

Informatiebeveiligingsbeleid voor leveranciersrelaties

Eigenaar Executive Committee (ExCo)
Auteurs Afdeling Cybersecurity

Kenmerk IBP-O.04
Versie 1.92
Datum Mei 2024

Bestand Informatiebeveiligingsbeleid voor leveranciersrelaties ProRail

Status Definitief
Informatieclassificatie Openbaar

Inhoudsopgave

1	Doel document, toepassingsgebied en gebruikers	3
2	Algemene uitgangspunten informatiebeveiliging in leveranciersrelaties	3
3	Uitgangspunten eisen aan leveranciers	4
4	Kritieke leveranciers	5
5	Assurance	6
6	Borging van cybersecurity in processen	6
7	BIO/ISO	7
	Bijlage A Toelichting assurance	8
	Bijlage B Cybercheck Rijksoverheid	11
	Bijlage C: Afkortingen en termen	12

1 Doel document, toepassingsgebied en gebruikers

In dit document worden doelstellingen, het toepassingsgebied, basisregels en uitgangspunten voor informatiebeveiliging in relatie tot leveranciersrelaties beschreven.

De scope van dit beleid omvat het Informatie en Communicatie Technologie (ICT) - en Operationele Technologie (OT)-domein en richt zich op:

- Leveranciers, uitbestedingspartners, leveranciers en ketenpartners (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 meest brede 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 op de eerste plaats de ProRail medewerkers die het beleid en eisen omtrent informatiebeveiliging in relatie tot leveranciersrelaties toepassen en beheren, zoals tendermanagers, contractmanagers, informatie security officers en coördinatoren, projectleiders, product owners, etc.,

Daarnaast kan dit document ter beschikking gesteld worden aan leveranciers in het kader van inkoop en aanbestedingstrajecten en de uitvoering van de gecontracteerde dienstverlening.

2 Algemene uitgangspunten informatiebeveiliging in leveranciersrelaties

In het kader van informatiebeveiliging in leveranciersrelaties worden door ProRail de volgende algemene uitgangspunten gehanteerd:

- A. ProRail is en blijft eindverantwoordelijk voor de informatiebeveiliging van de producten en dienstverlening die binnen de organisatie ingezet worden: ProRail draagt daarom zorg voor de monitoring van de dienstverlening en ziet actief toe op een goede bescherming van de informatie door de leverancier.
- B. Het informatiebeveiligingsbeleid van ProRail is leidend. Over onderwerpen waar ProRail geen beleid heeft of waar de leverancier ander beleid heeft wordt overleg gepleegd en afspraken worden gedocumenteerd (pas toe of leg uit). De leverancier is door ProRail op de hoogte gebracht van de belangrijkste en, voor de dienstverlening relevante, onderdelen van het informatiebeveiligingsbeleid en accepteert deze door ondertekening van het contract.
- C. In situaties waarin beveiligingseisen worden opgelegd door leveranciers, is voorafgaand aan het aangaan van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de ProRail.
- D. Informatiebeveiligingseisen worden gespecificeerd in alle fase van de levenscyclus van een leveranciersrelatie: van offertefase tot beëindiging van het contract.
- E. De security baselines ICT en OT vormen het minimale niveau van beveiliging voor de dienstverlening. De leverancier brengt de baselines in praktijk of neemt maatregelen die dezelfde mate van beheersing opleveren. Hier geldt 'pas toe of leg uit'.
- F. In situaties waarin contractvoorwaarden worden opgelegd door derde partijen, wordt voorafgaand aan het tekenen van het contract met een risicoafweging duidelijk gemaakt wat hiervan de consequenties zijn voor ProRail. Er dient expliciet gemaakt te worden welke consequenties geaccepteerd worden en welke gemitigeerd dienen te zijn bij het aangaan van de overeenkomst.
- G. Ongeacht de bepalingen in de overeenkomst heeft de leverancier een professionele zorgplicht en meldplicht voor de informatiebeveiliging van zijn producten en diensten. ProRail mag er in alle redelijkheid van uit gaan dat deze plichten worden vervuld.
- H. Met leveranciers zijn eenduidige en gedocumenteerde afspraken (contract, SLA, etc.) gemaakt over veilige dienstverlening en eisen aan informatiebeveiliging.

