Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Cybersecurity

Aanpak bij RWS

Hoofdwatersysteem (HWS)

90.219 km²
Wateroppervlak
incl. BES-eilanden

3.030 km²
Binnenwater

293 km
Kustlijnzorg

6
Stormvloed-
keringen

34 km
Primaire
dijken

122 km
Primaire
dammen

45 km
Primaire
duinen

507 km
Niet-primaire
dijken

98 km
Niet-primaire
duinen

10
Stuwen

86
Spui- en
uitwateringskolken

19
Gemalen

Hoofdvaarwegennet (HVWN)

3.646 km
Zeetoegangsgeulen en zeecorridors

3.426 km
Kanalen, rivieren en vaargeulen binnenwater

592 km
Verkeers-begeleiding

12
Verkeersposten

92
Sluiscomplexen met **131** schutsluiskolken

237
Vaste bruggen

112
Beweegbare bruggen

24
Vuurtorens incl. **6** op BES-eilanden

Hoofdwegennet (HWN)

3.078 km
Wegen

5.846 km
Hoofdrijbanen

716 km
Verbindingswegen en parallelbanen

896 km
Op- en afritten

308 km
Spitsstroken

2.931 km
Verkeers-signalering

6
Verkeers-centrales

17
Aquaducten

741
Vaste bruggen

50
Beweegbare bruggen

20
Tunnelcomplexen met **28** tunnels

2.914
Viaducten

56
Ecoducten

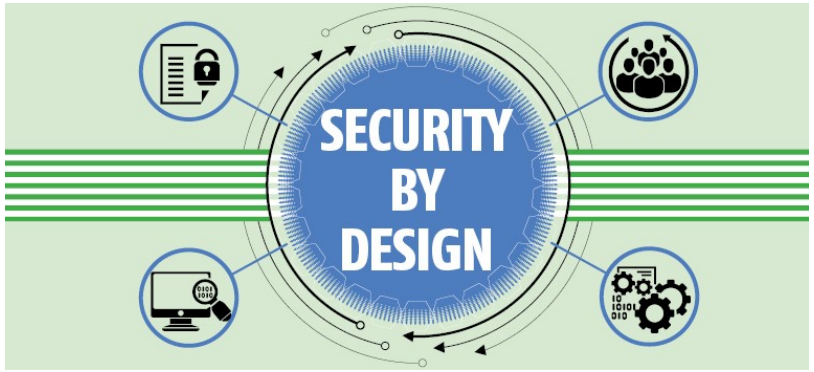
14
Aanleginrichtingen (veren)

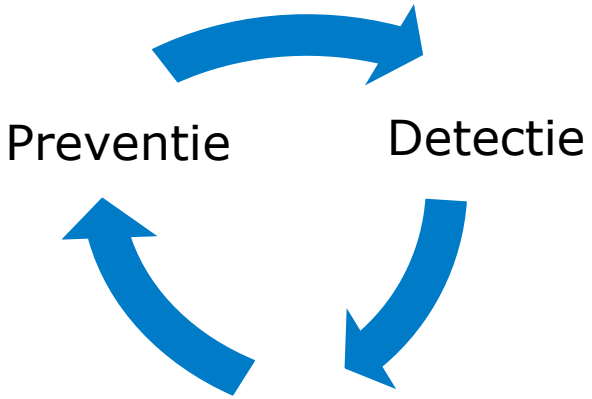
Digitalisering RWS

Gebruik van informatietechnologie (IT) en operationele technologie (OT)

