



# OEK.26 - Stappenplan Cybersecurity gebouwgebonden systemen RVB

Versie	: 1.0
Datum	: dinsdag 22 april 2025
Status	: DEFINITIEF
Rubricering	: INTERN VERTROUWELIJK
Rubriceringsduur	: Tot einde contractduur inclusief verlenging, plus 4 jaar
Auteur	: Rijksvastgoedbedrijf   T&P   A&T   Digitalisering & Beveiliging
Bestand	: 20250422 - OEK 26 Stappenplan Cybersecurity GGS 1.0.docx
Bijlagen	: IBRO, Cybersecurity Raamwerk Gebouw Gebonden Systemen, Cybersecurity Plan, Inventarisatie Systemen.
Verwijzingen wetgeving	: BIO, Meldplicht Security, Meldplicht Privacy AP, CBW-Zorgplicht



## Inleiding

Het Rijksvastgoedbedrijf (RVB) (hierna: de Opdrachtgever) werkt aan het verbeteren van de cybersecurity van haar gebouwgebonden systemen. In dit Stappenplan Cybersecurity staan de stappen die de Opdrachtgever samen met de Opdrachtnemer wil volgen. Dit Stappenplan bestaat uit drie delen:

- A. Cybersecurity – Basisonderhoud en beheer
- B. Cybersecurity – Gedetailleerd onderzoek
- C. Cybersecurity – Verbeterplannen opstellen en uitvoeren

Cybersecurity gaat over de borging van beschikbaarheid, integriteit en vertrouwelijkheid van deze systemen en de daarin besloten gegevens, en als onderdeel daarvan ook het veilig en betrouwbaar beheren van deze systemen en gegevens.

Het uitvoeren van het Stappenplan gebeurt op afroep van de Opdrachtgever, op basis van Bijkomend Werk (BKW). Gedurende de looptijd van de overeenkomst kan de Opdrachtgever **per locatie** vragen om één of meer delen van het stappenplan uit te voeren. Dit is afhankelijk van:

- het risicoprofiel van de Gebruiker;
- de classificatie van locatie en systemen;
- de prioriteiten van de Opdrachtgever of de Gebruiker; en
- de beschikbare capaciteit en middelen.

Een korte toelichting bij de drie gedeelten van het stappenplan:

### **A. Cybersecurity – Basisonderhoud en beheer**

De Opdrachtnemer verifieert en completeert de registratie en documentatie van de aanwezige gebouwgebonden systemen. Daarnaast worden, in samenwerking met de Opdrachtgever, de processen die noodzakelijk zijn voor basisbeheer en het naleven van wettelijke verplichtingen gecontroleerd en, waar nodig, ingericht of bijgesteld.

### **B. Cybersecurity – Gedetailleerd onderzoek**

De Opdrachtnemer brengt, op aanwijzing van en in samenwerking met de Opdrachtgever en de Gebruiker, (een selectie van) de gebouwgebonden systemen en netwerken gedetailleerd in kaart, inclusief de daarin aanwezige gegevens. De Opdrachtgever classificeert zowel de systemen en netwerken als de daarin aanwezige gegevens in detail, en bepaalt de bijbehorende risiconiveaus.

### **C. Cybersecurity – Verbeterplannen opstellen en uitvoeren**

De Opdrachtgever stelt in samenspraak met de Gebruiker de scope van uit te voeren verbeteringen vast op basis van de geïdentificeerde risiconiveaus. Dit omvat:

- (een selectie van) de gebouwgebonden systemen en netwerken
- (een selectie van) van toepassing zijnde normen op basis van het Cybersecurity Raamwerk (CSR).

De Opdrachtnemer stelt vast op welke punten het geboden beveiligingsniveau van de systemen en netwerken niet voldoet aan de normen zoals vastgelegd in het Cybersecurity Raamwerk (gap-analyse). Als er tekortkomingen zijn, stelt de Opdrachtnemer hiervoor een verbeterplan op. Dit plan, of een gedeelte ervan, wordt na goedkeuring door de Opdrachtgever uitgevoerd.