- I. De leverancier dient ProRail op verzoek te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.

3 Uitgangspunten eisen aan leveranciers

Hiërarchie in eisen

Er is sprake van een hiërarchie in eisen. Op het hoogste niveau staan de eisen uit de generieke voorwaarden die ProRail stelt door toepassing van:

- ProRail Inkoopvoorwaarden 2017 (algemeen); of
- ARBIT 2022 (ICT); of
- UAV-GC (bouwprojecten); of
- Algemene Voorwaarden assets (OT) of,
- Algemene Voorwaarden voor het Prestatiegericht Onderhoud.

De eisen uit het informatiebeveiligingsbeleid van ProRail zijn aanvullend of verdiepend hierop.

Het uitgangspunt hierbij is dat eisen rond informatiebeveiliging aan *leveranciersrelaties* zoveel mogelijk op het hoogste niveau geborgd worden, dus in inkoopvoorwaarden en andere generieke kaders. Hierdoor is op contractniveau beperkt, specifiek maatwerk nodig.

Echter, tussen de genoemde documenten bestaan anno 2024 zeer grote verschillen in hoe informatiebeveiliging geborgd is. Daarom bevat IBB 1.6 de complete lijst met eisen, ongeacht of ze al opgenomen zijn op een hoger niveau. Waar een eis uit IBB 1.6 al geborgd is, vervalt de eis uit het informatiebeveiligingsbeleid ten gunste van de bovenliggende eis.

Aanvulling en verdieping van generieke eisen aan de leveranciersrelatie en de betreffende dienstverlening vindt plaats door middel van toepassing van de eisen uit dit document en, indien de situatie dit vereist, de eisen uit andere onderdelen van het beveiligingsbeleid en de Security Baselines ICT en OT.

Eisen zijn proportioneel

Niet bij alle leveranciersrelaties kan men spreken over informatiebeveiligingsrisico's. Ook zijn niet alle risico's even groot. Daarom is het zaak om onderscheid aan te brengen, zodat informatiebeveiligingseisen, de methodes om vast te stellen dat de eisen ook goed in praktijk gebracht worden (assurance) en bijbehorende maatregelen proportioneel zijn. Bij het bepalen van eisen kan ook gebruik gemaakt worden van de *ICO Wizard* van de Rijksoverheid (beschikbaar op internet).

ProRail kent drie hoofdcriteria waarmee de risico's binnen de leveranciersrelatie geduid worden:

- Cruciaal voor de dienstverlening: uitval van het product, dienst of de leverancier zelf heeft een grote negatieve impact op de bedrijfsvoering van ProRail (beschikbaarheids/continuïteitsrisico). Hiermee wordt ook een 1-op-1 relatie gelegd met het BCM-beleid en BCM-planvorming.
- Toegang tot/verwerken van vertrouwelijke of geheime informatie: de leverancier heeft toegang (digitaal of papier) tot vertrouwelijke of geheime bedrijfsinformatie (incl. persoonsgegevens) en kan deze eventueel ook aanmaken, veranderen of wijzigen (vertrouwelijkheidsrisico). Subcriteria zijn:
 - Alleen kunnen lezen van informatie (digitaal of andere media);
 - Kunnen aanmaken, aanpassen of verwijderen van informatie;
- Toegang tot missie/businesskritieke systemen: de leverancier heeft als gebruiker/ontwikkelaar/beheerder toegang tot die systemen die een belangrijke rol spelen in de bedrijfsvoering van ProRail (beschikbaarheids- en integriteitsrisico). Subcriteria zijn:
 - De leverancier heeft de rol van gebruiker;
 - De leverancier heeft de rol van ontwikkelaar/beheerder;

Indien één of meer van deze drie criteria van toepassing zijn, dan is er sprake van een kritieke leverancier, waarbij de eisen en de wijze van assurance strenger zijn dan voor leveranciers die hierbuiten vallen.

Eisen zijn compliant aan wet- en regelgeving

De eisen die ProRail stelt zijn in lijn met de voor ProRail vigerende wet- en regelgeving op het gebied van informatiebeveiliging.

