Cybersecurity-voorschrift voor OT

Topdocument voor de beheersing van digitale beveiliging van GVB's Operationele Technologie

Versie: 1.7

Vertrouwelijkheidsniveau: Bedrijfsvertrouwelijk

GVB Door en door Amsterdam

Colofon

Vastlegging en beheer
De documenten worden beheerd door de Cybersecurity-office van GVB.
De documenten voor Cybersecurity OT worden vastgesteld door de Cybersecurity Board OT.
De documenten voor Cybersecurity OT vind je op het intranet van GVB onder ‘Cybersecurity OT’:
https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx

Versiebeheer en status
[] 6 jul 2022, Versie 1.7, In deze versie zijn alle Cybersecurity-eisen OT als bindend gesteld. Er kan door middel van een comply-or-explain worden afgeweken. In deze versie wordt ook het Cybersecurity-exceptieregister OT geïntroduceerd. Status: Deze versie dient te worden vastgesteld door de CybersecurityBoard OT.
[] 16 juni 2022, Versie 1.6, Deze versie is een inhoudelijke 1op1-omzetting van MET naar de layout van GVB op basis van het Cybersecurity Voorschrift OT MET, CEB/OVG/21876, versie 1.5, 14 juni 2021 dat met VTW ‘METRO0032’ geaccordeerd is door het CCB/Change Control Board in de vergadering van 28 januari 2021, onderdeel is geworden als Segmentspecificatie van het iPvE en vigerend is voor alle nieuwe projecten/wijzigingen/systemen van RS/RIB, RM, EX. Status: Met dit besluit in het CCB is het vigerend voor alle Operationele Technologie. Naast de 1op1-omzetting is dit document aangepast aan de GVB-organisatie en zijn enkele tekstuele verbeteringen aangebracht.
[] 14 juni 2021, Versie 1.5, Documenten/Referentielijst bijgewerkt, paragraaf 4.1.1
[] 5 augustus 2020, Versie 1.4, Hoofdstuk 3 Verantwoordelijkheden en hoofdstuk 7 PDCA aangevuld met de rol van systeem Cybersecurity-officer.
[] 6 februari 2020, Versie 1.3, Enkele aanscherpingen en typos door Wim van Asperen, Cybersecurity-officer OT MET, Status: Versie 1.3 is op 6-6-2020 getekend door Jacco de Regt, Manager Strategisch Assetmanagement, E&B, MET en is een onderdeel van het Meerjarenplan Cybersecurity OT.
[] 16 januari 2020, Versie 1.2, Opmerkingen van Hans Deuss en Andre van der Veen verwerkt.
[] 14 januari 2020, Versie 1.1, Opmerkingen van Frank Visscher MET/SI verwerkt.
[] 6 januari 2020, Versie 1.01, Hoofdstuk Toepasselijkheid toegevoegd door W.L. Van Asperen.
[] 16 december 2019, Versie 1.0, door W.L. van Asperen Cybersecurity & Privacy Officer OT MET

Contactpersoon Cybersecurity-officer OT, Wim van Asperen
Doorkiesnummer 0621854536

Inhoudsopgave

1 Inleiding

Dit is het **top-document** dat als inleiding fungeert voor de aanpak binnen GVB voor de digitale beveiliging (cybersecurity) van de Operationele Techniek (OT).

Met 'OT' wordt bedoeld alle bedienings- en bewakingssysteem voor OV en vastgoed (#Beleid).

> *Voorbeelden (niet-limitatief) zijn: centrale bediening, voedingsystemen, intercom, camerasystemen, verkeersleiding, liften, roltrappen, cctv- en gebouwbeheersystemen.*

2 Het doel van cybersecurity voor OT

Het doel van digitale beveiliging van de operationele systemen is het faciliteren van de

- **Veiligheid** (voorkomen van letsel reizigers en personeel)
- **Beschikbaarheid** (dienstregeling en algemene belemmeringen in de operatie)
- **Privacy** (voorkomen van datalekken van persoonsgegevens in de OT).

en alle afgeleide schade, zoals financiele (vervolg- en herstel)schade en imagoschade (#Beleid).

