

Cybersecurity Voorschrift OT MET

voor Operationele Technologie

Metro en Tram

Gemeente Amsterdam

Vertrouwelijkheid.

Dit document is niet vertrouwelijk

Document

Join: CEB/OVG/21876

Versie: 1.5

Datum: 14 juni 2021

Inhoudsopgave

1. Inleiding	4
2. Toepasselijkheid	4
3. Verantwoordelijkheden	4
4. Van generiek naar specifiek	6
4.4.1. Documenten/Referentielijst	7
5. Generieke documenten (rood).....	9
5.1. CS Dreigingsbeeld OT MET	9
5.2. CS-Beleid OT MET	9
5.3. CS-Eisen OT MET	9
5.3.1. Beveiligingsniveaus	10
5.4. CS-Risicomanagement OT MET	10
5.5. CS-Dossier OT MET	11
5.6. CS-Incidentmanagement	11
5.7. Vertrouwelijkheid OT MET	11
6. Specifieke documenten (blauw)	12
6.1. Projectidentificatie Document.....	12
6.2. Operationele KPI's en Procesbeschrijvingen	12
6.3. Vraagspecificaties.....	12
6.4. Ontwerpen	12
6.5. OTO (Opleiden, Trainen, Oefenen)	12
6.6. Gebruik- & Beheer	12
6.7. CS-Dossier	13
7. PDCA en borging.....	14
7.1. PDCA op systeem/objectniveau	14
7.2. PDCA op organisatieniveau Metro en Tram	14
8. Compliancy.....	15
9. Bronnen & referenties.....	15

Accordering

Dit document is een paraplu-document van een set aan documenten die te samen de aanpak beschrijven voor de bescherming tegen cyber-incidenten van of -aanvallen op de Operationele Technologie van MET. De set aan documenten is gegeven in paragraaf 4.4.1.

Elk afzonderlijk document van deze set is gereviewd door de direct betrokkenen en specialisten, waaronder de CISO van GVB, Daniel Wunderink. Met de leden van de Cybersecurity Board MET/GVB zijn de afzonderlijke documenten besproken en zijn de opmerkingen verwerkt. Bij de versies van elk van die documenten is aangegeven wie gereviewd hebben. De opmerkingen van de reviewers zijn alle verwerkt in de afzonderlijke documenten.

Goedkeuring:

Versie 1.3 is op 6-6-2020 getekend door
Jacco de Regt
Manager Strategisch Assetmanagement, E&B, MET

Versiebeheer van dit document

- 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
- 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

1. Inleiding

Dit is het **top-document** dat als inleiding fungeert naar het cybersecurity-beleid en de manier waarop de cybersecurity dient te worden ingericht voor een specifiek bedienings- en bewakingsstelsel van Metro en Tram.

2. Toepasselijkheid

Dit document is van toepassing voor alle operationele systemen voor bediening en bewaking van Metro en Tram die **software** bevatten.

Met software wordt bedoeld geprogrammeerde logica in de breedste zin van het woord, zoals - niet limitatief - applicatiesoftware, operating system, system utilities, netwerk- en communicatiesoftware, firmware en embedded software.

Daar hardware zoals processoren ook gecompromitteerd kunnen zijn, kan ook hardware een onderwerp van beschouwing zijn.

Systemen zijn hier **assets** of **objecten** over de **hele levenscyclus**: vanaf een PID tot en met het operationele gebruik en beheer en/of renovatie.

3. Verantwoordelijkheden

Cyber security is een lijnverantwoordelijkheid. Dat betekent dat afhankelijk van de life cycle waar het systeem/asset zich in bevindt de opdrachtgever, de project-, asset- of contractmanager verantwoordelijk is voor de cybersecurity en samen met de (toekomstige) gebruikers en/of beheerders (c.q. eigenaren, opdrachtgevers) bepalen welke maatregelen nodig zijn. Met contractmanager wordt hier bedoeld degene die verantwoordelijk is voor het onderhoud en beheer van het systeem, al of niet een externe leverancier.