- Wet Beveiliging Netwerken en Informatiesystemen (WBNI) - tot in werking treding van de Nederlandse wetgeving onder de NIS2;
- NIS2 - per 17 oktober 2024;
- Nederlandse wetgeving op basis van NIS2 - per begin 2024;
- ISO27001/2 - Informatiebeveiliging, met de BIO als Nederlandse verbijzondering;
- ISO22301 – Bedrijfscontinuïteit;
- Algemene Verordening Gegevensbescherming;
- IEC 62443, met de CSIR en BIACS als Nederlandse verbijzondering.

Daar waar aanwezig wordt gebruik gemaakt van (inter)nationale certificeringen en keurmerken ten behoeve van assurance.

4 Kritieke leveranciers

- Voor een (potentiële) kritieke leverancier worden de eisen en maatregelen bepaald door middel van een risicoanalyse. Dit gebeurt in de offertefase (generiek), de contracteringsfase (specifieke leverancier en dienstverlening) en eventueel ook in de implementatiefase en afrondingsfase van de betreffende dienstverlening. In de contracteringsfase kan een risicoanalyse ook een penetratietest omvatten.
- Voor een kritieke leverancier is een certificering tegen de ISO27001 verplicht, waarbij de dienstverlening aan ProRail volledig in de scope van de certificering valt. Indien deze daarover niet beschikt, dient de leverancier de assurance te geven dat de informatiebeveiliging op een vergelijkbaar niveau als de ISO-norm is ingericht door het overleggen van bewijsstukken.
- Voor een kritieke leverancier met een cruciaal belang voor ProRail is 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 assurance te geven dat de bedrijfscontinuïteit op een vergelijkbaar niveau als de ISO-norm is ingericht door het overleggen van bewijsstukken.

De lijst met kritieke leveranciers wordt beheerd door de afdeling Cybersecurity en gepubliceerd op de pagina Informatiebeveiliging op Focus.

5 Assurance

Aan de hand van het bovenstaande past ProRail de volgende methodes toe bij het verkrijgen van assurance en het vormgeven en bewaken van een leveranciersrelatie. Door deze op te nemen als item in een leveranciersovereenkomst krijgt ProRail de mogelijkheid om het niveau van informatiebeveiliging vast te stellen. Een korte toelichting per methode is te vinden in bijlage A.

De methodes zijn verdeeld in drie categorieën: voor contractering, tijdens uitvoering van het contract en na afronding van het contract.

Criterium	Vooraf	Tijdens	Na
Cruciaal voor de dienstverlening	Due diligence ISO/assurance toets Risicomanagement Right to audit	Toetsen actuele ISO/Assurance Wijzigingsbeheer Beheer sub-verwerking Periodiek overleg & rapportages Uitnuten auditrecht Toets continuïteitsmanagement Security posture monitoring	Toetsen uitvoering exitclausule
Vertrouwelijke /Geheime informatie	NDA ISO/assurance toets Risicomanagement Verwerkersovereenkomst (persoonsgegevens) Informatie uitwisseling Gebruiken, bewaren en vernietigen	Toetsen actuele ISO/Assurance Wijzigingsbeheer Beheer sub-verwerking Procedure datalekken Periodiek overleg & rapportages Monitoring & loganalyse Uitnuten auditrecht & rechten betrokkenen Security posture monitoring	Toetsen opheffing toegang (log/fysiek) Toetsen retour informatie en bedrijfsmiddelen
Missie/businesskritieke systemen	NDA ISO/assurance toets Risicomanagement ISO/assurance verklaringen Right to audit	Toetsen actuele ISO/Assurance Wijzigingsbeheer Beheer sub-verwerking Periodiek overleg & rapportage Monitoring & loganalyse Uitnuten auditrecht Security posture monitoring	Toetsen opheffing toegang (log/fysiek) Toetsen retour informatie en bedrijfsmiddelen
Overig	Selfassessment tegen beveiligingsbeleid	Jaarlijkse check toegangsrechten (log/fysiek) Jaarlijkse check BIV	Toetsen opheffing toegang (log/fysiek) Toetsen retour informatie en bedrijfsmiddelen
Security baselines			

6 Borging van cybersecurity in processen

Cybersecurity is een integraal kwaliteitsaspect en heeft daarom ook een plaats in de inkoop- en aanbestedingsprocessen en het contract/leveranciersmanagement.