Op systeemniveau betekent dit dat gewerkt wordt aan de **beschikbaarheid**, de **integriteit** en **vertrouwelijkheid** (BIV) van de OT zélf en gegevens in de OT.

3 Toepasselijkheid

Dit document is voor alle bedrijfsonderdelen van GVB van toepassing die over OT beschikken, waarin **software** is opgenomen.

> Met **software** wordt bedoeld geprogrammeerde logica in de breedste zin van het woord, zoals - niet limitatief - applicatiesoftware, operating system, system utilities, netwerk- en communicatiesoftware, configuratiebestanden, firmware en embedded software.
>
> NB. Daar **hardware** zoals processoren ook gecompromitteerd kunnen zijn, kan ook hardware een onderwerp van beschouwing zijn. In dit document benoemen we dat echter verder niet expliciet.

'Systeem' is (onderdeel van) **assets** of objecten dat software bevat over de **hele levenscyclus**: vanaf een PID tot en met het operationele gebruik en beheer, renovatie en beëindiging.

4 Beleid OT

Dit document beschrijft ook de beleidsaspecten van de Cybersecurity OT. Dit wordt aangegeven met '(#Beleid)' achter de zin die het beleid betreft. Zoek op #Beleid in dit document voor alle beleidsaspecten.

5 Verantwoordelijkheden

Cybersecurity is een lijnverantwoordelijkheid (#Beleid). Dat betekent dat - afhankelijk van de life cycle waar het Systeem zich in bevindt - de opdrachtgever, de project- of areaal/asset-manager en directie(s) verantwoordelijk zijn voor de cybersecurity bepalen welke maatregelen nodig zijn, na afstemming met en advies van de (toekomstige) gebruikers en/of beheerders (c.q. eigenaren, opdrachtgevers, beheerleveranciers).

De Cybersecurity-office GVB zorgt voor de inrichting en implementatie van het integrale ISMS (Information Security Management Systeem) in en begeleidt en adviseert de lijnorganisatie bij het toepassen van het ISMS c.q. de richtlijnen, eisen en de voorschriften. De Cybersecurity-office adviseert en begeleidt (#Beleid) de lijnorganisatie.

De **Cybersecurity-organisatie** kent de volgende indeling:

- Cybersecurity Board OT:
  - Regie en strategie door vertegenwoordigers van Vervoerregio, Safety Board, Cybersecurity-office GVB en van de betrokken bedrijfsonderdelen.
- Cybersecurity-office GVB:
  - Centrale afdeling GVB Holding, onder leiding van CISO van GVB (Holding)
- Cybersecurity-officer OT (bedrijfsonderdeel):
  - Aanspreekpunt voor Cybersecurity voor een GVB-bedrijfsonderdeel en functioneel onderdeel van de Cybersecurity-office GVB, richt zich op de implementatie van het ISMS en voor advies en begeleiding in het betrokken bedrijfsonderdeel.
- ProjectCybersecurity-officer:
  - Gedurende het project en inclusief de overdracht naar beheer, het aanspreekpunt voor de projectmanager, de areaal/assetmanager, de Cybersecurity-officer OT en de opdrachtnemer(s) en draagt zorg voor het toepassen van de uitvoering van de cybersecurity-richtlijnen.

In de opstartfase fase van een project (voor de ontwikkeling van een nieuw systeem, wijziging of renovatie) dient de rol 'projectcybersecurity-officer' te worden ingevuld door een medewerker die daarvoor wordt aangesteld door de respectievelijke opdrachtgever, de project- of areaal/assetmanager. Afhankelijk van de omvang van het project is dat meestal een parttime rol. De projectcybersecurity-officer draagt zorg voor de uitvoering van de cybersecurity namens de opdrachtgever of de projectmanager en op basis van dit Cybersecurity-voorschrift OT. De project cybersecurity-officer rapporteert in de lijn aan de opdrachtgever of de projectmanager en functioneel aan de Cybersecurity-officer OT die adviseert bij of helpt met het opstellen van een voor het systeem en project specifieke aanpak, maatregelen en documenten.

