Informatiebeveiligingseisen aan leveranciersrelaties

Eigenaar	CISO ProRail
Auteurs	Afdeling Cybersecurity
Kenmerk	IPP-O.04
Versie	1.93
Datum	November 2024
Bestand	Informatiebeveiligingseisen aan leveranciersrelaties ProRail
Status	Definitief
Informatieclassificatie	Intern

Inhoud

1	**Doel document, toepassingsgebied en gebruikers**	**4**
2	**Eisen**	**4**
3	**BIO/ISO**	**10**
Bijlage A	**Zorgplicht vanuit de NIS2**	**11**
Bijlage B	**Afkortingen en termen**	**12**

Versiebeheer en distributie

	Versiebeheer		
Versie	**Datum**	**Wijziging**	**Auteur**
1.9	21-04-2024	Nieuwe opzet	Afdeling Cybersecurity
1.91	7-05-2024	Reviewcommentaar verwerkt van J-P. van Eekelen, M. de Heuvel, J. Petit, R. Rensman	Afdeling Cybersecurity
1.92	14-06-2024	Reviewcommentaar verwerkt van A. Westendorp, M. de Heuvel, H. Taibi	Afdeling Cybersecurity
1.93	10-11-2024	Structuur document aangepast, herziening/verplaatsing beleidsitems die in feite eisen zijn.	Afdeling Cybersecurity

	Distributie		
Versie	**Datum**		
1.9	21-04-2024	ISM's afdeling Cybersecurity, J-P. van Eekelen, A. Westendorp, E. Hilgenga, R. Boot, M. de Heuvel, R. Rensman	
1.91	7-05-2024	Interne versie afdeling Cybersecurity	
1.92	14-06-2024	Afdeling Cybersecurity, J-P. van Eekelen, A. Westendorp, E. Hilgenga, M. de Heuvel, R. Rensman, H. Taibi, M. Lacomblé	
1.93	10-11-2024	J. Petit, S. van der Aa, C. de Jong, H. Taibi	

1 Doel document, toepassingsgebied en gebruikers

In dit document worden de eisen voor informatiebeveiliging in leveranciersrelaties beschreven.

De eisen zijn toe te passen op het Informatie Technologie (IT) - en Operationele Technologie (OT)-domein en richten zich op leveranciers en uitbestedingspartners (in dit document verder genoemd: leverancier),

- die toegang hebben tot en/of diensten verlenen ten behoeve van informatiesystemen, OT-objecten en informatie/data/gegevens(verzamelingen),
    - die gebruikt, verstrekt of bewaard wordt door of namens ProRail,
        - door medewerkers van deze partijen in de breedste zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Met ProRail wordt bedoeld de ProRail organisatie en de onder haar gestelde (dochter)ondernemingen.

Doelgroepen van dit document zijn in de eerste plaats de ProRail medewerkers die het beleid en eisen omtrent informatiebeveiliging in relatie tot leveranciersrelaties toepassen en beheren, zoals tendermanagers, contractmanagers, juristen, informatie security officers en coördinatoren, projectleiders, product owners, etc.

In bijlage B zijn de gebruikte afkortingen toegelicht.

Voor extern gebruik is een apart document beschikbaar ‘Informatiebeveiligingsbeleid en– eisen voor leveranciersrelaties’, met de classificatie Publiek/Openbaar. Dit document kan ter beschikking gesteld worden aan leveranciers in het kader van inkoop en aanbestedingstrajecten en de uitvoering van de gecontracteerde dienstverlening.

2 Eisen

In onderstaande tabel zijn de eisen weergegeven die ProRail stelt aan een formele leveranciersrelatie.

Toepassing van de eisen volgt het principe ‘Pas toe of leg uit’, aangezien niet alle eisen op iedere leveranciersrelatie betrekking (kunnen) hebben. Bij het bepalen van het programma van eisen, de inkoopvoorwaarden en/of het contract wordt deze afweging gemaakt in overleg met de afdeling Cybersecurity.

