# Informatiebeveiligingsbeleid voor leveranciersrelaties

| | |
|---|---|
| Eigenaar | Executive Committee (ExCo) |
| Auteurs | Afdeling Cybersecurity |
| Kenmerk | IBP-O.04 |
| Versie | 1.92 |
| Datum | Juni 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 |
| Bijlage A Toelichting assurance | | 7 |
| 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 Technology (OT)-domein en richt zich op:

- Leveranciers, uitbestedingspartners 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 breedste zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

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

Interne doelgroepen van dit document zijn op de eerste plaats de ProRail medewerkers die het beleid en eisen voor informatiebeveiliging in relatie tot leveranciersrelaties toepassen en beheren, zoals tendermanagers, contractmanagers, juristen, information 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. Hiervoor is een aparte versie beschikbaar met de classificatie Openbaar.

# 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 gemaakte afspraken worden gedocumenteerd (pas toe of leg uit). De voor de dienstverlening relevante onderdelen van het informatiebeveiligingsbeleid worden verwerkt in plannen van eisen en contracten.
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 ProRail en de leverancier.
D. Informatiebeveiligingseisen worden gespecificeerd in alle fasen van de levenscyclus van een leveranciersrelatie: van aanbestedingsfase tot beëindiging van het contract.
E. Indien een leverancier niet kan voldoen aan de informatiebeveiligingseisen van ProRail, maar het wel de wens van ProRail is om de leverancier te contracteren, dan zal de leverancier een verbeterplan opstellen waarin binnen een redelijke tijd alsnog aan de eisen wordt voldaan. Het verbeterplan wordt beoordeeld door de afdeling Cybersecurity.
F. De security baselines ICT en OT van ProRail vormen het minimale niveau van beveiliging voor de dienstverlening. De leverancier brengt de security baselines in praktijk of neemt maatregelen die dezelfde mate van beheersing opleveren. Hier geldt ‘pas toe of leg uit’.
G. In situaties waarin contractvoorwaarden m.b.t. informatiebeveiliging worden opgelegd door derde partijen, wordt in de aanbestedingsfase door middel van 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.

H. 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.
I. Met leveranciers zijn eenduidige en gedocumenteerde afspraken (contract, SLA, etc.) gemaakt over veilige dienstverlening en eisen aan informatiebeveiliging.
J. De leverancier dient ProRail op verzoek te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening, zie ook punt E in Bijlage A.

# 3 Uitgangspunten eisen aan leveranciers

Hiërarchie in eisen

Er is sprake van een hiërarchie in eisen. Op het hoogste, generieke, 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.

Vervolgens worden eisen vastgelegd in diverse templates voor bijvoorbeeld Programma's van Eisen en contracten. De eisen uit het informatiebeveiligingsbeleid van ProRail zijn aanvullend of verdiepend hierop.

Het uitgangspunt hierbij is dat eisen rond informatiebeveiliging aan leveranciersrelaties en de te leveren diensten en producten zoveel mogelijk in modelcontracten en modellen voor Programma van Eisen geborgd worden.

Aanvulling en verdieping van de eisen in modellen vindt plaats door middel van toepassing van de eisen uit dit document en, als de situatie dit vereist, de eisen uit andere onderdelen van het beveiligingsbeleid en de Security Baselines ICT en OT. De relevantie wordt vastgesteld door de opdrachtgever van de aanbesteding en de afdeling Cybersecurity.

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 bewijs te verkrijgen dat de informatiebeveiligingseisen ook goed in praktijk gebracht worden (assurance) en bijbehorende maatregelen proportioneel zijn.

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 werkingtreding van de Cyberbeveiligingswet;
- NIS2 – in werkingtreding per 17 oktober 2024;
- Cyberbeveiligingswet, wetgeving op basis van NIS2 - per medio 2025;
- ISO27001/2 - Informatiebeveiliging, met de BIO als Nederlandse verbijzondering voor de Overheid;
- 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

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 het treinverkeer (beschikbaarheids-/continuïteitsrisico). Hiermee wordt ook een 1-op-1 relatie gelegd met het BCM-beleid en de 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;

Als één of meer van deze drie criteria van toepassing zijn, dan is er sprake van een *kritieke leverancier:* een leverancier waaraan in het kader van informatiebeveiliging strengere eisen gesteld worden vanwege het belang voor ProRail van deze leverancier en de dienstverlening.