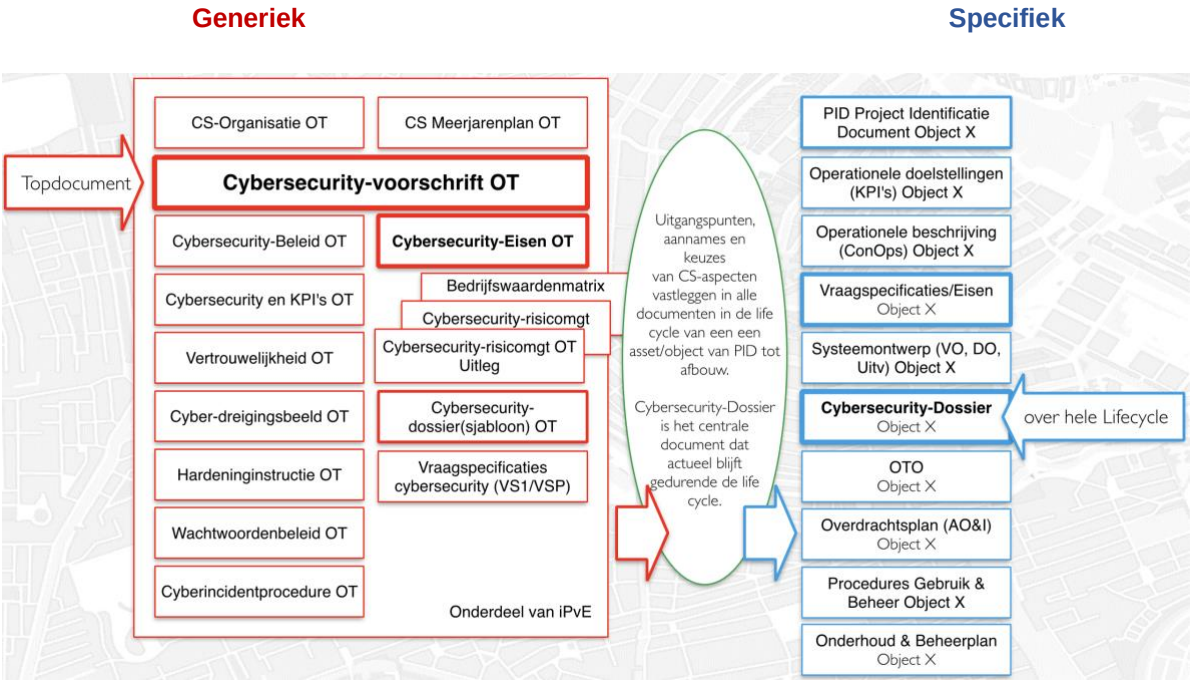
In de **beheerfase** van een systeem is de areaal/asset-manager de verantwoordelijke. De cybersecurity-rol wordt dan ingevuld door de Cybersecurity-officer OT van het betrokken GVB-bedrijfsonderdeel voor advies en begeleiding.

De Cybersecurity-officer OT kan en zal escaleren in geval de opdrachtgever, de project- of areaal/assetmanager - volgens het oordeel van de Cybersecurity-officer OT - te grote (rest)risico's laat, maar de beheerder of opdrachtgever en gebruikersorganisatie (ultiem: directie GVB) bepalen uiteindelijk of restrisico's acceptabel zijn.

6 Het gebruik van dit voorschrift

Dit hoofdstuk geeft een korte beschrijving van alle **(rode) cybersecurity-**richtlijnen die van toepassing zijn en die de leidraad vormen voor de cybersecurity-aanpak voor een specifiek Systeem. Zie hoofdstuk 7 ‘De cybersecurity-richtlijnen’.

De (**blauwe) systeem-specifieke** documenten hieronder zijn **voorbeelden** (niet limitatief!) van documenten die een Systeem begeleiden door de **hele levenscyclus**. De project- of areaal/asset manager (afhankelijk van de life cycle) draagt zorg voor het opstellen en/of beheren van die documenten. Zie hoofdstuk 8 ‘Systeemspecifiek aandachtspunten en documenten’.