De omschrijving van de eis geeft de essentie weer, niet de letterlijke verwoording zoals die in een contract e.d. opgenomen zou moeten zijn. Deze eisen zijn onderwerp van toetsing zoals in IBP-O.04 (Beleid voor leveranciersrelaties) beschreven is. Algemene eisen aan het product of dienst komen voort uit de Security baselines IT en OT en de toe te passen security architectuur. Specifieke eisen worden gesteld op basis van risicoanalyses.

De bronnen voor deze eisen zijn:

- De Wet beveiliging netwerken en informatiesystemen (Wbni);
- De tweede Europese richtlijn Netwerken en Informatiesystemen (NIS2);
- De ISO27002 norm voor Informatiebeveiliging;
- De ISO22301 norm voor Bedrijfscontinuïteit en de sub normen;
- De Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen (BIACS);
- De Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2022);
- De handreikingen van de Informatiebeveiligingsdienst.

A. AVG	Bij de verwerking van persoonsgegevens houdt de leverancier zich aan de eisen uit de Algemene Verordening Gegevensverwerking.

	Leveranciers dienen zich te conformeren aan de procedure Melding Datalekken van ProRail. Tijdlijnen, voorwaarden, contactpersonen, etc. worden opgenomen als onderdeel van de verwerkersovereenkomst.
	Met alle derde partijen die als verwerker voor of namens ProRail persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld. De leverancier verwerkt persoonsgegevens in voorkomende gevallen uitsluitend in opdracht en op basis van schriftelijke instructies van ProRail, tenzij er sprake is van andersluidende wettelijke voorschriften.
B. Awareness	De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers periodiek en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).
C. Bedrijfscontinuïteit	De leverancier heeft aantoonbaar en actueel inzicht in de risico's binnen zijn bedrijfsprocessen die een bedreiging zouden kunnen vormen voor de continuïteit en/of veiligheid van de bedrijfsprocessen van ProRail.
	De leverancier is aantoonbaar in staat een ernstige crisis te managen doordat deze een crisis/BCM-organisatie heeft ingericht en onderhoudt.
	De leverancier heeft BCM-beleid opgesteld t.a.v. zijn continuïteitsdoelstellingen, - organisatie en -strategie en deelt dit met ProRail.
	De leverancier heeft aantoonbaar adequate maatregelen genomen om de continuïteitsrisico's voor de eigen en de bedrijfsprocessen van ProRail te voorkomen (preventie), dan wel de impact op de bedrijfsvoering te beperken (repressie). Deze maatregelen zijn opgenomen in bedrijfscontinuïteitsplannen.
	Voor elke IT- of OT-asset dient ten minste volgens het ingerichte back-up proces een back-up te worden gemaakt na elke (functionele) systeemwijziging of op vooraf bepaalde, periodieke termijnen.Indien het om welke reden dan ook niet mogelijk is om een back-up te maken, dan wordt dit vastgelegd en, op basis van een risicoanalyse, een alternatieve werkwijze gekozen en beschreven.
	De leverancier maakt door test- en oefenverslagen aannemelijk dat, bij een onverhoopte calamiteit met onacceptabele impact voor ProRail, deze maatregelen daadwerkelijk toegepast worden en het belang van ProRail topprioriteit krijgt. Dit is vooral van belang als ProRail voor de leverancier niet een van de belangrijkste klanten is en/of een substantieel deel van de aandelen in handen zijn van een organisatie die gevestigd is in een land dat aangemerkt wordt als 'vijandige' statelijke actor.
	Indien relevant en mogelijk, wordt ProRail betrokken bij oefeningen en testen.
D. Certificeringen en normenkaders	Een certificering tegen de ISO27001 norm voor Informatiebeveiliging en de bijbehorende beheersmaatregelen is vereist, waarbij de dienstverlening aan ProRail volledig in de scope van de certificering valt. Indien deze daarover niet beschikt, dient de leverancier de verzekering te geven dat de informatiebeveiliging op een vergelijkbaar niveau als de ISO-norm is ingericht door het overleggen van bewijsstukken.