### **Wettelijke basis**

De Rijksoverheid, haar Opdrachtnemers (beheerpartijen / leveranciers) én de Gebruikers moeten aantoonbaar (gaan) voldoen aan de wet- en regelgeving op het gebied van cybersecurity ofwel informatiebeveiliging. Vigerende wet- en regelgeving cybersecurity is onverkort van toepassing op alle gebouwgebonden systemen en bijbehorende netwerken.

Voor de Rijksoverheid zijn de normen voor cybersecurity vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO)<sup>1</sup> en de Cyberbeveiligingswet (Cbw)<sup>2</sup> die voortkomt uit de Europese NIS2-richtlijn<sup>3</sup>. Daarnaast gelden voor specifieke Gebruikers en specifieke gebouwfuncties extra eisen, afhankelijk van de bijbehorende rubricering en classificatie.

Tijdens de looptijd van de Overeenkomst worden significante aanpassingen in wet- en regelgeving rondom cybersecurity verwacht. Hierdoor moeten misschien ook de contractuele afspraken worden aangepast. De Opdrachtnemer wordt hierover periodiek geïnformeerd, inclusief updates over relevante normen en hoe we hier samen actief mee omgaan.

### **Regelgeving: Cybersecurity Raamwerk (CSR) en CyberSecurity Plan (CSP)**

Als referentiedocument voor het beveiligen van gebouwgebonden systemen en de daarin besloten informatie heeft de Opdrachtgever het Cybersecurity Raamwerk Gebouwgebonden Systemen<sup>4</sup> (CSR) opgesteld. Dit raamwerk is gebaseerd op de BIO. Voor een aantal gebruikersgroepen zoals bijvoorbeeld de Dienst Justitiële Inrichtingen, de Belastingdienst en de Rechtspraak zijn specifieke aanvullingen opgenomen.

In een Cybersecurity Plan (CSP) wordt door de Opdrachtnemer per locatie en systeem, de precieze implementatie en de *compliance status* van de normen in het CSR gestructureerd vastgelegd.

**NB.** Het CSR en het CSP worden periodiek getoetst en aangepast aan de vigerende wet- en regelgeving.

### **Cyberinspectie**

De Opdrachtgever kan inspecties op het gebied van cybersecurity (laten) uitvoeren, al dan niet als onderdeel van de jaarlijkse BOEI-inspectie. De Opdrachtnemer is verplicht hier volledig aan mee te werken.

### **Monitoring**

De Opdrachtnemer dient voorzieningen voor monitoring door de Opdrachtgever op Gebouwgebonden systemen en netwerken toe te staan en te faciliteren.

<sup>1</sup> Baseline Informatiebeveiliging Overheid. Zie <https://www.bio-overheid.nl/>

<sup>2</sup> Vaststelling van de Nederlandse Cyberbeveiligingswet wordt verwacht in Q4 2025 [Cyberbeveiligingswet \(RDI\)](#), de Europese NIS2 directive is reeds van kracht.

<sup>3</sup> NIS2 EU richtlijn: [Richtlijn - 2022/2555 - EN - EUR-Lex](#)

<sup>4</sup> Gebouwgebonden systemen: Installaties en bijbehorende netwerken in eigendom van de Opdrachtgever die worden gebruikt voor beveiliging en beheer en exploitatie van gebouwen en terreinen, inclusief interne en externe koppelingen van die installaties.



## **A. Cybersecurity –Inrichting basis onderhoud en beheer**

De Opdrachtnemer verifieert en completeert de registratie en documentatie van de aanwezige gebouwgebonden systemen. Daarnaast worden, in samenwerking met de Opdrachtgever, de processen die noodzakelijk zijn voor basisbeheer en het naleven van wettelijke verplichtingen gecontroleerd en, waar nodig, ingericht of bijgesteld.