Referenties/Bijlagen

De vigerende versies van de gespecificeerde documenten zijn gegeven op de intranet-pagina en dienen als bindende bijlagen bij dit Cybersecurity-voorschrift OT en bij een aanbesteding:

https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx

7 De cybersecurity-richtlijnen

Hieronder volgt de uitleg voor het doel en het gebruik van de (rode) cybersecurity-richtlijnen.

Cyberdreigingsbeeld

Het Cyberdreigingsbeeld beschrijft de dreiging die we mogen verwachten uit de wereld en veronderstellen relevant te zijn voor bediening- en bewakingssystemen van het OV in Amsterdam. Het Cyberdreigingsbeeld OT is bedoeld als input basis voor de Cybersecurity-risicoanalyse OT. Het Cyberdreigingsbeeld OT is gebaseerd op het nationale dreigingsbeeld, dat door het NCSC jaarlijks wordt bijgestelden is opgezet specifiek voor deze specifieke situatie: operationele technologie van de infrastructuur voor het openbaar vervoer in Amsterdam. *NB. Het Cyberdreigingsbeeld is Vertrouwelijk. Het wachtwoord wordt op verzoek verstrekt door Cybersecurity-officer OT.*

Cybersecurity-eisen voor OT

De Cybersecurity-eisen OT is een tabel met de cybersecurity-maatregelen die voor OT-systemen van toepassing is. Het is de ‘default’-set met cybersecurity-maatregelen voor de OT. Alle OT-systemen dienen hier aan te voldoen (#Beleid).

> **Comply-or-explain.** Er mag worden afgeweken van Cybersecurity-eisen OT op basis van een cyberrisicoanalyse tijdens het ontwerp van (wijzigingen van) het Systeem uitgevoerd op basis van de aanpak Cyberrisicomanagement OT en schriftelijk goedgekeurd door de Cybersecurity-officer OT, of (eenvoudiger) op basis van een schriftelijk besluit door de Cybersecurity-officer OT (#Beleid). Goedkeuringen en Besluiten dienen gedocumenteerd te worden in het Cybersecurity-dossier van het Systeem (#Beleid) en in het Exceptie-register (door Cybersecurity-office GVB) (#Beleid).

Voor elke wijziging aan een Systeem, dient het Cybersecurity-dossier van het betrokken systeem te worden bijgewerkt door (of onder de verantwoordelijkheid van) de project- of areaal/assetmanager. Er dient te worden vastgesteld en opgenomen dat de wijziging de cybersecurity niet negatief beïnvloedt of juist (en hoe) verbetert.

Cyberrisicoanalyse voor OT

De cyberrisicomanagementaanpak beschrijft hoe de cyberrisicoanalyse wordt uitgevoerd op OT in geval van een 'explain’ voor een afwijking op de Cybersecurity-eisen OT. De 3 betrokken documenten zijn:

- ‘Uitleg’-document
- Cyberrisicomanagementsjabloon (tabel)
- Bedrijfswaardenmatrix (tabel)
- VUS/BOGT-matrix

Cyberrisicomanagementaanpak voor OT is gebaseerd op en is congruent aan de risicomanagementaanpak van de veiligheidsorganisatie van GVB. Vooraf aan de risicoanalyse, dienen de operationele KPI’s te worden vastgesteld, of dienen KPI’s als aannames vastgesteld te worden indien formele KPI’s ontbreken. KPI’s hebben betrekking op de **Veiligheid**, **Beschikbaarheid** en **Privacy**-doelstellingen van het betreffende/beoogde systeem en zijn (bijvoorbeeld) geformuleerd als jaarlijks te accepteren fysieke incidenten; feitelijk zijn dit de

cyberrestrisico's. Zie het document Cybersecurity en KPI's OT. De risicoanalyse dient specifieke hazards te benoemen die (met een zekere kans) kunnen optreden en een zekere impact kunnen bewerkstellingen, tegen de operationele doelen (kpi's) van het systeem betreffende **veiligheid**, **beschikbaarheid** en **privacy**. De cyberrisicoanalyse wordt gefaciliteerd door de projectcybersecurityofficer en inhoudelijk uitgevoerd door (technische) ontwerpers of beheerders, te samen met een onafhankelijke cybersecurity-expert (type ethical hacker). Een cyberrisicoanalyse dient te worden goedgekeurd door de Cybersecurity-officer.