Ook hier geldt het 3 Lines Model met een duidelijke taakafbakening tussen de eerste (operatie) en tweede lijn (Cybersecurity en Procurement). In onderstaande tabel is beschreven wat de taak is van de betrokken rollen en functies.

Rol	Fase	Taak
Opdrachtgever / projectleider	Vooraf	Borgen dat alle betrokken disciplines betrokken zijn bij het inkoop/aanbestedingsproces
Tendermanager	Vooraf	
Contractmanager		
Information Security Officer	Vooraf	
Expertiseteam	Vooraf	Security posture scan uitvoeren naar kwetsbaarheden en non-compliances

7 BIO/ISO

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

- 5.19 Informatiebeveiliging in leveranciersrelaties
- 5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten
- 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

Sommige van deze beheersmaatregelen worden verder ook uitgewerkt in de ICT- en OT-baselines van ProRail.

Bijlage A Toelichting assurance

In de volgende tabel zijn de assurance methodes per levensfasefase van een contract beschreven. **Om deze ook daadwerkelijk te kunnen uitvoeren worden ze als items in een offertes en contracten opgenomen.**

NB. De omschrijving geeft de essentie weer, niet de letterlijke verwoording zoals die in een contract e.d. opgenomen is. Deze hangt ook af van het gebruikte model met voorwaarden en bepalingen: die tekst is leidend.

Assurance	Omschrijving
Vooraf	
A. Bedrijfscontinuïteit	Middels een Business Impact Analyse (BIA) of vergelijkbare methode is door ProRail vastgesteld: - welke van de processen van de leverancier noodzakelijk zijn voor de levering/dienst aan ProRail en wat de mogelijke impact is van uitval van deze processen (na hoeveel tijd worden de gevolgen voor ProRail onacceptabel) - welke resources van de leverancier noodzakelijk zijn (gebouwen, IT/OT systemen, machines, personeel, data, nutsvoorzieningen etc.) - idem t.a.v. de subcontractors van de leverancier (Tier 2 en 3) - welke risico's de beschikbaarheid of kwaliteit hiervan zodanig zouden kunnen bedreigen dat voor ProRail onacceptabele gevolgen kunnen optreden)
B. Due diligence	Bij zeer cruciale leveranciersrelaties bestaat de mogelijkheid om een onderzoek te doen naar de (financiële) gezondheid van de leverancier. Een dergelijk onderzoek heeft z'n eigen randvoorwaarden en staat los van de uiteindelijke overeenkomst.
C. Geheimhouding	Ter waarborging van de vertrouwelijkheid van 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.
D. ISO/Assurance toets	Relevante certificaten (bv. ISO 27001) en/of assurance verklaringen (bv. SOC2, ISAE 3402) worden opgevraagd. De inrichting van het ISMS en BCMS wordt getoetst op relevantie voor ProRail.
E. Prestaties en rapportages	- In de contracten worden expliciete prestatie-indicatoren en bijbehorende verantwoordingsrapportages gespecificeerd. - In het geval van af te nemen diensten met afgesproken serviceniveaus op gebied van informatiebeveiliging wordt tussen de leverancier en ProRail een SLA afgesloten.
F. Right-to-audit	ProRail kan op enig moment een externe audit, waaronder een penetratietest, laten uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. 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. Dit recht moet worden opgenomen als onderdeel van de overeenkomst met de leverancier.
G. Risicomanagement	Informatiebeveiliging en bedrijfscontinuïteit worden door ProRail aantoonbaar (op basis van een BIV & business impactanalyse en risicoanalyse) meegewogen: bij het besluit een derde partij wel of niet in te schakelen.

