TP te zijn
12.3	Particuliere beveiliging	Wat zijn hun bevoegdheden Hoeveel man/vrouw zet je in?
12.4	Bedrijfsbeveiliging	Is een particuliere beveiliger alleen in eigen dienst, wat zijn de voor- en nadelen?
12.5	PPP	Graag uitleg..(misschien bewaking Belangrijk persoon, zoals burgemeester?)
12.6	Collectieve beveiliging	Altijd bovenop eigen beveiliging. Goede samenwerking en afspraken.
12.7	Keurmerk en brancheorganisaties	Weten welk keurmerk er is en wat je ervan kan verwachten en onder welke brancheorganisatie dit valt.
12.8	Receptionist (portier-manbewaker)	Weten wat het verschil is en rekening houden met de keuzen van het bedrijf of zij een receptionist(e) willen of een beveiliger die deze taak op zich neemt.
12.9	Uitgangscontrole	Weten wat Visteren en is en hoe dit toegepast kan worden
12.10	Juridisch kader	Hoofdlijnen WPBR. Herkenbaarheid; uniform, V teken enz

Bijlage 1: 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

Bijlage 2: Rapport van deelname workshops (voorbeeld)

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

Rapport van deelname gevolgde workshop

CIBV kandidaatnummer	:	
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?	:	