Het cybersecuritydossier

Een cybersecuritydossier wordt opgesteld en bijgehouden voor elk Systeem (#Beleid). Het cybersecuritydossier wordt gestart ten tijde (van de opstart) van een project en is een onlosmakelijk verbonden met een PID. Cybersecuritydossier is een centrale pijler en 'leeft mee' met het systeem en wordt steeds bijgewerkt. Het Cybersecuritydossier**sjabloon** OT geeft het stramien om voor elk systeem de relevante cybersecurityaspecten vast te leggen. De uitgangspunten voor en de resultaten van de cyberrisicoanalyse worden vastgelegd (of verwezen naar) in het cybersecuritydossier.

Cyberincidentprocedure

Cybersecurityincidenten kunnen worden gevonden, geïnitieerd en afgehandeld door GVB-medewerkers, maar dikwijls in de samenwerking met beheerleveranciers. De cyberincidentmanagementprocedure is verplicht voor alle betrokken organisaties en medewerkers (#Beleid).

Vertrouwelijkheid

Het document Vertrouwelijkheid beschrijft op welke **informatie over systemen en cybersecurity** vertrouwelijk is en hoe die vertrouwelijke informatie dient te worden opgeslagen en gedeeld, ondermeer met ketenpartners en beheerleveranciers. Het document Vertrouwelijkheid is verplicht van toepassing voor elk Systeem in de hele life cycle (#Beleid).

Vraagspecificatie Cybersecurity OT

Het document Cybersecurity-vraagspecificaties beschrijft de generieke VS1- en VSP-eisen voor cybersecurity en kunnen worden geïntegreerd in de totale vraagspecificaties ten behoeve van een aanbesteding/inkoop.

8 Systeemspecifieke aandachtspunten en documenten

Project- en/of systeemspecifieke (blauwe) documenten worden afgeleid van de (rode) cybersecurity-richtlijnen. Hieronder volgt de uitleg van enkele (niet limitatief!) documenten en aandachtspunten tijdens de totstandkoming (en beheeractiviteiten) van het systeem. Het voert te ver om voor alle situaties en documenten aan te geven hoe cybersecurity dient te worden opgenomen, daarom geldt dat voor andere dan hier beschreven documenten en aandachtspunten de uitleg hieronder geïnterpreteerd dient te worden naar de geest en bedoeling van die richtlijnen. Neem bij twijfel contact op met de Cybersecurity-officer OT.

Integraal management systeem

De Rasci's hieronder zijn richtlijnen om de Rasci's voor de betrokken bedrijfsprocessen van een bedrijfsonderdeel aan te passen en om daarmee de cybersecurityactiviteiten te integreren in de bestaande procesbeschrijvingen en procedures van een bedrijfsonderdeel en om de toepassing ervan te vergemakkelijken. Tot die tijd dient dit Voorschrift op pragmatische wijze en naar de geest ervan, geïntegreerd te worden in lopende trajecten in een afstemming tussen de betrokken project- of areaal/assetmanager en de Cybersecurity-officer OT.

ProjectIdentificatieDocument (PID)

Cybersecurity begint ten tijde van de definitie van een Project. In een Project Identificatie Document (PID) wordt vastgesteld of en hoe op hoofdlijnen cybersecurity relevant is voor het systeem en hoe daar in het vervolg van het project vorm en inhoud aan wordt gegeven. De Cybersecurity-office dient hierbij te worden geraadpleegd. Relevante onderwerpen voor het PID zijn operationele doelen/KPI's en het (beoogde) operationeel gebruik en beheer van het systeem.