### **Meldplicht Privacy- en Security incidenten**

**STAP CS A1:** De Opdrachtnemer is verplicht om binnen 24 uur melding te doen van Privacy-incidenten en van Securityincidenten en -kwetsbaarheden.

- Melding Privacy-incidenten: zie <https://www.autoriteitpersoonsgegevens.nl/datalek-melden>
- Melding Security-incidenten en -kwetsbaarheden: **Nog te bepalen**<sup>5</sup>

Van de melding dient een afschrift te worden verstrekt aan de Opdrachtgever.

**NB:** Voor bepaalde gebruikers kunnen specifieke eisen met betrekking tot melding van privacy- en securityincidenten van toepassing zijn. Opdrachtnemer dient dit af te stemmen met Opdrachtgever en Gebruiker.

### **Zorgplicht Opdrachtnemer**

**STAP CS A2:** De Opdrachtnemer werkt volgens de maatregelen die zijn vastgelegd in de Integrale Beveiliging Rijksvastgoedbedrijf Opdrachten (IBRO)<sup>6</sup>. Essentieel hierbij is de classificatie/rubricering van de informatie die bij de leverancier wordt verwerkt. Aan de hand van deze classificatie/rubricering is in de IBRO vastgelegd welke maatregelen van toepassing zijn.

**STAP CS A3:** Volgens de IBRO moet de Opdrachtnemer ook zijn eigen netwerken en informatiesystemen én de fysieke omgeving waarin deze systemen zich bevinden, beveiligen tegen incidenten met passende beheersmaatregelen.<sup>7</sup>

### **Cybersecurity in overleggen**

**STAP CS A4:** Cybersecurity is een vast agendapunt op het Operationeel overleg, het contractoverleg en het jaarlijkse overleg als vervolg op de jaarlijkse inspectie. Cybersecurity wordt als apart onderwerp opgenomen in de verslaglegging. In deze overleggen wordt Cybersecurity steeds besproken met een ter zake kundig persoon namens de Opdrachtgever.

### **Procesmatige borging cybersecurity / PDCA cyclus**

**STAP CS A5:** De Opdrachtnemer bewaakt samen met de Opdrachtgever de gestelde normen en *best practices* door middel van een PDCA-cyclus (*Plan Do Check Act*).

<sup>5</sup> Zie <https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/infosheet-meldplicht>. De exacte procedure voor melding van cybersecurity incidenten en kwetsbaarheden dient nader te worden afgestemd met de Opdrachtgever én de Gebruiker.

<sup>6</sup> De IBRO is van toepassing op alle RVB contracten die buiten de Rijksoverheid worden afgesloten, exclusief Defensie.

<sup>7</sup> Zie <https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/februari/27/infosheet-nis2-verplichtingen-zorgplicht>.



### ***Risicomanagement***

**STAP CS A6:** De Opdrachtgever hanteert een risicogestuurde aanpak. De Opdrachtnemer houdt hiervoor een risicodossier bij met betrekking tot cybersecurity-aspecten van de systemen die hij in onderhoud heeft. Op basis hiervan stelt de Opdrachtnemer verbeterplannen op, die door de Opdrachtgever worden goedgekeurd of afgewezen.

**NB.** De Opdrachtgever bepaalt de prioriteit bij het verhelpen van geconstateerde gebreken ten aanzien van de normen en *best practices*. Dit op basis van de financiële mogelijkheden, urgentie en rubricering en/of classificatie van de locaties, systemen en gegevens. De controle en evaluatie van de verbeterplannen vinden plaats op drie momenten:

- bij het Operationeel overleg (voor de afstemming van implementatie);
- in het contractoverleg: budgettering/controle voortgang; en
- tijdens het jaarlijkse overleg op basis van de jaarlijkse inspectie.

### ***Privacy - verwerkersovereenkomsten***

**STAP CS A7:** Als er sprake is van verwerking of aanwezigheid van persoonsgegevens, stellen de Opdrachtnemer en de Opdrachtgever een verwerkersovereenkomst op als onderdeel van het contract. Hierin worden afspraken vastgelegd over opslag, verwerking en beveiliging van persoonsgegevens.