In de aanbestedings-, project- en onderhoudsfase van een systeem dient de rol 'systeem cybersecurity officer' (SCO) te worden ingevuld door een medewerker die daarvoor wordt aangesteld door de respectievelijke opdrachtgever, de project-, asset- of contractmanager. Afhankelijk van de omvang van het project is dat een full time of parttime rol. De project cybersecurity officer draagt zorg voor de uitvoering van de cybersecurity namens de opdrachtgever, de project-, asset- of contractmanager en op basis van dit voorschrift, het cybersecuritydossier en de contractuele afspraken. De SCO rapporteert in de lijn aan de respectievelijke opdrachtgever, de project-, asset- of contractmanager en functioneel aan de CS Officer OT MET. De SCO is het inhoudelijke aanspreekpunt voor de CS Officer OT en v.v.

CS Officer OT MET adviseert bij of helpt met het opstellen van een voor het systeem specifieke aanpak, maatregelen en documenten, zoals hieronder genoemd.

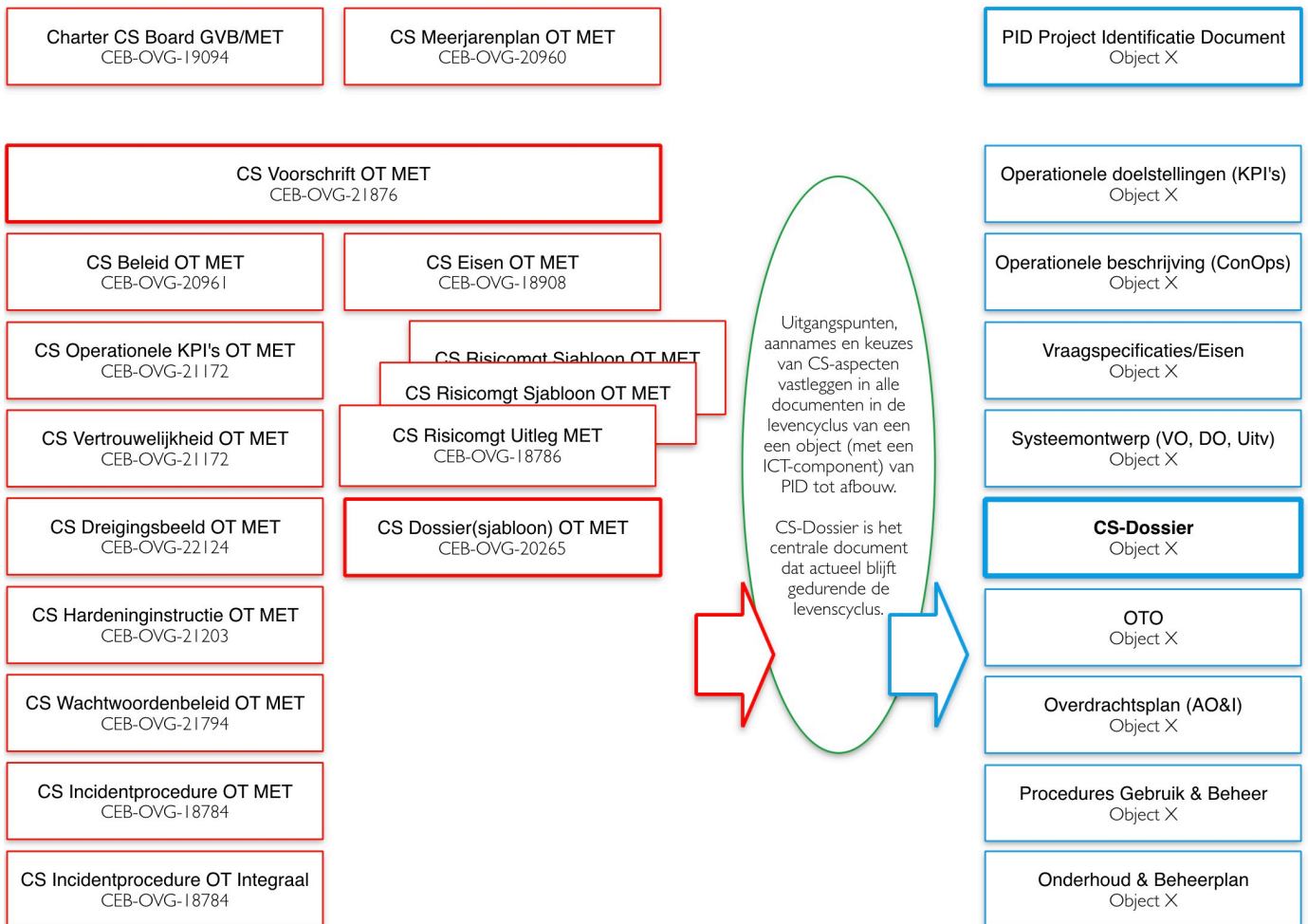
De opdrachtgever, de project-, asset- of contractmanager dient de CS(-documenten) te laten reviewen **in elke projectfase en/of bij elke asset change** door de CS Officer OT MET op diepgang en toepasselijkheid tegen het actuele Dreigingsbeeld OT MET.