- Voor een (potentiële) kritieke leverancier worden de eisen en maatregelen bepaald door middel van een risicoanalyse. Dit gebeurt voorafgaand aan de aanbestedingsfase (algemeen beeld, nog geen keuze voor leverancier of dienst) en eventueel voorafgaand aan de contracteringsfase (als de keuze voor specifieke leverancier en dienstverlening extra risico's met zich meebrengt).
- Voor een kritieke leverancier is een certificering tegen de ISO27001 norm voor Informatiebeveiliging en de bijbehorende beheersmaatregelen vereist, 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.

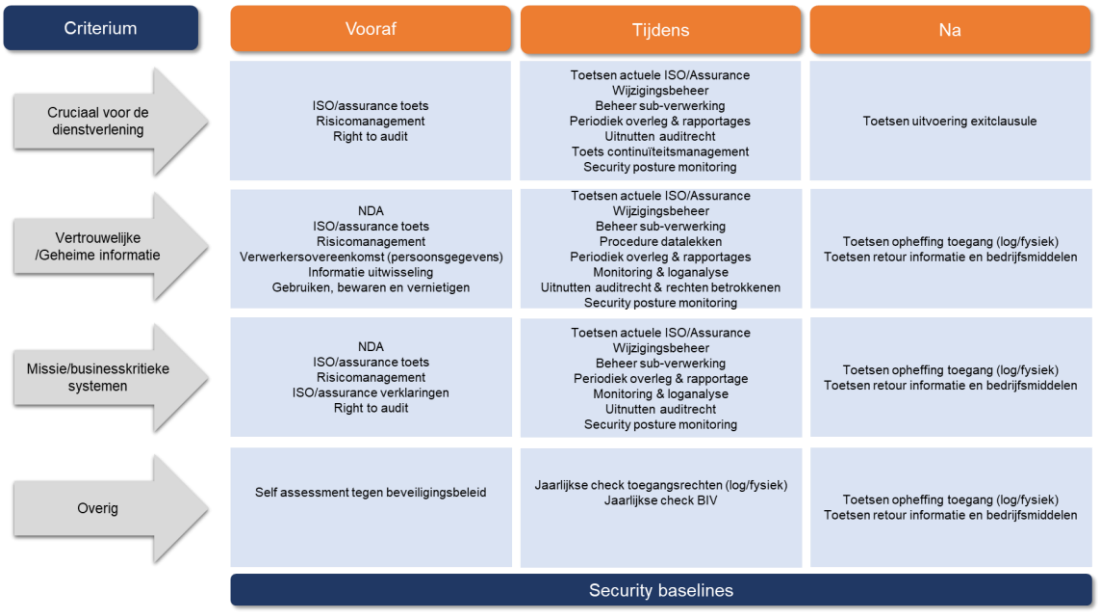
De lijst met kritieke leveranciers wordt beheerd door de afdeling Procurement, in samenwerking met de afdeling Cybersecurity.

# 5 Assurance

Onder assurance wordt in dit document verstaan: a. bewijs dat aan de informatiebeveiligingseisen van ProRail wordt voldaan en b. het proces/de methode om dat bewijs te verkrijgen.

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 Programma van Eisen en/of een contract krijgt ProRail formeel 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 fasen: voorafgaand aan contractering (veelal aanbestedingstraject), tijdens uitvoering van het contract en na afronding van het contract.