Voor de RASCI van een PID geldt:
Cybersecurity-officer OT = Consulted

Cybersecurity-officer OT controleert altijd het PID voor het borgen van een juiste dekking van het onderwerp.

Projectplan

Indien is vastgesteld dat cybersecurity relevant is voor een systeem, wordt in het projectplan de volgende onderwerpen opgenomen.

- Financiering. Als vuistregel kun je voor de begroting voor cybersecurity een bedrag opnemen van ca 10% van de totale begrote ICT/OT-kosten van een systeem.
- Projectcybersecurity-officer. Voeg de rol 'Projectcybersecurity-officer' toe aan de projectorganisatie. Dit kan praktisch worden ingevuld door bijvoorbeeld een technisch architect met affiniteit voor het onderwerp die begeleid wordt door de Cybersecurity-officer OT van het bedrijfsonderdeel. De Projectcybersecurity-officer is de contactpersoon voor de projectmanager, de opdrachtnemer en de Cybersecurity-officer OT.
- Vraag de Cybersecurity-officer OT een initiële cyberrisico-analyse uit te voeren op het beoogde systeem en neem de resultaten op in het Cybersecurity-dossier dat meegegeven wordt in de aanbesteding.
- Integreer de Cybersecurity-vraagspecificatie (VS1 en VSP) in de totale vraagspecificatie.

- Integreer gestelde eisen in de Cybersecurity-vraagspecificatie (VS1 en VSP) in het projectplan. Denk aan de V&V-activiteiten en de eventuele pen-testen (validatie).
- Vertouwelijkheid. Informatie over risico's, kwetsbaarheden, maatregelen en ontwerpen zijn vertrouwelijk van aard. In het project dienen maatregelen te worden genomen om die vertouwelijkheid te borgen. Vraag de Cybersecurity-officer OT naar mogelijkheden.
- Neem bij twijfel contact op met de Cybersecurity-officer OT.

Voor de RASCI van de totstandkoming van een Projectplan geldt:

De betrokken opdrachtgever of projectmanager = Accountable

voor al het bovenstaande

Projectcybersecurity-officer = Responsible

Projectcybersecurity-officer zorgt dat de VS1- en VSP-eisen voor cybersecurity in de finale vraagspecificatie van het project zijn geintegreerd.

Cybersecurity-officer OT = Consulted

Cybersecurity-officer OT controleert altijd een Projectplan voor het borgen van voldoende dekking van het onderwerp in het project aan de hand van de bovenstaande richtlijnen.

Operationele KPI's en Procesbeschrijving

De operationele KPI's en het operationele proces van het beoogde systeem zijn van belang (input) voor de cyberrisico-analyse en worden vastgelegd in het Cybersecurity-dossier van het te ontwikkelen systeem aan de hand van Cybersecurity-dossiersjabloon.

Voor de RASCI van de totstandkoming van een operationele KPI's en het operationele proces geldt:

De betrokken opdrachtgever of projectmanager = Accountable

Vraagspecificaties

In het geval van de aanbesteding/inkoop wordt vraagspecificaties (VS1 en VSP) uitgebreid met de vraagspecificaties voor de cybersecurity van OT. Zie het document 'Vraagspecificaties Cybersecurity OT'.

Voor de RASCI van een Vraagspecificaties geldt:

De betrokken opdrachtgever of projectmanager = Accountable

voor hetgeen gesteld in de cybersecurity-vraagspecificaties

Projectcybersecurity-officer = Responsible

Projectcybersecurity-officer zorgt dat de VS1- en VSP-eisen voor cybersecurity in de finale vraagspecificatie van het project zijn geintegreerd.

Cybersecurity-officer OT = Consulted

Cybersecurity-officer OT controleert altijd de vraagspecificaties voordat deze aan de markt worden aangeboden, voor het borgen van een juiste dekking van het onderwerp.