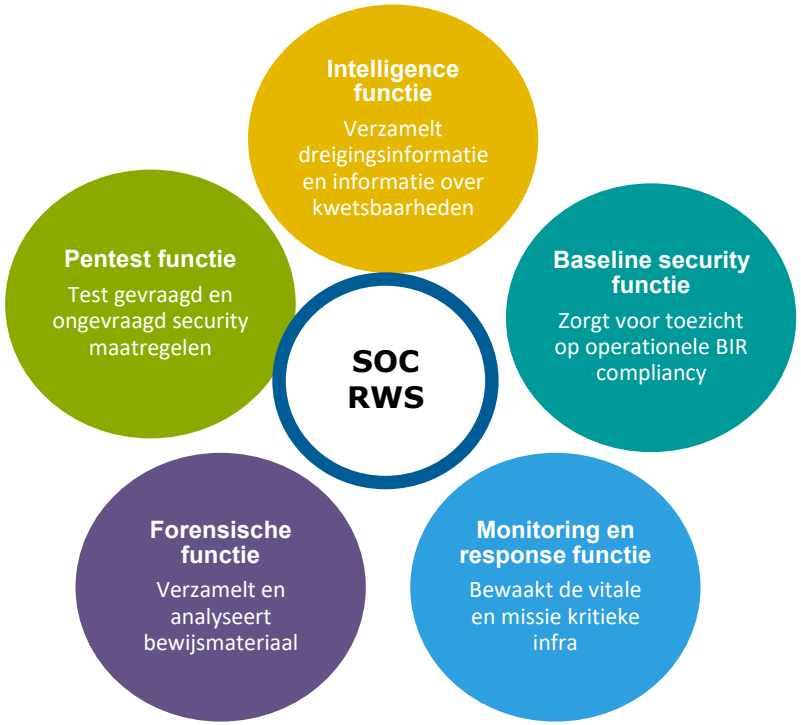
Digitale weerbaarheid

Cybersecurity
een opgave van ons allemaal





7x24 Incident mangement



Cybersecurity
digitale veiligheid

Security by Design proces

Security is integraal onderdeel van het te ontwerpen, bouwen, realiseren en te exploiteren Systeem. Dit betekent dat security integraal onderdeel moet worden van het ontwikkel, beheer en onderhoudsproces gedurende de hele life cycle.

Twee sporen voor security by design

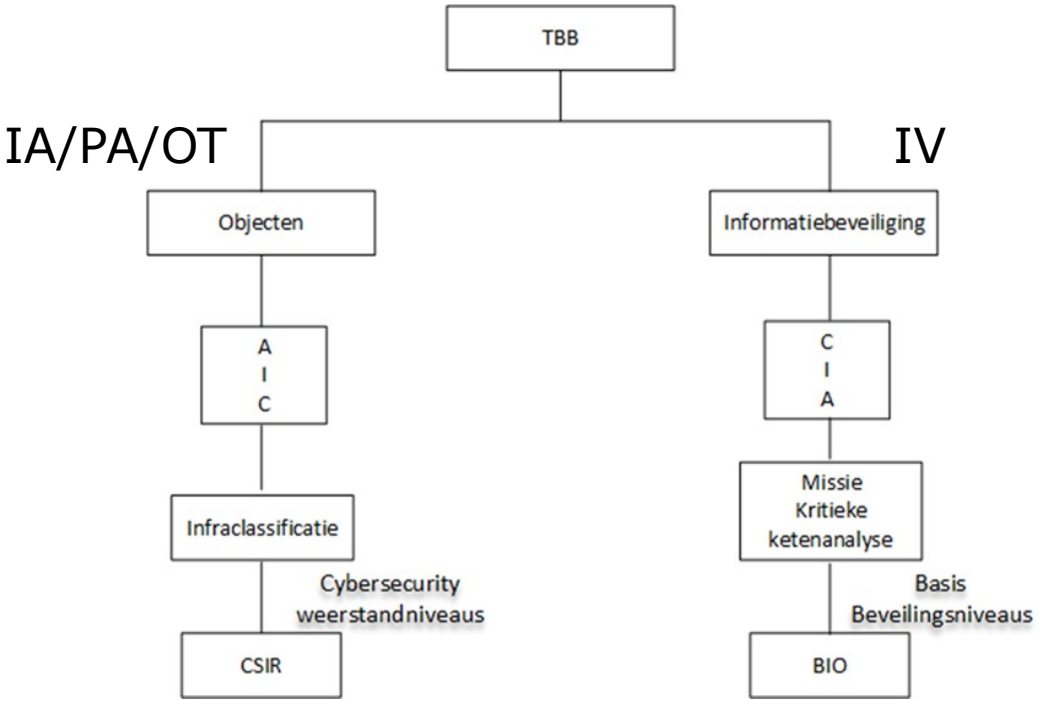
I – Security by Design voor Informatievoorziening (IV)