**STAP CS A8:** Als er sprake is van de verwerking of aanwezigheid van persoonsgegevens, dan zullen ook de leveranciers in de leveranciersketen een verwerkersovereenkomst met Opdrachtnemer moeten opstellen en ondertekenen. Hierin worden afspraken vastgelegd over opslag, verwerking en beveiliging van persoonsgegevens. De Opdrachtnemer levert hiervan bewijs aan.

### ***Regulier onderhoud, specifieke bepalingen***

Voor het reguliere onderhoud van systemen en netwerken gelden specifieke bepalingen met betrekking tot controle, reparatie, *patches* en *updates*.

#### **Inventaris**

**STAP CS A9:** De Opdrachtnemer houdt per locatie een inventaris bij van de Gebouwgebonden systemen en netwerken die hij in beheer heeft, inclusief rubricering, classificaties, documentatie etc.

**NB.** Deze gegevens zijn en blijven eigendom van de Opdrachtgever.

#### **Vakbekwaamheid leveranciers**

**STAP CS A10:** De Opdrachtnemer is verplicht het cybersecurity-onderhoud aan systemen uit te laten voeren door deskundige partijen. Deze partijen moeten **aantoonbaar bekwaam** zijn voor de systemen die zij onderhouden, bijvoorbeeld door relevante certificeringen en/of succesvol afgeronde, vereiste opleidingen.

**STAP CS A11:** De Opdrachtnemer onderhoudt een *register vakbekwaamheid leveranciersketen* met daarin de bewijsstukken van:

- vakbekwaamheid voor de specifieke systemen en netwerken die onder dit contract vallen; en
- vakbekwaamheid cybersecurity.

#### **Onderhoudsfrequentie**

**STAP CS A12:** Opdrachtnemer voert cybersecurity-onderhoud van systemen als volgt uit:



- *Air gapped* systemen<sup>8</sup>: minimaal 2x per jaar *patchen/updates* en controles uitvoeren;
- Verbonden systemen<sup>9</sup>: minimaal 6x per jaar *patchen/updates* en controles uitvoeren;

### **Externe verbindingen**

**STAP CS A13:** Externe verbindingen op gebouwgebonden systemen:

Als de Opdrachtnemer expliciete toestemming van Opdrachtgever heeft om externe verbindingen te gebruiken voor het gebruik, onderhoud en/of beheer op gebouwgebonden systemen op een locatie, dan zijn daarvoor de volgende normen van toepassing:

- Alle componenten die onderdeel uitmaken van externe connectiviteit zijn op basis van zero trust ontworpen (zie CSR);
- Externe connecties en ontwerpen moeten expliciet goedgekeurd worden door de Opdrachtgever;
- Updates voor detectie worden geautomatiseerd bijgewerkt binnen 1 uur na vrijgave.
- Externe verbindingen worden 24/7 gelogd en gemonitord.

**NB:** Niet toegestane externe verbindingen worden verwijderd in afstemming met Opdrachtgever.

### **Logisch toegangsbeheer**

**STAP CS A14:** Bij logisch toegangsbeheer is de Opdrachtnemer verantwoordelijk voor de volgende taken:

- Inventariseren of de logische toegang tot Gebouwgebonden systemen (zoals accounts, wachtwoorden en extra beveiligingsfactoren) is ingericht conform het CSR, of de door de Opdrachtgever aangewezen *best practice*.
- Zorgdragen dat de logische toegang voldoet aan de afgesproken beheersmaatregelen, met ingang van een datum die is overeengekomen met de Opdrachtgever;
- Borgen van de naleving van deze beheersmaatregelen gedurende de looptijd van het beheer.

### **Security Incidentafhandeling - Analyse**

**STAP CS A15:** Cybersecurity-incidenten worden door de Opdrachtnemer in alle gevallen opgevolgd met een *Root Cause Analysis* (grondoorzakenanalyse). De uitkomst hiervan wordt gecommuniceerd met de Opdrachtgever.

### **Rapportage**

**STAP CS A16:** De Opdrachtnemer rapporteert periodiek aan de Opdrachtgever in het Contractoverleg en tijdens de Jaarrapportage naar aanleiding van de jaarlijkse inspectie.

### **Rapportage voor het contractoverleg**

- Status en historie security incidenten, kwetsbaarheden en meldingen.

### **Jaarrapportage (op basis van de jaarlijkse inspectie)**

#### *Assets*

- Actueel overzicht systemen en netwerken;
- Invulling rechten en rollen ter review/accordering management.

<sup>8</sup> *Air gapped* systemen: systemen die geen connectiviteit hebben buiten de locatie.

<sup>9</sup> Verbonden systemen: systemen die connectiviteit hebben buiten de locatie.



### *Risicomanagement*

- Actueel risicoregister.

### *Leveranciersketen*

- Actueel register Vakbekwaamheid van onderhoudspartijen voor de te onderhouden systemen.
- Beheersing cybersecurity met betrekking tot leveranciersketen.
- Afhankelijkheden, afspraken en alternatieven in de leveranciersketen in verband met leveringszekerheid.



## **B. Cybersecurity – Gedetailleerd onderzoek**

De Opdrachtnemer brengt - op aanwijzing van en in samenwerking met de Opdrachtgever en de Gebruiker - (een selectie van) de gebouwgebonden systemen en netwerken gedetailleerd in kaart, inclusief de daarin aanwezige gegevens. De Opdrachtgever classificeert zowel de systemen en netwerken als de daarin aanwezige gegevens in detail, en bepaalt de bijbehorende risiconiveaus.

### **Ondersteuning vanuit Opdrachtgever**

De Opdrachtgever biedt ter ondersteuning:

- een bijlage Inventarisatie systemen<sup>10</sup>, waarin is vastgelegd welke informatie wordt gevraagd;
- een sjabloon Cybersecurityplan waarin Opdrachtnemer de verzamelde, en nieuwe documentatie vastlegt;
- de *Webbased* applicatie van de Opdrachtgever en daaraan gerelateerde tools.

**NB.:** De beschikbaarheid van de ondersteunende middelen van de Opdrachtgever is afhankelijk van interne ontwikkelingen.

### ***Inventarisatie en Registratie***

De eerste stap in het realiseren van een effectief cybersecurity-beheer, is het op orde brengen van de documentatie, rubricering en de classificatie van gebouwgebonden systemen.

### **Systemen en netwerken**

**STAP CS B1:** De Opdrachtnemer inventariseert en documenteert, op verzoek van de Opdrachtgever, de gebouwgebonden systemen en -netwerken in detail volgens de specificaties in de bijlage Inventarisatie systemen.

**STAP CS B2:** De Opdrachtnemer geeft voor de classificatie van gegevens gedetailleerd inzicht in de data(velden) die in de gebouwgebonden systemen zijn vastgelegd en over koppelvlakken worden uitgewisseld.

### **Compliance**

**STAP CS B3:** De Opdrachtnemer vraagt de Opdrachtgever naar de rubricering en classificatie van systemen en houdt per locatie een overzicht bij van de verschillende rubriceringen en classificaties voor elk systeem en de verschillende koppelvlakken.

### **Rubricering en Classificatie van locaties, systemen en gegevens**

Voor het doelgericht kunnen uitvoeren van het onderhoud houdt de Opdrachtnemer overzicht op de rubricering en classificatie van locaties, systemen en gegevens. De Opdrachtgever rubriceert en classificeert.

#### *Rubricering*

De Opdrachtgever stelt de rubricering op basis van Te Beschermen Belang (TBB) beschikbaar voor een groot aantal locaties en systemen via de *Webbased* applicatie.

---

<sup>10</sup> OEK26 Bijlage CS - Inventarisatie systemen





#### *Classificatie op basis van kritikaliteit*

De Opdrachtgever bepaalt het belang van een locatie en de daarin aanwezige systemen en netwerken. Een locatie en/of systeem is 'kritisch'<sup>11</sup> of 'niet kritisch'. Dit is afhankelijk van de bedrijfsprocessen die op een locatie plaatsvinden.