CS Officer OT MET adviseert de opdrachtgever, de project-, asset- of contractmanager. De CS Officer kan en zal escaleren in geval de opdrachtgever, de project-, asset- of contractmanager, volgens het oordeel van de CS Officer, te grote (rest)risico's laat, maar de beheerder of opdrachtgever en gebruikersorganisatie bepalen uiteindelijk of restrisico's acceptabel zijn.

4. Van generiek naar specifiek

Dit hoofdstuk geeft een korte beschrijving van alle **(rode) generieke** documenten die van toepassing zijn. Deze documenten vormen de leidraad voor het vaststellen van een specifieke cyber aanpak voor een specifiek systeem/asset.

De **(blauwe) systeemspecifieke** documenten hieronder zijn **voorbeelden** (niet limitatief!) van documenten die een asset begeleiden door de hele levenscyclus. Het project of asset manager (afhankelijk van de life cycle) draagt zorg voor het opstellen van die documenten.



4.1.1. Documenten/Referentielijst

Titel	Join code	versie	datum	Vertrouwkhkd	doelgroep	mee met uitvraag
Cybersecurity Voorschrift OT	CEB-OVG-21876	1.5	14 juni 2021	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurity-eisenset MET OT systemen	CEB-OVG-18908	1.2	21 dec 2020	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurity en Operationele KPI's	CEB-OVG-21172	1.0	21 aug 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurity en Vertrouwelijkheid OT	CEB-OVG-20264	2.0	2 dec 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cyber dreigingsbeeld OT	CEB-OVG-22124	-	5 jan 2021	Zeer-Vertrouwelijk **)	OG (MET/GVB) en ON	nee
Cybersecurity-dossier Sjabloon	CEB-OVG-20265	-	16 mrt 2020	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurity-dossier Systeem	project/systeem specifiek	-	-	Zeer-Vertrouwelijk **)	OG (MET/GVB) en ON	nee
Cybersecurityrisicomanagement, 1-3 OT Uitleg	CEB-OVG-18786	1.1	18 sep 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurityrisicomanagement, 2-3 OT Bedrijfswaarden	CEB-OVG-18786	-	18 sep 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurityrisicomanagement, 3-3 OT Sjabloon	CEB-OVG-18786	-	24 jul 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurityhardeninginstructie OT	CEB-OVG-21203	0.1	20 aug 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurity-handreiking wachtwoordbeleid (IBD)	CEB-OVG-21794	2.11	sep 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurityincident managementprocedures Integraal	CEB-OVG-20126	1.4	26 mrt 2019	Bedrijfs vertrouwelijk *)	OG (MET/GVB) en ON	ja
Cybersecurityincident managementprocedures Integraal, Bijlage A Contactpersonen ON	project/systeem specifiek aanvullen	-	-	Zeer-Vertrouwelijk **)	OG (MET/GVB) en ON	nee
Cybersecurityincident managementprocedures Integraal, Bijlage A	CEB-OVG-20126	1.4	26 mrt 2019	Zeer-Vertrouwelijk **)	OG (MET/GVB)	nee