BIO (ARBIT/ARVODI) (ISO 27001)

II – Security by Design voor Industriële Automatisering (IA/PA/OT)

CSIR (UAV-GC) (ISO 27001 + IEC62443)

Cybersecurity aanpak IA en IV

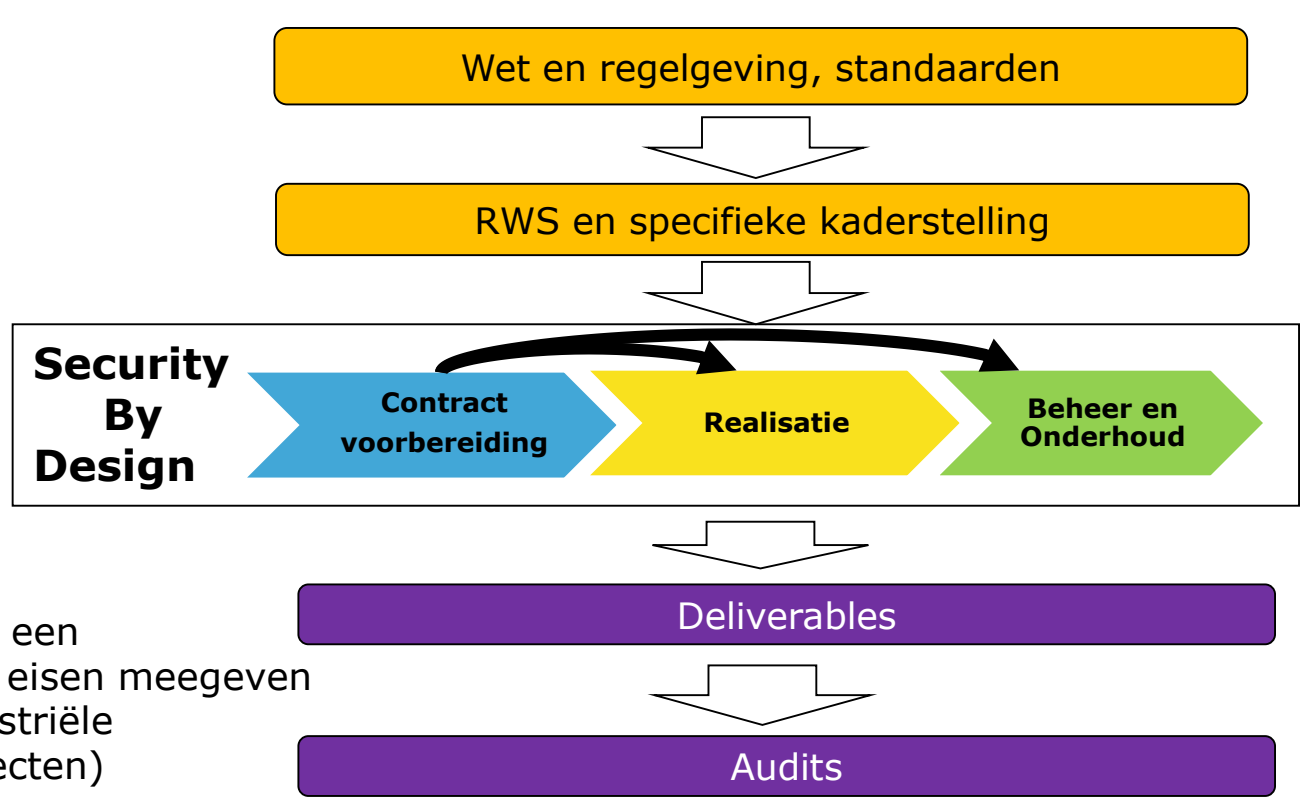


- Processen AO en OAM
- UAV-GC inkoop contract
- Systems engineering
- ISO27001 + IEC 62443