Ontwerp, realisatie en implementatie en overdracht

Cybersecurity is een systeemaspect in de RAMSHEEP-reeks en is daarmee een aandachtspunt in het ontwerp van een systeem, dat tijdens de realisatie tot inrichting komt en bij implementatie en

overdracht wordt toegepast, zowel door gebruikers (waar van toepassing) en door beheerders/onderhouders (AO&I). De projectcybersecurity-officer ziet toe op de juiste uitvoering.

Voor de RASCI zie de RASCI van het Projectplan.

Verificatie & Validatie

In elke V&V-activiteit van het project dient expliciet aandacht te zijn voor Cybersecurity. In het V&Vplan van het project dient een pen-test ter zijn opgenomen, die wordt uitgevoerd onder auspiciën van de Cybersecurity-Officer OT.

Voor de RASCI zie de RASCI van het Projectplan (hierboven).

OTO (Opleiden, Trainen, Oefenen)

Gebruikers en beheerders dienen ook getraind (op de bewustzijn) te worden op cybersecurity-aspecten, zoals phishing en het trainen van processen en procedures voor cyberincidenten en cybercalamiteiten.

Voor de RASCI zie de RASCI van het Projectplan (hierboven).

Gebruik en Beheer en Overdracht

Procedures voor de cybersecurity (zoals backup-, incident- en herstelprocedures) worden opgenomen toegevoegd aan de andere procedures voor het gebruik en beheer. Afspraken (contracten) met de leveranciers worden opgenomen in het onderhouds- en beheerplan van het betrokken Systeem. Cybersecurity-dossier wordt actueel en compleet overgedragen aan de areaal/assetmanager. Project- of areaal/assetmanager laat bij overdracht deze documenten reviewen door de Cybersecurity-officer OT op compleetheid.

Voor de RASCI zie de RASCI van het Projectplan.

De betrokken opdrachtgever of projectmanager = Accountable
voor een actueel en compleet cybersecurity-dossier.

Projectcybersecurity-officer = Responsible
De projectcybersecurity-officer zorgt voor een actueel en compleet cybersecurity-dossier.

Cybersecurity-officer OT = Consulted
De Cybersecurity-officer OT controleert de dekking van het cybersecurity-dossier.

Cybersecurity-dossier

Alle uitgangspunten, beslissingen, afwijkingen, resultaten en referenties (of verwijzingen daarnaar) die de cybersecurity betreffen, worden vastgelegd in het Cybersecurity-dossier van het betrokken Systeem. Dat dient gedurende de ontwikkel- en beheer-life cycle bijgehouden te blijven. Het Cybersecurity-dossier wordt in het AO&I-proces formeel overgedragen van de project- naar de areaal/assetmanager. Cybersecurity-dossier beschrijft de beheersaspecten van de cybersecurity van het systeem: zoals de cybersecurity-risico-analyse, het cybersecurity-ontwerp(aspecten), relevante wachtwoorden, vertrouwelijkheid en patchmanagement. Voor het opstellen van een

Cybersecurity-dossier voor een systeem kan gebruik worden gemaakt van het Cybersecurity-dossier-sjabloon.

Voor de RASCI zie de RASCI van het Projectplan (hierboven).

9 PDCA en Borging

De PDCA en borging van de cybersecurity-maatregelen van de OT systemen van GVB, gebeurt op basis van een integraal information security management systeem (i-ISMS) en vindt op drie niveaus plaats:
1. op Holding-niveau (IT en OT)
2. op Bedrijfsonderdeel-niveau (IT en OT)
3. op Systeem-niveau (OT)

Voor ad 1. en ad 2. (de borging op organisatie-niveau 1 en 2) wordt verwezen naar Integrale information security management systeem. Ad 3. Hieronder in dit document wordt beknopt de manier aangegeven hoe op Systeemniveau (OT) de PDCA en borging is voorzien.

PDCA en borging op Systeemniveau (OT)

Het cybersecuritydossier van het Systeem is het centrale document en start ten tijde van het PID. Initieel is de (ambtelijk) opdrachtgever de lijnverantwoordelijke voor het inbrengen van het (laten) vastleggen van de cybersecurity-systeemaspecten van het betrokken systeem en het (laten) invullen en vastleggen van de bovenstaande documenten. Zie ook Hoofdstuk 3 Verantwoordelijkheden.