Titel	Join code	versie	datum	Vertrouwkhkd	doelgroep	mee met uitvraag
Cybersecurity-incidentmanagementprocedure OT MET	MET CEB-OVG-18784	1.3	26 mrt 2019	Bedrijfsvertrouwelijk *)	OG (MET/GVB)	nee
Cybersecurity-beleid	CEB-OVG-20961	1.3	4nov19	Bedrijfsvertrouwelijk *)	OG (MET/GVB)	nee
Cybersecurity-organisatie OT	CEB-OVG-21793	1.0	4nov19	Bedrijfsvertrouwelijk *)	OG (MET/GVB)	nee
Charter cybersecurity board MET/GVB	CEB-OVG-19094	1.0	16jul18	Bedrijfsvertrouwelijk *)	OG (MET/GVB)	nee
Cybersecurity Meerjarenplan	CEB-OVG-19819	1.0	11 sep 2019	Zeer-Vertrouwelijk **)	OG (MET/GVB)	nee
Cybersecurity Meerjarenbegroting	CEB-OVG-19819	-	11 nov 20	Zeer-Vertrouwelijk **)	OG (MET/GVB)	nee
Cybersecurity Jaarplan	CEB-OVG-19819	V1.5	22 mrt 21	Zeer-Vertrouwelijk **)	OG (MET/GVB)	nee

*) Bedrijfsvertrouwelijk, alleen gedeeld en gebruikt worden in professionele communicatie tussen OG en ON en betrokken organisaties, mag worden gedeeld via email.

***) Zeer-vertrouwelijk, versleuteld document. Sleutel wordt gedeeld door CybersecurityOfficer. Mag alleen selectief worden gedeeld met direct betrokkenen na ondertekening van de Vertrouwelijkheidsverklaring. Dit document wordt alleen (pas) gedeeld met ON zodra de opdracht is geformaliseerd.

5. Generieke documenten (rood)

Hieronder volgt de uitleg van enkele generieke (rode) documenten.

5.1. CS Dreigingsbeeld OT MET

Dit document beschrijft de dreiging die we mogen verwachten uit de wereld en veronderstellen relevant te zijn voor bediening- en bewakingssystemen van metro en tram. Het dreigingsbeeld is bedoeld als input basis voor de CS-risicoanalyse. Join-referentie: CEB-OVG-22124.

Het dreigingsbeeld OT MET is gebaseerd op het nationale dreigingsbeeld, dat door het NCSC jaarlijks wordt bijgesteld. Het cyber dreigingsbeeld is opgezet specifiek voor deze specifieke situatie: operationele technologie van de infrastructuur voor de spoorse openbaar vervoer in Amsterdam.

Dit document is Zeer-Vertrouwelijk. Het wachtwoord wordt op verzoek verstrekt door Cybersecurity Officer OT MET.

5.2. CS-Beleid OT MET

Dit document beschrijft de scope, de doelstellingen, de definitie en het beleid van de OT-systemen van Metro en Tram. Join-referentie: CEB-OVG-20961.

MET's beleid is ondermeer dat voor elk systeem een separate CS risicoanalyse dient te worden uitgevoerd op basis van het CS Dreigingsbeeld OT MET. MET hanteert dus bewust geen vaste beveiligingsniveaus (confectie), omdat de systemen onderling te veel verschillen en dus maatwerk nodig is.

5.3. CS-Eisen OT MET

De Cybersecurity-eisen OT MET is een tabel met de cybersecurity-maatregelen die voor de OT-systemen van toepassing is. Het is de 'default'-set met cybersecurity-maatregelen voor de OT van MET. Join-referentie: CEB-OVG-18908.

Deze Cybersecurity-eisenset is gebaseerd op de maatregelen van RWS (CSIR 2015), maar ontdaan van de doublures en de meervoudige maatregelen zijn opgesplitst tot enkelvoudige maatregelen. Er zijn definities toegevoegd en er is uitleg gegeven.

Het bevat alle maatregelen (niveau 4 van de CSIR) en geldt als een default-set, die specifiek wordt gemaakt (aan de hand van het CS risicomangementaanpak MET OT) tijdens het ontwerp van het Object.

De Cybersecurity-eisen OT MET is van toepassing op alle OT systemen van MET. Voor elk beheerd systeem (asset) en voor elk project (nieuw systeem herbouw) waarin met software en/of firmware is/wordt opgenomen, geldt deze Cybersecurity-eisenset OT MET.

Voor elke Change, dient het Cybersecuritydossier OT MET van het betrokken systeem te worden bijgewerkt door de uitvoerder van de change en dient te worden vastgesteld en opgenomen op het change-formulier dat de 'change' de cybersecurity niet negatief beïnvloedt of juist verbetert.