- IV proces
- ARBIT/ARVODI inkoop contract
- ICT werkwijze
- ISO 27001/02

- Bij Informatie Voorziening (IV) focus op de informatie en de vertrouwelijkheid ervan
- Bij Industriële Automatisering (IA) focus op de functies van het object of systeem/proces en de betrouwbaarheid ervan
- Bij Industriële Automatisering ook focus op safety.
- Bij IV wordt betrouwbaarheid gedefinieerd in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) met focus op informatie
- Bij IA wordt betrouwbaarheid en beschikbaarheid afzonderlijk gedefinieerd met de focus op de functies van het object middels RAMSSHEEP aspecten
- Bij IV is de Baseline Informatiebeveiliging Overheid (BIO) leidend
- Bij IA is aanvullende normering nodig hiervoor heeft RWS een Cyber Security Implementatie Richtlijn (CSIR) ontwikkelt

Implementatie SBD bij RWS



RWS = Regie organisatie

NIS/WBNI, BIO*, ISO 2700x, IEC 62443

Cyber Security Implementatie Richtlijn (CSIR)

Aanleg & Onderhoud

Assetmgt

Cybersecurity Dossier

Audits / toezicht

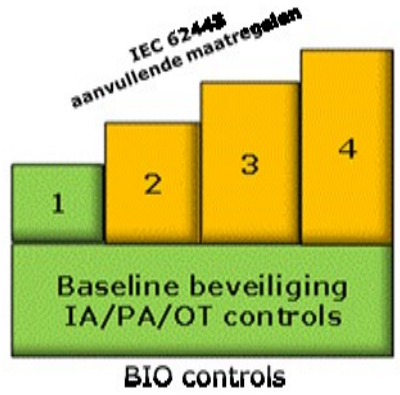
- Zo vroeg mogelijk in een bouwtraject security eisen meegeven
- Zowel bij IT als Industriële Automatisering (objecten)
- Voor IT: BIO
- Voor IA: CSIR (CyberSecurity Implementatie Richtlijn Objecten)