**Figuur 1.** Assurance methodes per fase

## Bijlage A Toelichting assurance

In de volgende tabel zijn de assurance methodes per levensfase van een contract beschreven**. Om deze ook daadwerkelijk te kunnen uitvoeren worden ze als items in 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 | • Met een Business Impact Analyse (BIA) of vergelijkbare methode is door ProRail vastgesteld:<br>  ○ Welke 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).<br>  ○ Welke resources van de leverancier noodzakelijk zijn (gebouwen, IT/OT systemen, machines, personeel, data, nutsvoorzieningen etc.).<br>  ○ Idem t.a.v. de subcontractors van de leverancier (tier 2)<br>  ○ Welke risico's de beschikbaarheid of kwaliteit hiervan zodanig zouden kunnen bedreigen dat voor ProRail onacceptabele gevolgen kunnen optreden).<br>• 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 'statelijke actor'. |
| B. 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. |
| C. 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. |
| D. Prestaties en rapportages | • In de contracten worden expliciete prestatie-indicatoren en bijbehorende verantwoordingsrapportages gespecificeerd.<br>• In het geval van af te nemen diensten met afgesproken serviceniveaus op gebied van informatiebeveiliging wordt tussen de leverancier en ProRail een SLA afgesloten. |
| E. 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.<br><br>Dit recht moet worden opgenomen als onderdeel van de overeenkomst met de leverancier. |

| | |
|---|---|
| F. Risicomanagement | Informatiebeveiliging en bedrijfscontinuïteit worden door ProRail aantoonbaar meegenomen (op basis van een Beschikbaarheids-, Integriteits- en Vertrouwelijkheid- (BIV) analyse & business impactanalyse en risicoanalyse):<br>• Bij het besluit een derde partij wel of niet in te schakelen.<br>  • De *Cybercheck*[1] en de *Quickscan Nationale Veiligheid bij Inkoop en Aanbesteden*[2] van de Rijksoverheid worden uitgevoerd.<br>  • Van zowel leveranciers als hun onderaannemers wordt nagegaan of er issues zijn met economische veiligheid (aandeelhouders uit China/Rusland/etc.)<br>• Bij het vaststellen van de relevante risico's om zo eisen in een offerte, inkoop en aanbestedingstraject te bepalen.<br>• Indien vereist worden risicoanalyses uitgevoerd tijdens uitvoering van het contract en bij afsluiting. |
| G. 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. |
| H. 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 ICT- en OT-systemen. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.<br>• 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).<br>• Alleen bij een aantoonbare noodzaak krijgen leveranciers remote toegang tot de ProRail omgeving.<br>• 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.<br>• Om toegang te krijgen tot systemen van ProRail wordt gebruik gemaakt van beveiligde verbindingen met multi-factor authenticatie (token) die voldoen aan ProRail beleid/architectuur.<br>• Toegang tot de systemen is beperkt met wachtwoorden volgens de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail. |
| I. 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. |
| J. Verwerkersovereenkomst | Met alle derde partijen die als verwerker voor of namens ProRail persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.<br><br>Als 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 voorkomende gevallen uitsluitend in opdracht en op basis van schriftelijke instructies van ProRail, tenzij er sprake is van andersluidende wettelijke voorschriften. |
| Tijdens | |

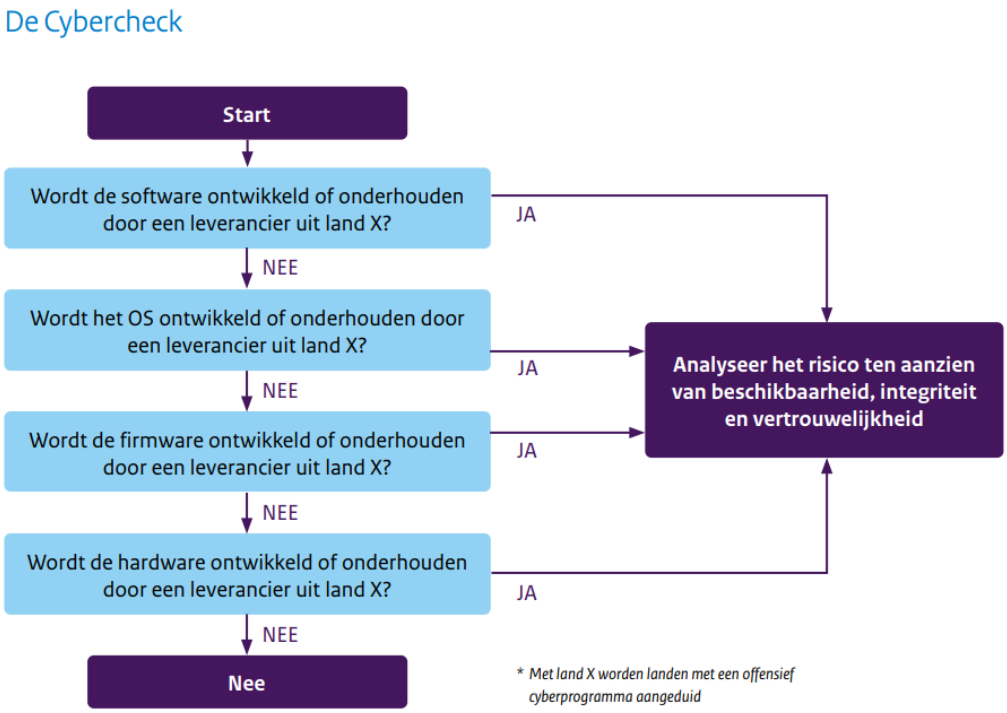
[1] Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