	• de <i>Cybercheck</i>¹ en de <i>Quickscan Nationale Veiligheid bij Inkoop en Aanbesteden</i>² van de Rijksoverheid worden uitgevoerd. • van zowel leveranciers als hun onderaannemers wordt nagegaan of er issues zijn met economische veiligheid (aandeelhouders uit China/Rusland/etc.) • bij het vaststellen van de relevante risico's om zo eisen in een offerte, inkoop en aanbestedingstraject te bepalen. • indien vereist worden risicoanalyse uitgevoerd tijdens uitvoering van het contract en bij afsluiting.
H. Self assessment tegen beveiligingsbeleid	De leverancier vult als onderdeel van de contractering een self assessment in waaruit de mate van beveiliging blijkt, met als kader het beveiligingsbeleid van ProRail (of BIO norm).
I. Toegang tot digitale infrastructuur en gegevens	• Er wordt een gedocumenteerde formele en actuele procedure afgesproken zijn voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot ICT- en OT-systemen. Deze procedure wordt periodiek 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 ICT- en OT-omgevingen dient via de door ProRail gebruikte oplossing plaats te vinden en te worden gemonitord. • Om toegang te krijgen tot systemen van ProRail wordt gebruik gemaakt van beveiligde verbindingen met twee-factor authenticatie (token) die voldoen aan ProRail beleid/architectuur. • Toegang tot de systemen is beperkt met wachtwoorden conform de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail.
J. 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.
K. Verwerkersovereenkomst	Met alle derde partijen die als verwerker voor of namens ProRail persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld. Indien er sprake is van verwerking van persoonsgegevens, houdt de leverancier zich aan de geldende wet- en regelgeving op het terrein van het beschermen van persoonsgegevens. De leverancier verwerkt persoonsgegevens in voorkomend geval uitsluitend in opdracht en op basis van schriftelijke instructies van ProRail, tenzij er sprake is van andersluidende wettelijke voorschriften.
Tijdens	
L. Periodieken check BIV	De beoordeling van het vereiste niveau van de beschikbaarheid, integriteit en vertrouwelijkheid wordt periodiek (jaarlijks) herijkt. Bij gebleken wijziging wordt de risico's en maatregelen herijkt.
M. Monitoren en Loganalyse	• Indien leverancier onbegeleid toegang heeft tot IT/OT en/of locaties van ProRail, dient regelmatige monitoring en/of loganalyse plaats te vinden op deze toegang (door ProRail). • Activiteiten van gebruikers en beheerders dienen in het kader van audittrailing passend beveiligd in logbestanden vastgelegd te

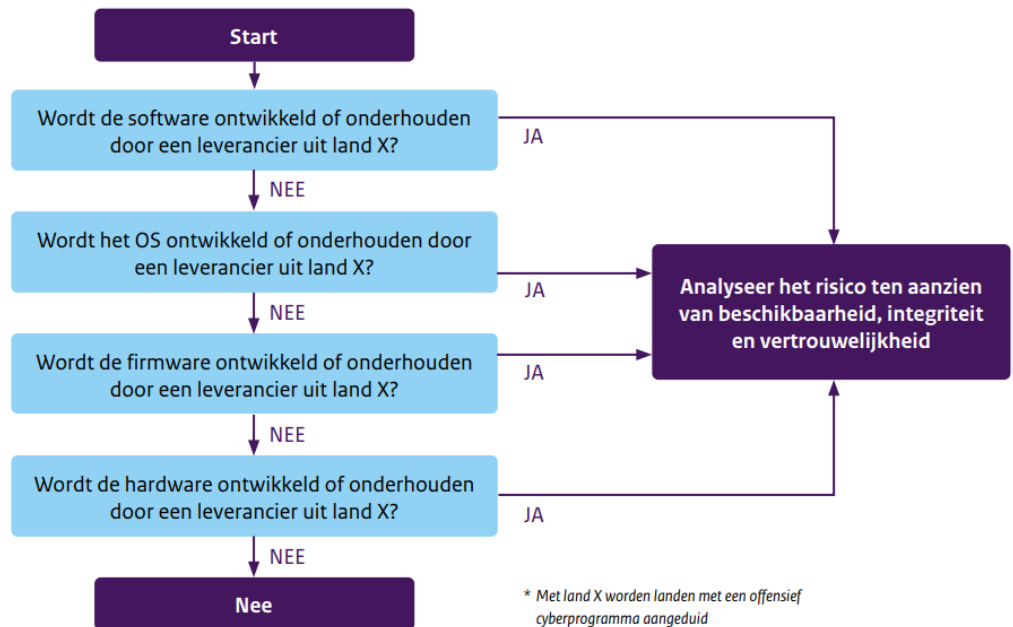
¹ [Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