* Baseline Informatiebeveiliging Overheid

CSIR uitgangspunten

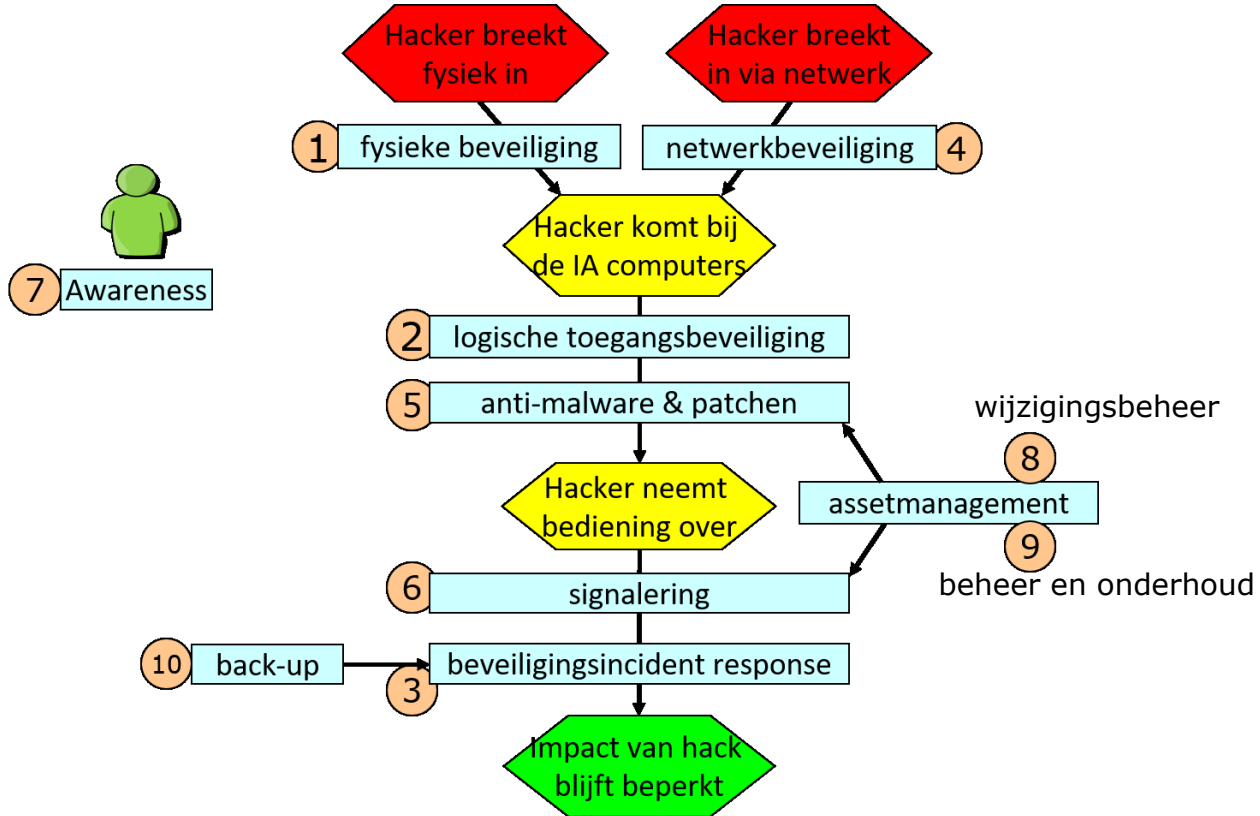
- Contractuele borging Cybersecurity met ca 70 proces- en 40 techniekeisen

- Infraclassificatie objecten met cybersecurity weerstandsniveaus



Op basis van het cybersecurity **weerstandsniveau (1-4)** wordt een aanvullende set met security maatregelen bepaald.

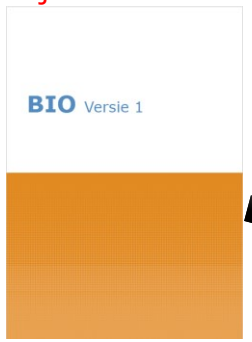
- Eisen en maatregelen obv risico's en gelaagde beveiliging



Cyber Security Implementatie Richtlijn (CSIR)

Kaders & Richtlijnen

Rijkskader BIO



27001 beheersdoelen
27002 maatregelen

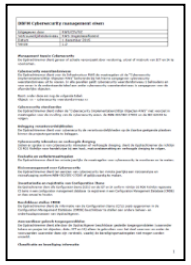
IEC 62443

Controls
maatregelen

Inkoop contracteisen

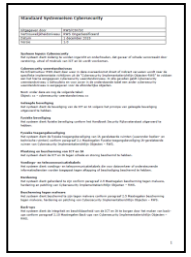
controls

PA/OT/IA **proces** eisen



69 controls

PA/OT/IA **Systeem** eisen

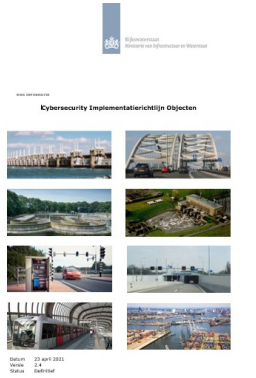


39 controls

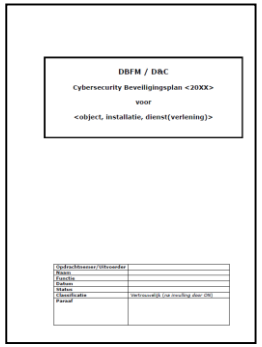
Contract documenten

maatregelen

CSIR 3.x



- 10 paragrafen met de te treffen cybersecurity maatregelen (100-en)
- 23 security richtlijnen



Cybersecurity dosier

Voor uitwerking, beheer en onderhoud van de cybersecurity maatregelen conform de jaarlijkse PDCA cyclus

centrum informatiebeveiliging en privacybescherming

De ICO-Wizard

Inkoopeisen Cybersecurity Overheid

Met deze Wizard stel je een set van informatiebeveiligingseisen samen voor inkopen/aanbestedingen en contracten. Desgewenst met diverse supplementen, waaronder privacy-eisen en eisen uit de ABDO.