#### *Classificatie gevoeligheid BIV(R)*

De gevoeligheid van gebouwgebonden systemen en netwerken wordt bepaald op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) en relevante Regelgeving (R). Dit wordt in detail vastgesteld in overleg met de Opdrachtgever.

#### *Classificatie gevoeligheid Privacy*

De privacygevoeligheid van gegevens die aanwezig zijn in de gebouwgebonden systemen moeten volgens de Algemene verordening gegevensbescherming (AVG) in detail worden vastgesteld in afstemming de Opdrachtgever.

**STAP CS B5:** De Opdrachtnemer registreert de inventarisatie in het Cybersecurity Plan (CSP) van de betreffende locatie(s) en/of de *Webbased* applicatie van de Opdrachtgever.

Locatie	Systeem	Koppelvlak met	Rubricering	Kritisch J/N	BIV(R)	Privacy gegevens

<sup>11</sup> Kritisch: Uitval van locatie en/of systeem heeft significante impact heeft op het primaire proces, de bedrijfsvoering en/of de te beschermen belangen van de Gebruiker.



## **C. Cybersecurity – Verbeterplannen opstellen en uitvoeren**

De Opdrachtgever stelt in samenspraak met de Gebruiker de scope van uit te voeren verbeteringen vast op basis van de geïdentificeerde risiconiveaus. Dit omvat:

- (een selectie van) de gebouwgebonden systemen en netwerken
- (een selectie van) van toepassing zijnde normen op basis van het Cybersecurity Raamwerk (CSR).

De Opdrachtnemer stelt vast op welke punten het geboden beveiligingsniveau van de systemen en netwerken niet voldoet aan de normen zoals vastgelegd in het Cybersecurity Raamwerk (gap-analyse). Als er tekortkomingen zijn, stelt de Opdrachtnemer hiervoor een verbeterplan op. Dit plan, of een gedeelte ervan, wordt na goedkeuring door de Opdrachtgever uitgevoerd.

### **Ondersteuning Opdrachtgever**

De Opdrachtgever biedt ter ondersteuning:

- een sjabloon Cybersecurityplan waarin Opdrachtnemer de verzamelde en nieuw gemaakte documentatie kan vastleggen,
- de *Webbased* applicatie van de Opdrachtgever en eventueel daaraan gerelateerde systemen.

Opdrachtgever en de Opdrachtnemer werken samen aan:

- *best practices* per ingebrachte norm, waarin toepasselijke maatregelen worden uitgewerkt en vastgelegd.
- voorlichting en *tools* voor nieuwe geïntroduceerde normen.

### **Aanpassingen normenkader**

Gedurende de looptijd van de Overeenkomst kunnen bijkomende werkzaamheden per locatie/complex worden gevraagd.

- De Opdrachtgever kan jaarlijks de selectie van normen uit het CSR en toe te passen *best practices* uitbreiden. Voor de implementatie wordt altijd een inventarisatie en een verbeterplan opgesteld voor de gesignaleerde tekortkomingen.
- De Opdrachtgever kan jaarlijks wijzingen en aanvullingen opnemen in het CSR en toe te passen *best practices*. Dit naar aanleiding van wijzigende omstandigheden zoals wijzigingen in wet- en regelgeving. Voor de implementatie wordt altijd een inventarisatie en een verbeterplan opgesteld voor gesignaleerde tekortkomingen.

### **Risico's**

De Opdrachtgever draagt de volgende risico's van het niet of gedeeltelijk voldoen aan normen uit het CSR:

- het risico van niet of gedeeltelijk voldoen aan niet-ingebrachte normen;
- het restrisico van niet of slechts gedeeltelijk opgedragen verbeterplannen met betrekking tot ingebrachte normen.

Opdrachtnemer draagt de volgende risico's van niet of gedeeltelijk voldoen aan ingebrachte normen uit het CSR:

- het risico van incompleet opgeleverde verbeterplannen met betrekking tot de ingebrachte normen



- het risico van het niet (meer) voldoen aan ingebrachte normen na oplevering van in opdracht gegeven verbeterplannen.

### **Selectie van Systemen/netwerken / control-selectie**

**STAP CS C1:** De Opdrachtgever selecteert een set normen en bijbehorende maatregelen en kiest welke systemen en netwerken gecontroleerd of geëffectueerd moeten worden.

De keuze voor bepaalde systemen en netwerken en de keuze voor een set normen en bijbehorende maatregelen zijn afhankelijk van een aantal factoren:

- Classificatie van een locatie;
- Classificatie van het specifieke systeem of netwerk en de daarin aanwezige data.
  - Rubricering
  - Kritikaliteit (het belang)
  - BIV
  - Privacy
- Prioritering en beschikbare resources van de Opdrachtgever.

### **Inventarisatie**

**STAP CS C2** De Opdrachtnemer inventariseert de status van geselecteerde CSR normen voor de systemen en netwerken, signaleert tekortkomingen en verifieert deze met de Opdrachtgever. Geverifieerde risico's worden door de Opdrachtnemer geregistreerd in het risicodossier en door de Opdrachtgever vastgesteld.

### **Verbeterplan opstellen**

**STAP CS C3** De Opdrachtnemer stelt voor de geverifieerde tekortkomingen een verbeterplan op en legt deze ter beoordeling en goedkeuring voor aan de Opdrachtgever.

### **Verbeterplan uitvoeren**

De Opdrachtgever bepaalt of voorgestelde verbeteringen wel of niet worden gerealiseerd.

**STAP CS C4:** De Opdrachtnemer voert goedgekeurde verbeterplannen uit.

Bij de implementatie van normen die door de Opdrachtgever zijn ingebracht, volgt de Opdrachtnemer de volgende stappen in de PDCA cyclus:

1. (P) Normstelling – De Opdrachtgever bepaalt de normen en maatregelen van toepassing
2. (P) GAP analyse - de Opdrachtnemer inventariseert gebreken zoals van toepassing voor bepaalde locaties en systemen en registreert deze in een risicoregister.
3. (P) De Opdrachtnemer stelt op aanvraag de Opdrachtgever een verbeterplan en een kostenraming op voor de geconstateerde tekortkomingen per locatie/systeem;
4. (P) De Opdrachtgever bepaalt of de voorgestelde verbetering binnen of buiten de Overeenkomst valt (BKW of niet)
5. (P) De Opdrachtgever bepaalt of de opdracht ter verbetering wordt verstrekt (bijstelling/aanpassing van de opdracht)
6. (D) Uitvoeren van het verbeterplan
7. (C) Controle op uitvoering
8. (C) Acceptatie door de Opdrachtgever
9. (A) Beheer/Evaluatie



### **Registratie Compliance**

**STAP CS C5:** De Opdrachtnemer onderhoudt voor elke locatie een Cybersecurity Plan (CSP) voor de normen van toepassing uit het Cybersecurity Raamwerk (CSR), zoals vastgesteld voor een specifieke locatie en/of specifieke systemen.

### **Rapportage aanvullend**

**STAP CS C6:** De Opdrachtnemer rapporteert aanvullend in het contractoverleg en bij de jaarlijkse inspectie.

#### **Rapportage voor het contractoverleg (aanvullend)**

- Status verbeterplannen

#### **Jaarrapportage (aanvullend)**

##### *Assets*

- Actuele status compliance aan de door de Opdrachtgever geselecteerde CSR normen.

##### *Risicomanagement*

- Toezicht op de naleving van de geselecteerde CSR normen.
- Actuele status van de risico's en de verbeterplannen.
  - Welke verbeterpunten zijn uitgevoerd;
  - Welke punten uit de jaarlijkse inspectie worden in de verbeterplannen opgenomen voor het komende jaar.