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

| | |
|---|---|
| K. Periodieke check BIV | De beoordeling van het vereiste niveau van de beschikbaarheid, integriteit en vertrouwelijkheid wordt periodiek (jaarlijks) herijkt. Bij gebleken wijziging worden de risico's en maatregelen herijkt. |
| L. 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).<br>• 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.<br>• Monitoring is ingericht voor alle 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. |
| M. Periodiek overleg & rapportages | • ProRail ontvangt periodieke rapportages van de leveranciers over de geleverde dienstverlening.<br>• 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 (bv. service-levels, incidenten, changes, projecten, etc.). |
| N. Procedure datalekken | Leveranciers dienen zich te conformeren aan de procedure Melding Datalekken van ProRail. Tijdlijnen, voorwaarden, contactpersonen, etc. worden opgenomen als onderdeel van de verwerkersovereenkomst. |
| O. Security posture monitoring | De (internetfacing) infrastructuur van een SaaS leverancier wordt door ProRail periodiek geautomatiseerd gescand ter beoordeling van de kwaliteit van beveiliging (open poorten, verouderde protocollen, etc.). |
| P. 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. |
| Q. 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). |
| R. Toets continuïteitsmanagement | Jaarlijkse beoordeling van de maatregelen van de leverancier op BCM-gebied (onderdeel van periodiek overleg). |
| S. 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. |
| T. Uitnutten rechten Betrokkenen | Indien relevant (en onderdeel van de verwerkersovereenkomst) dient de leverancier mee te werken aan het uitnutten van rechten van/door betrokkenen (bv. recht op inzage). |
| U. 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 | |
| V. Toetsen opheffing toegang | Toetsen of de rechten van de medewerkers van de leverancier ook daadwerkelijk zijn ingetrokken. |
| W. Toetsen retour informatie en bedrijfsmiddelen | Toetsen of de afspraken die bij het item Gebruiken, bewaren en vernietigen ook volgens afspraken zijn uitgevoerd. |

| | |
|---|---|
| X. Toetsen uitvoering exit clausule | Wanneer de exit-strategie is toegepast, wordt achteraf gecontroleerd of dit ook daadwerkelijk opgeleverd heeft wat afgesproken was. |

## Bijlage B Cybercheck Rijksoverheid




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 c.q. het proces om daartoe te komen. |
| AVG | Algemene Verordening Gegevensverwerking |
| BCM | BedrijfsContinuïteitsManagement |
| BCMS | BedrijfsContinuïteitsManagementSysteem |
| BIACS | Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen |
| CSIR | CyberSecurity Implementatie Richtlijn (Rijkswaterstaat) |
| IBP | InformatiebeveiligingsBeleid ProRail |
| ICT | Informatie en Communicatie Technologie |
| IPP | InformatiebeveiligingsProcedure ProRail |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| NIS2 | Verordening Network and Information Systems |
| OT | Operationele Technology |
| SLA | Service Level Agreement |
| Wbni | Wet beveiliging netwerken en informatiesystemen |