Selecteer hieronder en op de volgende schermen wat van toepassing is en druk op Resultaat. Daarna kan de set opgevraagd worden in Word en Excel. Handig om (evt. met eigen aanpassingen/aanvullingen) mee te sturen met de aanbesteding of het inkoopcontract.

Klik hier voor meer informatie over de ICO-Wizard (o.a. handreiking inkoop en ICO en tips bij invullen van de Wizard).

1 2 3 4 5

Inkoop-onderdelen. Kies er tenminste één.

- [ ] Algemeen Ketenpartners
- [ ] Clouddiensten
- [ ] DiGiD Applicaties
- [ ] Maatwerk of maatwerkpakket
- [ ] Mobiele apparatuur & telewerken
- [x] Procesautomatisering (IACS-toepassingen)
- [ ] Softwarepakketten
- [ ] Applicatieontwikkeling algemeen
- [ ] Communicatievoorzieningen
- [ ] Huisvesting IV
- [ ] Middleware
- [ ] Mobiele Applicaties
- [ ] Serverplatform
- [ ] Toegangsbeveiliging

100/108 eisen geselecteerd

Naam	Referentie code norm	Referentie brondocument	Samenvatting eis	Suggesties voor Verificatie	Relevante standaard PToLU-lijst For Standaardisatie
Risicoanalyse	VSP04	VSP/VSE-eisen CSIR3.100	De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever. In de exploitatiefase dient de Opdrachtnemer ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken.	Overleg bewijsstukken en/of verklaring	
Aanstellen verantwoordelijke cybersecurity	VSP05	VSP/VSE-eisen CSIR3.99	De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de Werkzaamheden met betrekking tot cybersecurity.	Overleg bewijsstukken en/of verklaring	
Proces voor kwetsbaarheidsmeldingen	VSP06	VSP/VSE-eisen CSIR3.98	De opdrachtnemer dient een proces in te richten voor het ontvangen van meldingen van kwetsbaarheden van buitenaf conform de "Leidraad Coordinated Vulnerability Disclosure" van het Nationaal Cyber Security Centrum.	Overleg bewijsstukken en/of verklaring	
Cybersecurity-eisen aan test- en onwikkelomgeving	VSP07	VSP/VSE-eisen CSIR3.97	De Opdrachtnemer dient de eisen ten aanzien van cybersecurity onverkort aan te houden bij de inrichting en onderhoud van een test- en ontwikkelomgeving.	Overleg bewijsstukken en/of verklaring	
			De Opdrachtnemer dient voor alle beheerobjecten de		

Cybersecurity - 3 Sporen Aanpak

Nieuwe systemen of objecten

Voorbereiding → Realisatie Ontwerp/bouw → Beheer en onderhoud tot end of life

SbD IT - BIO
SbD OT/IA/PA - CSIR

Security eisen voor inkoop

Uitleveren security eisen

Review security eisen

Compliance of explain aanvraag

PDCA cyclus Cybersecurity Beveiligingsplan

Cybersecurity Risico Management

Ranking tool kwetsbaarheden

PEN testen

Bestaande systemen of objecten met installed technical base

SbD IT – BIO ??
SbD OT/IA/PA – CSIR ??

CSIR Assessment tool

Beheer en onderhoud tot end of life

Bekendheid, samenwerking en toepasbaarheid

Opvraagbaar via:

https://www.bio-overheid.nl/ico-wizard/

csir@hetwaterschapshuis.nl


Den Haag filevrij
Gouda filevrij