	Een certificering tegen de ISO22301 gewenst, waarbij de dienstverlening aan ProRail volledig in de scope van de certificering valt. In ieder geval dient de leverancier de verzekering te geven dat de bedrijfscontinuïteit op een vergelijkbaar niveau als de ISO-norm is ingericht door het overleggen van bewijsstukken.
	Relevante certificaten (bv. ISO 27001/22301/IEC62443/BIACS) en/of assurance verklaringen (bv. SOC2, ISAE 3400/2) worden ter beschikking gesteld aan ProRail. De scope en inrichting van het ISMS en BCMS worden door ProRail getoetst op relevantie en effectiviteit.
E. Contactpersoon	Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in bijvoorbeeld de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.
F. Escrow	De leverancier draagt zorg voor een escrow regeling, indien relevant. Zo heeft ProRail in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur.
G. Exit-strategie	De leverancier beschikt over een uitwerking van een exit-strategie, die goedgekeurd is door ProRail. Deze strategie omvat minimaal afspraken over hoe de data overgedragen en daarna verwijderd/vernietigd wordt bij wisseling van leverancier of overname van de dienst door ProRail.
H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.
I. Gegevensverwerking en -opslag	De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
	Indien informatie opgeslagen wordt binnen de infrastructuur van de leverancier, dient deze beveiligd te worden conform het beveiligingsniveau dat bij deze informatie is overeengekomen. Dit betekent dat persoonsgegevens per definitie minimaal Vertrouwelijk geclassificeerd zijn. (Bij bijzondere persoonsgegevens : Geheim)
	De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.
J. Geheimhouding	Ter waarborging van de vertrouwelijkheid van Vertrouwelijke en/of Geheime informatie wordt een Non Disclosure Agreement (NDA) of vergelijkbare vertrouwelijkheidsverklaring ondertekend door de leverancier (en indien relevant door ProRail). De leverancier verplicht zijn personeel aantoonbaar om de geheimhoudingsverplichting na te komen.
K. Incidenten	Er wordt een vaste procedure voor het melden van (IT en OT) beveiligingsincidenten en kwetsbaarheden afgesproken tussen ProRail en de leverancier. Deze dient aan te sluiten bij de bestaande incidentmanagementprocessen binnen Prorail.

	De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan de Autoriteit Persoonsgegevens. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
	De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.
L. Monitoren en loganalyse	Monitoring is ingericht voor alle IT- en OT-systemen. Wanneer monitoring niet mogelijk is of niet rendabel is, dan dient hiervoor een risico gebaseerde redeneerlijn te worden opgesteld. Monitoring van de remote toegang en beheer op afstand dient altijd te worden ingericht.
	Activiteiten van gebruikers en beheerders dienen ten behoeve van audittrailing passend beveiligd vastgelegd te worden in logboeken. Deze registratie wordt op verzoek van ProRail door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld.
M. Onderaanneming en toeleveranciers	De leverancier dient inzicht te geven in welke derden mogelijk toegang kunnen hebben tot ProRail data. Denk aan hosting providers, softwareleveranciers, support partijen, subverwerkers, etc.
	Alle voorwaarden en eisen op het gebied van informatiebeveiliging die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
	De leverancier moet desgevraagd inzage geven in de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden.
	Het is de leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ProRail, de uitvoering van een contract geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten. Deze toestemming zal niet op onredelijke gronden geweigerd worden.
	ProRail wordt zo snel mogelijk op de hoogte gebracht indien de leverancier wijzigingen aanbrengt bij het uitbesteden van zijn eigen (deel)processen. Hierdoor kan ProRail bepalen of er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen in de wijze van beheersing van de door de leverancier uitbestede (deel) processen. Deze inzet, beheersing en wijziging van sub verwerking wordt opgenomen in de overeenkomst met de leverancier.
N. Periodiek overleg en rapportages	In de contracten worden expliciete prestatie-indicatoren en bijbehorende verantwoordingsrapportages gespecificeerd met betrekking tot informatiebeveiliging.
	ProRail ontvangt periodiek rapportages van de leveranciers over de geleverde prestatie met betrekking tot informatiebeveiliging en bespreekt die conform een vooraf afgesproken frequentie.
	In het geval van af te nemen diensten met afgesproken serviceniveaus op gebied van informatiebeveiliging wordt tussen de leverancier en ProRail een SLA afgesloten.
O. Personeel	Medewerkers van de leverancier overleggen voor aanvang van de werkzaamheden bij ProRail een recente Verklaring Omtrent het Gedrag (VOG) conform de eisen uit het ProRail beleid. De

	leverancier stemt met ProRail voorafgaand de noodzaak en de wijze van overleggen en beheren af.
	ProRail kan het personeel van de leverancier, dat voor de uitvoering van het contract wordt ingeschakeld, aan een veiligheidsonderzoek (laten) onderwerpen als bijvoorbeeld een Vertrouwensfunctie wordt vervuld. De leverancier verleent aan dat onderzoek zijn volledige medewerking. ProRail kan op grond van de uitkomsten daarvan de inzet van het betrokken personeelslid bij de uitvoering van de overeenkomst weigeren.
	De leverancier toont aan dat het personeel voldoende kennis en kunde heeft om de werkzaamheden binnen ProRail te verrichten. Dit hangt samen met beveiligingseisen, die bijvoorbeeld door scholing en/of voldoende kennis en kunde gebruikersfouten beperken.
	Extern personeel dient zich te houden aan de gedragsregels van ProRail.
	Indien een medewerker van de leverancier, die door zijn werkzaamheden op locatie van ProRail komt en/of toegang heeft tot infrastructuren en gegevens, uit dienst gaat, wordt dit minimaal twee weken van tevoren gemeld aan de contractmanager van ProRail.
P. Retour/vernietiging bedrijfsmiddelen en informatie	Op verzoek retourneert of vernietigt de leverancier, dit naar keuze van ProRail, onverwijld alle door ProRail ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevensdragers en back-ups). Dit geldt ook voor alle gegevens, inclusief persoonsgegevens, ook in cloudomgevingen.
	Voorafgaand aan hergebruik of verwijdering van apparatuur dienen alle gegevens op de daarin aanwezige opslagmedia op betrouwbare wijze te worden verwijderd. Dit gebeurt door een hiertoe gecertificeerde organisatie. Als bewijs van verwijdering dient een certificaat door het vernietigingsbedrijf te worden aangeleverd.
Q. Auditrecht	ProRail kan op enig moment een audit, waaronder een penetratietest, (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit is niet nodig als de leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met ProRail.
R. Risicomanagement	De leverancier vult direct na contractering een self-assessment in waaruit de mate van beveiliging blijkt, met als kader het beveiligingsbeleid van ProRail.
	De gecontracteerde leverancier dient gedurende de looptijd van het contract te beschikken over een actuele, gedocumenteerde en door zijn management geaccordeerde classificatie en risicoanalyse, uitgevoerd voor de te leveren IT-en OT-diensten. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de continuïteit van de bedrijfsprocessen van ProRail zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald.
	Beheersmaatregelen die voortkomen uit de risicoanalyse en waar ProRail een aandeel in de implementatie heeft, worden afgestemd met ProRail.

	De leverancier dient ProRail (op verzoek) te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.
S. Security en BCM by Design	De gangbare principes rondom Security by Design/Default en BCM by Design zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet binnen de opdracht inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
T. Security testing	ProRail kan een security test, zoals een penetratietest, laten uitvoeren als onderdeel van de acceptatie en/of validatie om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Een security test is niet nodig als de leverancier door middel van rapportages aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke security test heeft plaatsgevonden en de relevante resultaten deelt met ProRail.
	Indien ProRail in het kader van acceptatie of validatie een security test (laat) verricht(en), stelt ProRail zo spoedig mogelijk een testverslag op en zendt dat ondertekend aan Opdrachtnemer. In het testverslag worden geconstateerde bevindingen en gebreken vastgelegd alsook of ProRail de geteste asset goed- of afkeurt. Afspraken worden tussen ProRail en de leverancier gemaakt over de opvolging van de bevindingen.
U. Toegang tot digitale infrastructuur en gegevens	Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT- en OT-systemen. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.
	De toegang van medewerkers van de leverancier is beperkt tot systemen bij ProRail, de leverancier en afgenomen diensten bij derden, die benodigd zijn voor het leveren van de dienst (need to know principe).
	Alleen bij een aantoonbare noodzaak krijgen leveranciers remote toegang tot de ProRail omgeving.
	Remote toegang en beheer op afstand tot IT- en OT-omgevingen dient via de door ProRail voorgeschreven oplossing plaats te vinden en te worden gemonitord.
	Om toegang te krijgen tot systemen van ProRail wordt gebruik gemaakt van beveiligde verbindingen met multi-factor authenticatie (token) die voldoen aan ProRail beleid en architectuur.
	Toegang tot de systemen is beperkt met wachtwoorden volgens de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail.
V. Toegang tot fysieke infrastructuur	Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen, wat geborgd is in een (mechanisch) sluitplan.
W. Wijzigingsbeheer	Substantiële wijzigingen van de leveranciersorganisatie en -processen met impact voor ProRail dienen door de leverancier tijdig kenbaar gemaakt te worden aan ProRail. Dit wordt opgenomen als onderdeel van de overeenkomst met de leverancier.