² [Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden | PIANOo - Expertisecentrum Aanbesteden](#)

	worden. Deze registratie wordt op verzoek van ProRail, door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld. Monitoring is ingericht voor alle OT-systemen. Wanneer monitoring niet mogelijk is of niet rendabel is, dan dient hiervoor een risicogebaseerde redeneerlijn te worden opgesteld. Monitoring van de remote toegang en beheer op afstand dient altijd te worden ingericht.
N. Periodiek overleg & rapportages	- Periodiek dient de prestatie van de leverancier op het gebied van informatiebeveiliging beoordeeld te worden op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen zijn, zoals service-levels, incidenten, changes, projecten, etc. - ProRail ontvangt periodieke rapportages van de leveranciers over de geleverde dienstverlening (incidenten, changes, patches, servicelevels, etc.).
O. Procedure datalekken	Leveranciers dient zich te conformeren aan de procedure melding datalekken van ProRail. Tijdlijnen, voorwaarden, contactpersonen, etc. worden opgenomen als onderdeel van de verwerkersovereenkomst.
P. Security posture monitoring	De (internet facing) infrastructuur van een SaaS leverancier wordt periodiek geautomatiseerd gescand ter beoordeling van de kwaliteit van beveiliging (open poorten, verouderde protocollen, etc.).
Q. Toegang tot infrastructuur en gegevens	Periodiek wordt door ProRail een review uitgevoerd van de toegangsrechten van medewerkers van de gecontracteerde Leverancier (en de derden die de Leverancier inschakelt) voor de systemen bij ProRail en de Leverancier.
R. Toetsen actuele ISO/Assurance	Periodiek (bv. jaarlijks) opvragen bij leverancier van relevante en actuele certificaten (bv. ISO 27001) en/of assurance verklaringen (bv. SOC2, ISAE 3402).
S. Toets continuïteitsmanagement	Jaarlijkse beoordeling van de maatregelen van de leverancier op BCM gebied (onderdeel van periodiek overleg).
T. Uitnutten auditrecht	Naar behoefte van ProRail en in overleg met de leverancier uitnutten van het recht om (bij behoefte) onderzoek te (laten) doen bij de leverancier (en/of zijn subverwerkers) naar opzet, bestaan en/of werking van processen en maatregelen. Dit recht wordt opgenomen als onderdeel van de overeenkomst met de leverancier.
U. Uitnutten rechten Betrokkenen	Indien relevant (onderdeel verwerkersovereenkomst) dient de leverancier mee te werken aan het uitnutten van rechten van /door betrokkenen (bv. recht op inzage)
V. 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.
Na	
W. Toetsen opheffing toegang	Toetsen of de rechten van de medewerkers van de leverancier ook daadwerkelijk zijn ingetrokken.
X. Toetsen retour informatie en bedrijfsmiddelen	Toetsen of de afspraken die bij het item Gebruiken, bewaren en vernietigen ook conform zijn uitgevoerd.
Y. Toetsen uitvoering exit clause	Indien de exit-strategie is toegepast, wordt achteraf gecontroleerd of dit ook daadwerkelijk opgeleverd heeft wat afgesproken was.

Bijlage B Cybercheck Rijksoverheid

De Cybercheck



[Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

Bijlage C: Afkortingen en termen

Assurance	Het bewijs dat afspraken, eisen e.d. ook daadwerkelijk in de praktijk zijn gebracht zoals ze zijn bedoeld.
AVG	Algemene Verordening Gegevensverwerking
BIACS	Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen
CSIR	CyberSecurity Implementatie Richtlijn (Rijkswaterstaat)
ICT	Informatie en Communicatie Technologie
ISO	International Organization for Standardization
NIS2	Network and Information Systems
OT	Operationele Technology
Wbni	Wet beveiliging netwerken en informatiesystemen