Voor elke maatregel van deze default-set wordt - voor elk systeem (asset) – aangegeven of of in hoeverre de maatregel wordt/is geïmplementeerd (comply-of-explain). De onderbouwing van de 'explain' dient te worden gegeven op basis van de CS-risicomanagementaanpak OT van MET.

De CS-eisenset wordt in samenhang gebruikt met documenten:

- CS-risicomanagementaanpak voor OT van MET en met het
- CS-dossier(sjabloon) voor OT van MET
- Cybersecurity en KPI's voor OT van MET
- CS-Dreigingsbeeld voor OT van MET

5.3.1. Beveiligingsniveaus

De CSIR 2015 hanteert een 4-tal beveiligingsniveaus specifiek voor de RWS objecten. Alle infra-objecten van RWS zijn geclassificeerd op de 4 beveiligingsniveaus. Het 4e niveau is bedoeld voor objecten met een nationale impact. Het 3e niveau is bedoeld voor objecten met een regionale impact.

De CS-eisen MET OT bevatten alle maatregelen uit de CSIR en komt dus overeen met beveiligingsniveau 4 van de CSIR. Echter, de CS-eisen MET OT geldt als default-set dat specifiek wordt gemaakt tijdens de ontwerpfasen en op basis van een **specifieke risicoanalyse** van het object. MET hanteert dus **geen vaste beveiligingsniveaus**.

MET's beleid is dat voor elk systeem een **separate risicoanalyse** dient te worden uitgevoerd op basis van het CS Dreigingsbeeld OT MET en risicoanalyse benoemt de specifieke hazards 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 operationele kpi's zijn gelijk aan de cyberrestrisico's die als acceptabel worden gesteld door beheerder en gebruiker.

5.4. CS-Risicomanagement OT MET

Cybersecurity-risicomanagementaanpak voor OT van MET beschrijft hoe de risicoanalyse wordt uitgevoerd op OT van MET. Join-referentie: CEB-OVG-18786.

De documenten bevatten een:

- 'Uitleg' document,
- Risicomanagementsjabloon (tabel)
- Bedrijfswaardenmatrix (tabel)
- VUS/BOGT-matrix

Cybersecurity-risicomanagementaanpak voor OT van MET is gebaseerd op en is congruent aan de veiligheidsaanpak van Metro en Tram. Cybersecurity faciliteert immers de fysieke veiligheid van het systeem.

De cybersecurityrisicoanalyse is verplicht voor elke asset met software/firmware.

Vooraf aan de risicoanalyse, dienen de KPI's te worden vastgesteld; of dienen KPI's als aannames vastgesteld te worden, indien formele KPI's ontbreken. Zie het document Cybersecurity KPI's OT MET, Join: CEB-OVG-21172.

KPI's hebben betrekking op de Veiligheid, Beschikbaarheid en Privacy-doelstellingen van het betreffende/beoogde systeem en zijn geformuleerd als jaarlijks te accepteren fysieke incidenten; feitelijk zijn dit de cybersecurity-restrisico's.

De risicoanalyse wordt gefaciliteerd door de cybersecurity-medewerker/officer van het project of van MET en inhoudelijk uitgevoerd door (technische) ontwerpers, te samen met een onafhankelijke cybersecurity-expert. De rol van de cybersecurity-expert wordt ingevuld door een externe pen-tester en/of de cybersecurity-officer.

Bij het ontwerpen van de cybersecuritymaatregelen kan gebruik worden gemaakt van de cybersecurity handleidingen, zoals de wachtwoordenbeleid en hardeningsinstructies van MET. Deze handleidingen zijn grotendeels gebaseerd op de handleidingen van het IBD, de InformatieBeveiligingsDienst van de Vereniging van Nederlandse Gemeenten (VNG). Zie ook IBD.nl.

5.5. CS-Dossier OT MET

Een cybersecuritydossier wordt opgesteld voor elk systeem. 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 sjabloon voor het Cybersecuritydossier OT MET geeft het stramien om voor elk systeem de relevante cybersecurityaspecten vast te leggen. Join-referentie: CEB-OVG-20265.

De uitgangspunten voor en de resultaten van de cs-risicoanalyse worden vastgelegd in het CS-Dossier. Het cybersecuritydossier is een verplicht document voor elke asset met software/firmware.

5.6. CS-Incidentmanagement

Voor cyberincidenten onderscheidt MET twee niveau's:

1. Cybersecurityincidenten die door MET-medewerkers worden gevonden, geïnitieerd en afgehandeld en
2. Cybersecurityincidenten die in alleen in samenwerking met ketenpartners en leveranciers afgehandeld kunnen worden.

5.7. Vertrouwelijkheid OT MET

Het document Vertrouwelijkheid beschrijft op welke informatie over de cybersecurity vertrouwelijk is en hoe die vertrouwelijke informatie dient te worden opgeslagen en gedeeld. Join-referentie: CEB-OVG-20264. Het document over Vertrouwelijk is een verplicht document voor elke asset met software/firmware.

6. Specifieke documenten (blauw)

Hieronder volgt de uitleg van enkele (niet limitatief!) generieke (blauwe) documenten die de (totstandkoming of beheeractiviteiten) van de asset beschrijven.

6.1. Projectidentificatie Document

Cybersecurity begint bij de Project Identificatie Document (PID), waarin wordt vastgesteld of en hoe op hoofdlijnen cybersecurity relevant is en hoe daar in het vervolg van het project vorm en inhoud aan wordt gegeven. Relevante onderwerpen voor het PID zijn: operationele doelen/KPI's en operationeel gebruik en beheer.

6.2. Operationele KPI's en Procesbeschrijvingen

De documenten CS Operationele KPI's vastgelegd in het CS Dossier van het te ontwikkelen systeem aan de hand van CS Dossier(sjabloon) OT MET. Project stelt specifieke contracteisen op als onderdeel van de vraagspecificatie voor (kandidaat)leveranciers.

6.3. Vraagspecificaties

Het project- of assetmanager In Vraagspecificaties/Eisen Object X worden de CS-eisen opgesteld aan de hand van CS Eisen OT MET.

6.4. Ontwerpen

Tijdens de (verschillende) ontwerpfasen (van VO, DO en uitvoering) worden de cybersecuritymaatregelen ontworpen, gebruik makend van het document CS-Risicomangementaanpak OT MET (CEB-OVG-18786).

6.5. OTO (Opleiden, Trainen, Oefenen)

In OTO (Opleiden, Trainen, Oefenen) kunnen o.b.v. de risicoanalyse, de cybersecurity aspecten en processen en procedures worden getraind; inclusief de bewustzijnsaspecten.

6.6. Gebruik- & Beheer

Procedures voor de cybersecurity (zoals backup- en herstelprocedures en CERT-processen) worden opgenomen in de Procedures Gebruik- & Beheer. Afspraken (contracten) met de leveranciers worden opgenomen in het onderhouds- en beheerplan van het betrokken object/asset.

Project- of assetmanager laat bij overdracht deze documenten reviewen door CS Officer OT MET op compleetheid en adviseert de project- of assetmanager.

6.7. CS-Dossier

Alle uitgangspunten, beslissingen, afwijkingen, resultaten en referenties worden vastgelegd in het **CS-Dossier** van het betrokken object/asset. Dat dient gedurende de life cycle bijgehouden te blijven.

7. PDCA en borging

De borging van de cybersecurity-maatregelen van de OT systemen van MET, vindt op twee niveaus plaats:

1. op systeem (project/asset) niveau en
2. op organisatieniveau.

7.1. PDCA op systeem/objectniveau

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.

Het cybersecuritydossier(sjabloon) is het centrale document en start ten tijde van het PID.

Bij de overdracht van project naar beheer dient door middel van de AO&I-procedure het cybersecuritydossier volledig ingevuld te worden overgedragen aan de Beheerder (c.q. de assetmanager). De cybersecurity officer van het project zorgt voor de uitvoering daarvan.

Op systeemniveau is de asset-manager de lijnverantwoordelijke voor het beheren van de cybersecurity. De contractmanager (van de leverancier) is verantwoordelijk voor de uitvoering van cybersecurity op basis van de eisen gesteld in het contract en het cybersecuritydossier van het systeem.

De assetmanager laat het cybersecuritydossier bijwerken bij elke change; of vaststellen op het change-formulier dat de cybersecurity niet wordt beïnvloedt door de wijziging.

Cybersecurity is een onderdeel van het assetmanagement van MET en is opgenomen in het Strategisch Assetmanagement Plan van MET/E&B (Join: CEB-OVG-19260).

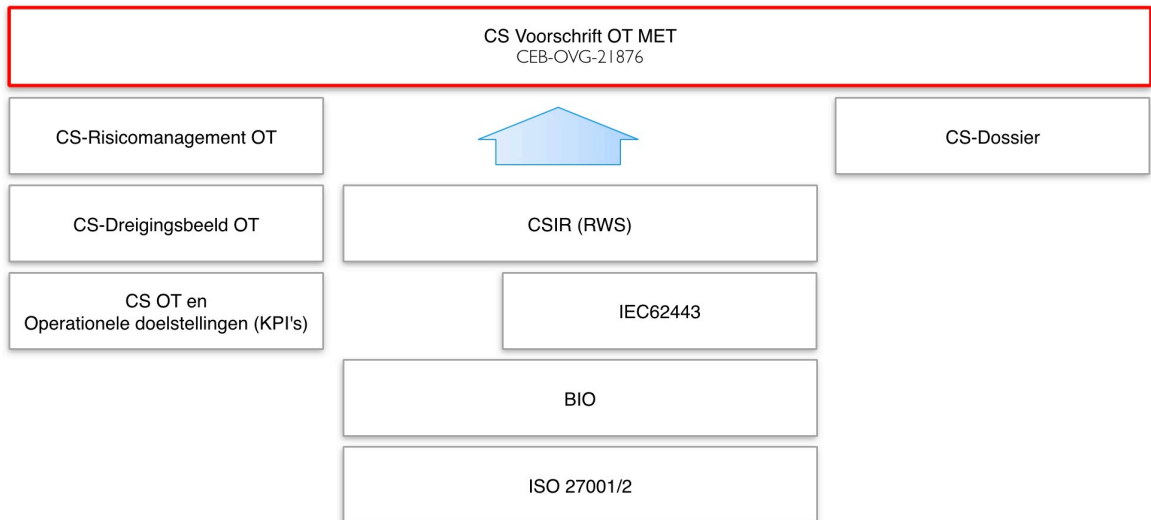
7.2. PDCA op organisatieniveau Metro en Tram

Op het organisatieniveau en het Information Security Management System (ISMS) van Metro en Tram ziet de cybersecurity-officer toe, door middel van audits, pen-testen en/of assessment, op naleving van de bovenstaande processen in projecten en bij assetmanagers en leveranciers en in de Metro en Tram organisatie zelf.

Het ISMS voor de OT wordt door de afdeling Kwaliteit & Organisatie van Metro en Tram periodiek geaudit. De eerste audit in 2019 resulteerde reeds in concrete aanbevelingen.

8. Compliancy

Hieronder volgt de onderbouwing voor de compliancy van de CS-Voorschrift/CS-Eisen MET OT tegen de BIO.



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 eisenset.

De IEC62443 bevat een relevante subset van de ISO27001/2 maatregelen.

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 CS-eisen van de OT van MET zijn gebaseerd op de CSIR 2015 van RWS.

De BIG-Eisen aan leveranciers van het IBD zijn -waar relevant- opgenomen.

De IEC62443 stelt risicomanagement centraal, voor het ontwerpen van maatregelen.

De BIO stelt risicomanagement centraal, voor het ontwerpen van maatregelen.

De CS-Voorschrift van MET OT stelt de risicomanagement centraal.

De CS-Risicomanagement OT MET is de aanpak om maatregelen te ontwerpen.

MET hanteert voor OT een specifiek CS-Dreigingsbeeld als input voor risicomanagement.

De uitgangspunten en resultaten van de risicoanalyses worden vastgelegd in de CS-Dossier voor elke afzonderlijk object (ICT/OT-systeem).

De wijze waarop de borging is georganiseerd is vastgelegd in dit document.

Door het volgen van de aanpak in dit Voorschrift wordt de informatiebeveiliging voor operationele systemen ingevuld en wordt voldaan aan de BIO.

9. Bronnen & referenties

[1] Rapport 'Digitale dijkverzwarening' van de Algemene Rekenkamer, 2019.

[2] CSIR 2015, Cybersecurity-implementatieRichtlijnen, Rijkswaterstaat.