3 BIO/ISO

Dit beleidsdocument beschrijft de invulling van de volgende beheersmaatregelen van de BIO:

5.19 Informatiebeveiliging in leveranciersrelaties
5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten
5.21 Beheren van informatiebeveiliging in de ICT-keten
5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
5.23 Informatiebeveiliging voor het gebruik van clouddiensten
6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten
8.30 Uitbestede systeemontwikkeling

Een aantal van deze beheersmaatregelen wordt verder ook uitgewerkt in de IT- en OT Security baselines van ProRail.

Bijlage A Zorgplicht vanuit de NIS2

Onder de NIS2 is sprake van een zorgplicht van organisaties voor informatiebeveiliging. Deze komt neer op het uitvoeren en actueel houden van een risicomanagement. Op basis hiervan dienen organisaties passende maatregelen te nemen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en hun informatie te beschermen.

Deze zorgplicht geldt voor ProRail, maar wordt door ProRail ook gevraagd van haar leveranciers. Onderstaande tabel bevat de tien punten van de zorgplicht (bron: NCSC) en de eisen waarmee ProRail deze in haar leveranciersrelatie geborgd heeft. **Het is van belang om te beseffen dat niet alleen de eisen uit dit document voor die borging zorgen, maar ook ander beleid, security baselines, afspraken, richtlijnen, e.d.**

Deze tien punten zijn per definitie onderwerp van gesprek bij het verkrijgen van assurance van kritieke leveranciers.

NIS2 eisen	Borging door
1. Een risicoanalyse en beveiliging van informatiesystemen	R. Risicomanagement
2. (Beleid en procedures over) incidentenbehandeling	K. Incidenten
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen	C. Bedrijfscontinuïteit G. Exit strategie
4. Beveiliging van de toeleverancierskeketen	Dit document en het bijbehorende beleid. A. AVG D. Certificeringen en normenkaders E. Contactpersoon J. Geheimhouding N. Periodiek overleg en rapportages Q. Auditrecht W. Wijzigingsbeheer
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden	F. Escrow I. Gegevensverwerking L. Monitoring en loganalyse S. Security en BCM by Design
6. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen	T. Security testing
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging	B. Awareness
8. Beleid en procedures over het gebruik van cryptografie en encryptie	H. Gegevensuitwisseling
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa	M. Onderaanneming en toeleveranciers O. Personeel P. Retour/vernietiging bedrijfsmiddelen en informatie U. Toegang tot digitale infrastructuren en gegevens V. Toegang tot fysieke infrastructuren
10. Het gebruik van multifactor-authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit	H. Gegevensuitwisseling

Bijlage B Afkortingen en termen

Assurance	Het bewijs dat afspraken, eisen e.d. ook daadwerkelijk in de praktijk zijn gebracht zoals ze zijn bedoeld c.q. het proces om daartoe te komen.
AVG	Algemene Verordening Gegevensverwerking
BCM	BedrijfsContinuïteitsManagement
BIACS	Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen
CSIR	CyberSecurity Implementatie Richtlijn (Rijkswaterstaat)
IBP	InformatiebeveiligingsBeleid ProRail
IT	Informatie Technologie
IPP	InformatiebeveiligingsProcedure ProRail
ISO	International Organization for Standardization
NIS2	Verordening Network and Information Systems
OT	Operationele Technology
SLA	Service Level Agreement
Wbni	Wet beveiliging netwerken en informatiesystemen