Bij de overdracht van project naar beheer dient (via de AO&I-procedure) het cybersecuritydossier volledig ingevuld te worden overgedragen aan de areaal/assetmanager. De projectcybersecurity-officer zorgt voor de uitvoering daarvan.

De areaal/assetmanager is de lijnverantwoordelijke voor het beheren van de cybersecurity-aspecten en tijdens de beheer-fase en voor het actueel houden van het cybersecuritydossier van het Systeem. De areaal/assetmanager laat het cybersecuritydossier bijwerken bij elke wijziging en/of vaststellen op het wijzigingsformulier dat de cybersecurity niet wordt beïnvloedt door de wijziging.

De Cybersecurity-officer OT van het bedrijfsonderdeel adviseert, begeleidt, controleert periodiek over de actualiteiten van het cybersecuritydossier en rapporteert daarover aan de lijn-organisatie. De rapportages zijn op verzoek te reviewen door de Cybersecurity-office GVB. De Cybersecurity-office GVB heeft the-right-to-audit op uitvoering van het i-ISMS binnen een bedrijfsonderdeel.

10 Compliancy

Ten tijde van het schrijven van dit moment (medio 2022) wordt een vergelijk opgesteld van de betrokken normenkaders voor de cybersecurity van OT gebaseerd op de IS27001/2, de IEC62443 en de Cenelec TS50701. De verwachting is dat dat eind 2022 gereed is. Die samengestelde set aan normenkaders wordt de basis voor de VVT, Verklaring Van Toepasselijkheid van het ISMS OT van GVB.

Tot die tijd wordt - voor de compliancy tegen de BIO- een pragmatische redenatie gevolgd voor de onderbouwing van de cybersecurityvoorschriften, eisen en richtlijnen voor OT. En die redenatie is als volgt.

De BIO is gebaseerd op ISO27001 en ISO27002.
De ISO27001/2 zijn niet alle direct toepasbaar voor OT.
De BIO heeft geen BasisBeveiligingsNiveau (BBN) voor OT systemen.
De CSIR 2015 van RWS is een voor OT relevante subset van de BIO.
De IEC62443 is een alom erkende en voor OT relevante maatregelen/eisenset.
De IEC62443 is een -voor OT- een relevante toevoeging op de ISO27001/2.
De CSIR 2015 van RWS is mede gebaseerd op de IEC62443.
De CSIR 2015 is door de Algemene Rekenkamer beschouwd [1] als geschikt voor OT.
De Cybersecurity-eisen van de OT van GVB zijn gebaseerd op de CSIR 2015 van RWS.
De Cybersecurity-eisen van de OT van GVB is gelijk aan weerstandsniveau 4 van de CSIR.

De Cybersecurity-eisen van de OT van GVB is de default set; afwijken mag o.b.v. comply/explain.
De IEC62443 stelt risicomanagement centraal, voor het ontwerpen van maatregelen.
De BIO stelt risicomanagement centraal, voor het ontwerpen van maatregelen.
De Cybersecurity-voorschrift OT van GVB eist de risicomanagementaanpak voor de ‘explain’.

De uitgangspunten en resultaten van de risicoanalyses worden vastgelegd in de cybersecuritydossier voor elke Systeem. De wijze waarop de borging voor een Systeem is georganiseerd is vastgelegd in de cybersecuritydossier. Door het volgen van de aanpak in dit Voorschrift wordt de informatiebeveiliging voor operationele systemen ingevuld en wordt voldaan aan de BIO.

11 Bronnen en Referenties

[1] Rapport 'Digitale dijkverzwaring' van de Algemene Rekenkamer, 2019.
[2] CSIR 2015, Cybersecurity-implementatieRichtlijnen, Rijkswaterstaat.

De vigerende versies van de set aan cybersecurity-documenten zijn gegeven op de intranet-pagina en dienen als bindende bijlagen bij dit Cybersecurity-voorschrift OT en bij een aanbesteding:
https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx