Risicomanagementbeleid ProRail

Eigenaar	RvB
Auteur	Hoofd IRC
Datum vastgesteld door de ExCo	08 februari 2023
Datum goedgekeurd door de RvB	08 februari 2023
Status	Definitief

Miljoenen euro's schade én onnodig drukke wegen: hét spoor naar de Rotterdamse haven is te vaak kapot

De enige spoorlijn die door de Rotterdamse haven loopt, is regelmatig stuk en onbruikbaar. Daardoor lopen vervoersbedrijven miljoenen euro's mis én is het onnodig druk op de wegen. ProRail belooft, na publicatie van een vernietigend rapport, beterschap.

ProRail: tot zeker 12.00 uur geen treinverkeer

Lees voor

UTRECHT - Door het winterse weer rijden zondag in elk geval tot 12.00 uur geen treinen. Of het treinverkeer daarna wel kan worden opgestart, is nog onzeker. Overal in het land zijn storingen, bijvoorbeeld aan wissels.

'Spoorwerkers staan bloot aan kankerverwekkende stof'

08 april 2021 08:32
Aangepast: 08 april 2021 09:18

Zestig vacatures, 5.000 sollicitanten: waarom is er dan toch een tekort aan treindienstleiders?

Tekort aan verkeersleiders dreigt: minder treinen als ProRail ze niet vindt

Er dreigt een groot tekort aan treinverkeersleiders bij ProRail. Als de spoorbeheerder deze niet vindt, dan zit er niets anders op dan minder treinen te laten rijden.

Wil je dit voorkomen? Lees dan het beleid!!

Inhoud

1 Inleiding

Risicomanagement is het identificeren en kwantificeren van risico's binnen een organisatie en het opstellen van maatregelen om deze risico's te mitigeren. Hierbij hoort het in kaart brengen van risico's met kans en effect, en maatregelen om de kans of het effect te verkleinen. Iedereen is in zijn of haar dagelijks werk - bewust of onbewust - bezig met risicomanagement, want onze werkzaamheden zijn gericht op het bereiken van bepaalde doelen, groot of klein. Vrijwel altijd zijn er onzekere factoren die ertoe kunnen leiden dat ProRails doelen niet of niet volledig bereikt worden. Hoe eerder eventuele risico's worden geïdentificeerd, hoe meer mogelijkheden er zijn om belangen, strategieën en risico's tegen elkaar af te wegen. Risicomanagement draagt bij aan het behalen van de doelstellingen van ProRail en vormt een onmisbaar onderdeel van de bedrijfsvoering van de organisatie.

Uitgangspunt bij risicomanagement is dat alle bedrijfsonderdelen zelf als eerste lijn verantwoordelijk zijn voor de beheersing van de risico's en maatregelen in hun eigen afdeling en hiervoor ook passende risicomanagement methodes hanteren zolang deze binnen dit beleid vallen. Best practices op het gebied van corporate governance geven aan dat in een complexe organisatie een risicomanagementafdeling nodig is die hier zelfstandig toezicht op houdt. Dit wordt vormgegeven door de afdeling IRC als 2e lijnverantwoordelijke, welke bestaat uit het hoofd IRC en risico adviseurs.

Dit beleid beschrijft het kader en de werkwijze voor risicomanagement op alle niveaus in de besturing van de organisatie en de rol van IRC hierin. Het is bedoeld voor directie, management en medewerkers van ProRail. Het helpt de 1e lijn bij het doeltreffend inrichten van risicomanagementprocessen en het opstellen van rapportages die aansluiten op de centrale rapportages van ProRail en de besluitvorming over de beheersmaatregelen. De RvB is eindverantwoordelijk voor de ProRail risico's maar delegeert de praktische uitvoering naar de hoofden van de afdelingen. Indien er verschillen bestaan tussen de afdelingsniveaus in het behandelen van risico's, wordt dit expliciet in dit document aangegeven.

Het risicomanagementbeleid behandelt de systematische verbetering van risicomanagement voor een periode van tien jaar voor de hele organisatie. Na tien jaar wordt het beleid geëvalueerd. Tussentijdse voorstellen voor wijzigingen worden beoordeeld door de afdeling IRC en eventueel in het beleid aangepast.
Dit beleid is van toepassing op ProRail B.V. en haar deelnemingen, voor zover ProRail daarover zeggenschap heeft. De inhoud van het beleid zal periodiek worden geactualiseerd, voorgelegd ter besluitvorming aan de Raad van Bestuur en ter informatie aan de Raad van Commissarissen.

De ExCo heeft het beleid goedgekeurd en de RvB heeft met het beleid vastgesteld d.d. 08 februari 2023.

2 Belang risicomanagement

ProRail is eindverantwoordelijk voor het behalen van de eigen bedrijfsdoelstellingen en onderkent dat dit alleen mogelijk is door kennis te nemen van en rekening te houden met de belangen van externe partijen.

De wereld waarin ProRail opereert is complex door de veelheid aan regels, voorschriften en toezichthouders en het beperkte aantal grote leveranciers voor het ontwerp, de aanleg en het onderhoud van stations en spoorweginfrastructuur. Dit gegeven, gecombineerd met een ambitieus prestatieniveau dat vervoerders, reizigers en concessieverleners van de organisatie verwachten, maakt de externe omgeving uitdagend en inherent risicovol.

Investeringen in de spoorweginfrastructuur betreffen vaak plannen voor de lange termijn. De vele belanghebbenden vragen goed overleg en een lange aanloop bij de uitvoering van onze plannen. Dit maakt de besluitvorming over financiering van aanleg, onderhoud en vervanging, onder invloed van de politiek, de economische en technologische ontwikkelingen tot een complexe exercitie.

De steeds sneller veranderende omgeving waarbinnen ProRail opereert, kenmerkt zich door veranderingen in klimaat, technologie en maatschappij en de inherente traagheid van planontwikkeling en hoge kosten die hiermee gepaard gaan. Dit maakt aanpassing van het spoorsysteem en de besluitvorming hierover risicovol. Voor ProRail is het daarom van zeer groot belang om systematisch en structureel om te gaan met de risico's die voortkomen uit de regiefunctie op het spoor.

ProRail draagt de eindverantwoordelijkheid om haar doelstellingen op doeltreffende, doelmatige en rechtmatige wijze te verwezenlijken. Risicomanagement helpt bij het realiseren van die doelstellingen.

Risicomanagement stelt ons in staat om op een proactieve manier onzekere risicovolle gebeurtenissen of situaties te identificeren en maatregelen te treffen. Het geeft ons de mogelijkheid om door middel van transparante communicatie van elkaar te leren en elkaar te helpen. Hoe eerder we eventuele risico's identificeren hoe sneller we kunnen acteren door na zorgvuldige analyse, belangen, strategieën en risico's tegen elkaar af te wegen. Risicomanagement draagt zo bij aan weloverwogen continue verbetering en een goed bestuur van de organisatie.

Het systeem van risicomanagement dat door ProRail wordt gehanteerd is gebaseerd op de internationale normen voor risicomanagement volgens COSO ERM.[1] Het risicomanagement is onderdeel van de bedrijfsvoering en daarmee een continu verbeterproces.

3 Verantwoordelijkheden binnen risicomanagement

Het risicomanagement van ProRail is georganiseerd langs het zogenaamde Three Lines Model (3LM).

Uitgangspunt van het 3LM model is dat het lijnmanagement (de business) als 1e lijn verantwoordelijk is voor haar eigen processen en voor het behalen van de aan hem / haar gedelegeerde doelstellingen en de beheersing van de risico's die hiermee verbonden zijn.

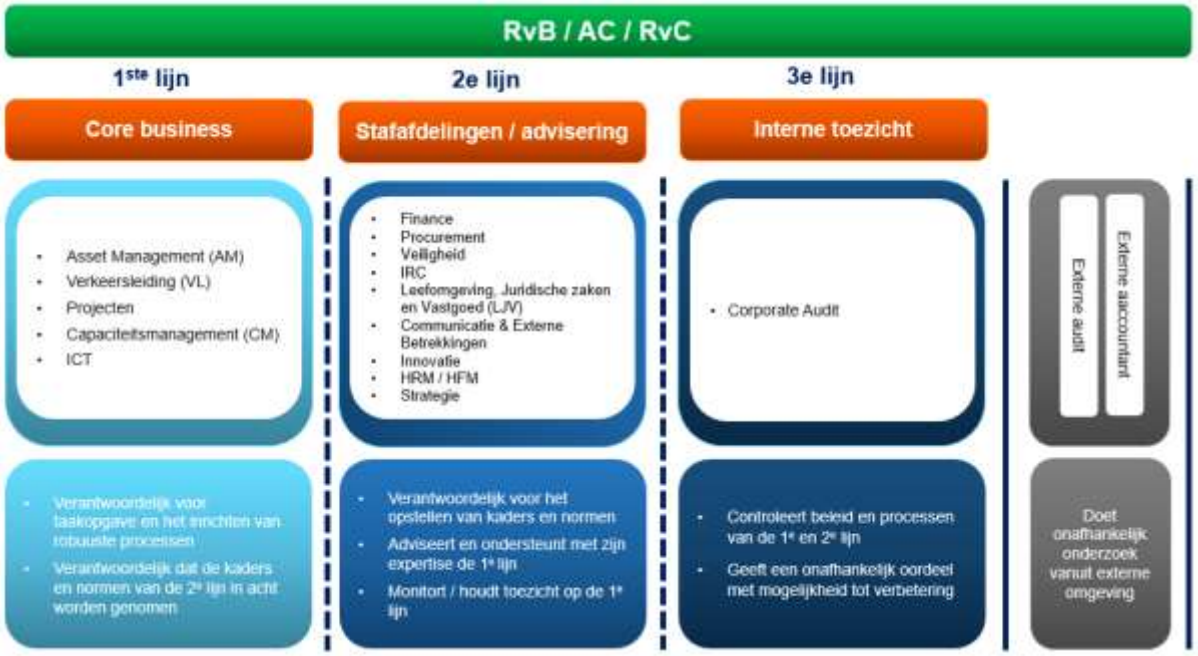
De afdeling IRC is de 2e lijn die de 1e lijn ondersteunt, adviseert en uitdaagt, en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. De 2e lijn ontwikkelt de systemen voor een goed proces van risicomanagement en beheersing, altijd ter ondersteuning van de 'business'. Hieronder valt ook het ontwikkelen, bijhouden en stellen van beleid en normen. Business Continuity Management (BCM) is ook 2e lijn maar beperkt zich tot het inrichten van uitwijkmogelijkheden en fall-back scenario's voor de business continuity risico's.

Ten slotte is het wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de 1e en 2e lijn soepel functioneert en daarover een objectief, onafhankelijk een oordeel velt met mogelijkheden tot verbetering. Of er geen overlapping is, of, erger, blinde vlekken bestaan. Deze functie betreft de 3e lijn, die bij ProRail wordt uitgeoefend door Corporate Audit. De 3e

[1] Het COSO ERM-model is verreweg het meest gebruikte raamwerk voor het beoordelen en inrichten van risicomanagement. COSO ERM staat voor: *Committee of Sponsoring Organizations of the Treadway Commission* (COSO); Enterprice Risk Management (ERM).

lijnverantwoordelijke ziet ook toe op de activiteiten van de 1e en 2e lijnverantwoordelijke. Dit kan ook een externe partij zijn zoals ILT of ISZW.

Three Lines Model



3.1 De Raad van Bestuur (RvB)

De RvB stelt als eindverantwoordelijke het kader voor risicomanagement vast. RvB als eindverantwoordelijke delegeert verantwoordelijkheid voor risicomanagement naar de risico-eigenaren (bijvoorbeeld de hoofden van desbetreffende afdelingen).

3.2 Het management

Het management is verantwoordelijk voor het realiseren van de doelstellingen van de organisatie en voor de opgedragen taken en/of prestaties. Deze verantwoordelijkheid gaat gepaard met de daartoe noodzakelijke bevoegdheden. Bij het nastreven van de doelstellingen die aan het management zijn toegewezen, kunnen risico's ontstaan. Het identificeren, analyseren en beheersen van de risico's vormt een belangrijk onderdeel van de verantwoordelijkheid van de manager. De manager voorziet geïdentificeerde risico's van een beheersingsmaatregel en van een taakhouder. Daarnaast is de manager verantwoordelijk voor een adequate vastlegging van de beheersing van de risico's.

3.3 De afdeling IRC

De afdeling IRC opereert onafhankelijk van de belangen van de afdelingen en is als 2e lijn verantwoordelijk voor het opstellen van het beleid en de algemene normen voor het risicomanagement bij ProRail, waardoor gezorgd wordt voor een uniform begrip in het omgaan met risico's binnen de organisatie. Ook is IRC verantwoordelijk voor het up-to-date houden van de risicomatrix die als heatmap door de hele organisatie kan worden gebruikt bij het beoordelen van de ernst van risico's (op kans en impact). Wijzigingen van de risicomatrix voor specifieke doeleinden dienen altijd te worden afgestemd met IRC en daar te worden vastgelegd. Indien applicaties, systemen of andere tools voor registratie m.b.t. risicomanagement worden aangeschaft of ontwikkeld, dan heeft IRC hierin een adviserende rol. IRC is tevens verantwoordelijk voor het adviseren over, faciliteren van en houden van toezicht op de werking van risicomanagementsystemen (risicomanagementprocessen, de administratie en ontwikkeling ervan) in de 1e lijn. De 1e lijn is zelf verantwoordelijk voor de deugdelijke werking van systemen en processen op het gebied van risicomanagement die binnen zijn of haar verantwoordelijkheid vallen.

Wanneer vanuit de 1e lijn risicomanagementbeleid wordt opgesteld voor deelgebieden of wanneer opleidingen risicomanagement worden gegeven, is het management verantwoordelijk om dit af te stemmen met de 2e lijn (IRC). Op deze manier wordt de 2e lijn in de gelegenheid gesteld om (i) te toetsen of het deelbeleid risicomanagement van de 1e lijn past binnen dit risicomanagementbeleid en (ii) het beleid in de deelgebieden op een consistente manier samenhangt met risicomanagementbeleid en -activiteiten binnen andere afdelingen en deelgebieden.

3.4 Corporate Audit

Corporate Audit kan op aangeven van de AC / RvC een audit uitvoeren op de opzet en de werking van het risicomanagementsysteem en rapporteert dan hierover aan de organisatie en de RvB. Op basis hiervan worden verbetervoorstellen geformuleerd en geïmplementeerd wanneer de audit hiertoe aanleiding geeft.

3.5 De Audit Commissie

De Audit Commissie (als onderdeel van de Raad van Commissarissen) houdt toezicht op de kwaliteit van de risicobeheersing en de doelmatigheid en doeltreffendheid van het risicomanagementsysteem.

4 Risicomanagement-componenten

4.1 Risiconiveaus en risicogebieden

Risico's kunnen zich voordoen op ProRailbreed, tactisch of uitvoerend niveau. Wij onderscheiden bij ProRail 16 risicogebieden die elk een risico eigenaar met een dashboard hebben.

4.2 Risicobereidheid

De risicobereidheid komt tot uitdrukking in de risicomatrix en het verband tussen impact en kans (en de verschillende gradaties daarbinnen). De risicobereidheid geeft aan hoeveel risico men bereid is aan te gaan bij het realiseren van de doelstellingen.

4.3 Risicomatrix

Het kwantificeren van de restrisico's gebeurt met behulp van de risicomatrix. Hierin worden enkel de netto (of rest) risico's gemeten, dat wil zeggen een restrisico dat overblijft na toegepaste mitigerende maatregelen. Het meten gebeurt door op basis van expert judgement te bepalen in een bepaalde periode (afhankelijk van de doelstelling) hoe groot de kans van optreden is en hoe groot het gevolg is. Hierbij wordt mede een inschatting gemaakt van de werking van de bestaande beheersingsmaatregelen. Hiermee wordt de positie van het risico in de risicomatrix bepaald. De positie in de matrix bepaalt de acceptatiegraad. Dit wordt uitgedrukt in de kleuren groen, geel, oranje, rood:

- Groen: Geen aanvullende beheersingsmaatregelen zijn nodig;
- Geel: Beheersingsmaatregelen zijn nodig;
- Oranje: Beheersingsmaatregelen zijn nodig;
- Rood: Beheersingsmaatregelen zijn nodig.

De kleur zegt iets over de combinatie van kans en impact. Hoe roder het risico, hoe groter de kans en impact.

Gevolgen worden bepaald aan de hand van de impact die de risicogebeurtenis kan hebben op de realisatie van de doelstellingen en op de bedrijfswaarden van ProRail. De bedrijfswaarden zijn afgeleid uit de missie en de doelstellingen van ProRail. De volgende bedrijfswaarden staan in de impactcategorieën opgenomen:

- **Financiële schade / kosten**: de mate waarin ProRail efficiënt en effectief omgaat met haar financiële middelen;
- **Fysieke veiligheid**: de mate waarin de activiteiten / bedrijfsvoering van ProRail veilig zijn voor mensen onder wie reizigers, baanwerkers en bedienend personeel, omwonenden en overweggebruikers. Dit betreft ook ARBO-veiligheid;

- **Compliance: wet- en regelgeving**: de mate, waarin ProRail zich houdt aan vigerende wet- en regelgeving;
- **Duurzaamheid**: de mate, waarin ProRail haar bedrijfsactiviteiten duurzaam uitvoert;
- **Reputatie / Stakeholders**: de mate waarin ProRail waarde hecht aan haar positie in de maatschappij bij de stakeholders;
- **Impactvolle storingen op de infra**: de mate, waarin storingen impact hebben op de infra.

De risico-eigenaar als 1e lijn verantwoordelijke kiest op welke bedrijfswaarde het risico de meeste impact heeft. Het is mogelijk dat het risico impact heeft op meerdere impactcategorieën. De bedrijfswaarde waar het hoogst op gescoord wordt, bepaalt de positie op de impactschaal. De impact neemt van links naar rechts in ernst toe.

Het inschatten van risico's kent altijd een bepaalde mate van subjectiviteit. Daarom is het goed om de inschattingen aan de hand van de risicomatrix te toetsen / samen te doen met anderen. Daarmee wordt de betrouwbaarheid van de risico-inschatting verhoogd.

De risicomatrix dient elke tien jaar opnieuw door de RvB te worden vastgesteld. De afdeling IRC houdt elk jaar een evaluatie en stelt zo nodig een tussentijdse wijziging voor. Risico-eigenaren kunnen een voorstel tot wijziging bij IRC indienen.

Risicomatrix

KANS	IMPACT: wordt gerelateerd aan de bedrijfswaarden van ProRail					
	1. Geen tot zeer gering (A)	2. Gering (B)	3. Beperkt (C)	4. Aanzienlijk (D)	5. Groot (E)	6. Zeer groot (F)
6. Zeer regelmatig: meer dan 100 keer per jaar of dagelijks (100+)	5	6	7	8	9	10
5. Regelmatig: 10 tot 100 x per jaar of dagelijks (10-100)	4	5,5	6	7	8	9
4. Waarschijnlijk: 1x per jaar tot 10x per jaar (1-10)	3	4	5,5	6	7	8
3. Incidenteel: 1x in 10 jaar tot 1x per jaar (1/10-1)	2	3	4	5,5	6	7
2. Onwaarschijnlijk: 1x in 100 jaar tot 1x in 10 jaar (1/100-1/10)	1	2	3	4	5,5	6
1. Zeer onwaarschijnlijk: minder dan 1x in 100 jaar (1/1000-1/100)	0	1	2	3	4	5,5

	IMPACT wordt gerelateerd aan de bedrijfswaarden van ProRail					
	1. Geen tot zeer gering (A)	2. Gering (B)	3. Beperkt (C)	4. Aanzienlijk (D)	5. Groot (E)	6. Zeer groot (F)
Fysieke veiligheid (Verbetert)	Geen of zeer gering en herstelbaar letsel, geen medische behandeling. Voorbeelden: schram of buil.	Gering en herstelbaar letsel. Voorbeeld: verstuikte enkel.	Matig en herstelbaar letsel. Voorbeeld: gebroken arm/ brandwonden.	Ernstig en beperkt blijvend letsel. Voorbeeld: gecompliceerde breuk.	1 t/m 5 personen overleden en/of zwaargewond met blijvende ernstige beperkingen. Voorbeeld calamiteit met zwaargewonden: gemis van arm, been, gehoor, zicht.	Meer dan 5 personen overleden en/of zwaargewond met blijvende ernstige beperkingen. Voorbeeld: grootschalige calamiteit.
Impactvolle storingen op de infra (Verbindt en Verbetert)	Beschikbaarheid reizigers: Geen tot zeer gering effect. Beschikbaarheid Goederentrein: Geen tot zeer gering effect.	Beschikbaarheid reizigers: vertragingsminuten: 1 - 39. Voorbeelden: spoorlopers, koeltemperatuur, eenvoudige storing op rustiger baanvak. Beschikbaarheid Goederentrein: Vertraging goederentrein minder dan 30 minuten.	Beschikbaarheid reizigers: Vertragingsminuten 40 - 679. Voorbeelden: assen- of seinstoring op klein emplacement, overwegstoring, aanrijding persoon op rustiger baanvak. Beschikbaarheid Goederentrein: Vertraging goederentrein van 30 min. tot 3 uur.	Beschikbaarheid reizigers: Vertragingsminuten: 680 - 2399. Voorbeelden: aanrijding persoon op druk baanvak, brandmelding Schipholtunnel, wissel- of seinstoring op groot emplacement. Beschikbaarheid Goederentrein: Vertraging goederentrein tussen de 3 en 24 uur.	Beschikbaarheid reizigers: Vertragingsminuten: 2400 - 5999. Voorbeelden: (bijna) aanrijding wegverkeer met veel schade, extreem weer (storm, sneeuw, ijzel en/of bliksem). Beschikbaarheid Goederentrein: Vertraging goederentrein tussen 24 en 48 uur verspeeld.	Beschikbaarheid reizigers: Vertragingsminuten: > 6000. Voorbeelden: grote ICT-storing, stroomstoring. Beschikbaarheid Goederentrein: Vertraging goederentrein meer dan 48 uur verspeeld.
Compliance: wet- en regelgeving (Verbetert)	Geen afwijking / schending van wettelijke normen, 100% compliant.	Beperkte, kortdurende overschrijding van wettelijke normen.	Overtreding van wettelijke normen, bijv. aanschrijving van bevoegd gezag (bestuurlijke waarschuwing).	Overtreding van wettelijke normen, bijvoorbeeld bevoegd gezag kan een dwangsom of bestuursdwang opleggen.	Ernstige of langdurige overtreding van de wettelijke normen, bijvoorbeeld bestuurlijke strafvervolging kan worden ingesteld.	Zeer ernstige overtreding van de wettelijke normen, bijvoorbeeld aanleiding voor de minister om beheerconcessie te heroverwegen.
Duurzaamheid (Verduurzaamt)	Risico gebeurtenis heeft 0 tot 5% impact op de realisatie van de doelstellingen van duurzaamheid.	Risico gebeurtenis heeft 6% tot 20% impact op de realisatie van de doelstellingen van duurzaamheid.	Risico gebeurtenis heeft 21% tot 40% impact op de realisatie van de doelstellingen van duurzaamheid.	Risico gebeurtenis heeft 41% tot 60% impact op de realisatie van de doelstellingen van duurzaamheid.	Risico gebeurtenis heeft 61% tot 80% impact op de realisatie van de doelstellingen van duurzaamheid.	Risico gebeurtenis heeft > 81% impact op de realisatie van de doelstellingen van duurzaamheid.
Reputatie/ Stakeholders (bijv. overheden en vervoerders) (Verbetert)	Geen schade aan relatie met stakeholder zoals vervoerders en overheden. Geen negatieve aandacht in de (sociale) media.	Geringe schade aan relatie met vervoerders en/of overheden. Negatieve aandacht in de plaatselijke (sociale) media.	Beperkte schade aan relaties met vervoerders en/of overheden. Kortstondige negatieve aandacht in de regionale (sociale) media.	Aanzienlijke schade aan relaties en/of overheden. Middellange negatieve aandacht in de nationale (sociale) media.	Grote schade aan relatie met vervoerders en/of stakeholders. Langdurige negatieve aandacht in de nationale media, vermeldingen in internationale (sociale) media.	Zeer grote schade aan relatie met vervoerders en/of overheden. Zeer langdurige negatieve aandacht in de internationale (sociale) media. Bedreiging voor concessie.
Financiële schade, kosten a: ProRail-niveau b: Project- of afdelingsniveau (Betaalbaar Spoor)	a. Tot € 25.000,- b. 0% tot 5% van het budget.	a. Tussen de € 25.000,- en € 500.000,- b. 6% tot 20% van het budget.	a. Tussen de € 500.000,- en € 5 mln. b. 21% tot 40% van het budget.	a. Tussen de € 5 mln. en € 20 mln. b. 41% tot 60% van het budget.	a. Tussen de € 20 mln. en € 50 mln. b. 61% tot 80% van het budget.	a. Boven de € 50 mln. b. > 81% van het budget.

Toelichting risicoclassificatie		
(rood)	Zeer hoog	Beheersingsmaatregelen zijn nodig
(oranje)	Hoog	Beheersingsmaatregelen zijn nodig
(geel)	Gemiddeld	Beheersingsmaatregelen zijn nodig
(groen)	Laag	Geen aanvullende beheersingsmaatregelen zijn nodig

Indien een risico buiten het groene gedeelte van de risicomatrix gepositioneerd staat, dan zijn volgens de matrix aanvullende mitigerende maatregelen nodig. Echter de risico-eigenaar kan bepalen dat het risico toch geaccepteerd wordt en dus geen aanvullende maatregelen getroffen dienen te worden. Dit moet dan worden vastgelegd zodat dit zichtbaar en achteraf toetsbaar is.

De risicomatrix met de schalen voor kans en impact wordt vastgesteld door de RvB. Indien afgeweken wordt van de risicomatrix, dient dit eerst overlegd te worden met de afdeling IRC.

De risicomatrix moet worden gebruikt door iedereen binnen ProRail die zich bezighoudt met het beoordelen van risico's op kans en impact. Voor een toelichting op het gebruik van de risicomatrix zie bijlage 3.

5 Risicomanagementproces

5.1 Vaststellen van de context

Het begin van het risicomanagementproces valt samen met de start van het planningsproces (Planning & Control-cyclus) en is daarmee onderdeel van de PDCA cyclus. De start bestaat uit het beoordelen of doelstellingen zijn veranderd, vervallen of erbij zijn gekomen. Vervolgens dient onderzocht te worden de context waarbinnen prestaties zullen worden geleverd met de daaraan verbonden kosten. Zowel de interne als de externe context wordt onderzocht en beschreven. De externe context bestaat respectievelijk uit ontwikkelingen en trends op gebied van politiek, economie, technologie en milieu. Het bestuur, de rollen en verantwoordelijkheden, de doelstellingen van de organisatie en de afdeling, de risicohouding, de middelen en kennis, de cultuur van de organisatie, de besluitvormingsprocessen en informatiesystemen, de normen, modellen en richtlijnen en de vorm en reikwijdte van contractuele verplichtingen vormen een (niet limitatief) overzicht van de interne omgeving.

5.2 Risico-identificatie

De risico-identificatie start altijd bij de doelstellingen. Zijn de doelstellingen ‘vaag’ geformuleerd, dan kunnen risico’s ook niet duidelijk worden vastgesteld. De risico-identificatie zelf wordt onder verantwoordelijkheid van de risico-eigenaar uitgevoerd. De risico-eigenaar is ‘*accountable*’ voor het risico en bepaalt daarmee welke mitigerende maatregelen getroffen moeten worden (hierbij rekening houden met de risicobereidheid). Degene die de acties daadwerkelijk uitvoert, is de taakhouder. Voor het identificeren van risico’s maakt ProRail gebruik van informatie uit o.a. databases, interviews en andere technieken. Doel van de risico-identificatie is om een overzicht van risico’s te genereren op basis van gebeurtenissen die het behalen van doelstellingen kunnen belemmeren of vertragen.

5.3 Risicoanalyse

De risicoanalyse heeft tot doel om inzicht in het risico te verkrijgen. Risicoanalyses worden gebruikt bij het kiezen van behandelmethodes en besluitvorming. Een risicoanalyse start met het inschatten van de kans dat het risico in een periode kan optreden, en de impact dat het risico per gebeurtenis kan hebben. Hierbij wordt gebruik gemaakt van de ProRail risicomatrix. Bij de analyse van de risico’s wordt de bestaande risicobehandeling (treffen van mitigerende maatregelen) meegenomen.
De risico-eigenaar beoordeelt periodiek op basis van expert judgement welke maatregelen goed werken en welke maatregelen verbetering behoeven en/of dat aanvullende maatregelen nodig zijn omdat deze er nog niet zijn, of onvoldoende werken. De risico-eigenaar bepaalt daarmee op basis van de risicobereidheid het feitelijke restrisico dat nog overblijft nadat maatregelen zijn getroffen. Indien dit niet acceptabel is, dienen verdere aanvullende maatregelen getroffen te worden en hier te worden beschreven.
Een risicoanalyse kan op verschillende manieren plaatsvinden, zoals bijvoorbeeld met de BowTie-methode. Afdelingen zijn vrij in het bepalen van de methode zolang maar wel aan de basisprincipes, zoals gesteld in dit beleid, wordt voldaan.

5.4 Risico-evaluatie

Bij een risico-evaluatie worden gezamenlijk alle mogelijke risico’s in kaart gebracht, voorzien van kans en impact, mitigerende maatregelen, taakhouder en deadline. Bij de evaluatie moet tevens het volgende worden aangegeven:

- per maatregel aangeven of de maatregel naar behoren werkt en/of in hoeverre de maatregel al volledig is geïmplementeerd;
- of aanvullende maatregelen nodig zijn om het risico te mitigeren;
- of het risico (indien buiten het groene gedeelte) moet worden geaccepteerd omdat het niet mogelijk (of te kostbaar) is om aanvullende maatregelen te nemen;
- aangeven of de positie van het restrisico zich verplaatst op de matrix. Hierop moet een toelichting gegeven worden en worden vastgelegd in het dashboard.

5.5 Monitoring en beoordeling

Monitoren en beoordelen van de restrisico’s en de (doelmatigheid en doeltreffendheid) van de risicobehandeling vindt 1 keer per kwartaal plaats op afdelingsniveau, bedrijfsonderdeel en organisatieniveau.

6 Vastleggen risico's in systemen

Risico's moeten worden vastgelegd om zeker te stellen dat ze gevolgd kunnen worden.

6.1 Inhoud vastlegging

Van belang is dat alleen risico's worden vastgelegd die een onzekere gebeurtenis of situatie zijn die mogelijk in de toekomst plaatsvindt. Dit betekent dat issues of problemen die al manifest zijn, niet worden opgenomen als risico tenzij ze zelf weer risico's veroorzaken. Verder moeten risico's een directe relatie hebben met een doelstelling van ProRail. Het zijn de risico's die de realisatie van de doelstellingen van ProRail bedreigen.

De risicobeschrijving bestaat altijd uit de volgende onderdelen:

- Risico (gebeurtenis);
- Oorzaak waardoor het risico kan optreden;
- Gevolg als het risico optreedt.

Voor het beschrijven van risico's, moet de volgende format gebruikt worden:

Het risico dat …….... doordat / veroorzaakt door …… met als gevolg ……..

Bijvoorbeeld: Het risico dat computersystemen van ProRail gehackt worden doordat toegang tot systemen niet goed beveiligd is met als gevolg dat treinen uitvallen.

6.2 Maatregelen

Mitigerende maatregelen moeten worden beschreven die het risico mitigeert tot het beoogde restrisico. Beoogde restrisico wordt bepaald aan de hand van de risicobereidheid.

Bij de maatregelen wordt het volgende opgenomen:

- beschrijving van de belangrijkste maatregelen die de gebeurtenis kunnen voorkomen door oorzaken weg te nemen of de impact te verkleinen waardoor het risico wordt gemitigeerd;
- per maatregel moet worden aangegeven of de maatregel al naar behoren werkt, afgerond of gereed is en wat de implementatiedatum is indien deze nog niet gereed is.

Wanneer de beoordeling van de beheersing van risico's leidt tot tegenstrijdige belangen en/of kwesties met betrekking tot de toewijzing van bedrijfsmiddelen wordt er binnen de organisatie geëscaleerd.

6.3 Taakhouder

Voor iedere maatregel (actie) moet worden vastgelegd wie verantwoordelijk is voor het uitvoeren ervan. Dit is de taakhouder. De risico-eigenaar bepaalt welke maatregelen getroffen moeten worden om het risico te beheersen. Eigenaar van het risico hoeft niet te betekenen dat hij / zij ook verantwoordelijk is voor implementeren van de maatregel zelf (taakhouder). Het is mogelijk dat de taakhouder in een andere afdeling zit omdat onderliggende processen over meerdere afdelingen kunnen lopen (integraliteit van risicomanagement). Het is de verantwoordelijkheid van de risico-eigenaar om erop toe te zien dat de taakhouder (tijdig) de maatregel (actie) opvolgt.

6.4 Deadline

De risico-eigenaar bepaalt samen met de taakhouder wat de uiterlijke datum (deadline) is wanneer de maatregel of actie gereed moet zijn of dat een tijdelijke maatregel opgeheven moet zijn. De risico-eigenaar en de taakhouder zien erop toe dat dit tijdig gebeurt. Van maatregelen die pas over een aantal jaren gereed zijn dient te worden aangegeven wat de tussentijdse voortgang is op deze maatregel. Indien verder dan een jaar, dan dienen tussenliggende (kwartaal) mijlpalen als actie met datum ingevuld te worden. Er dient altijd een concrete datum (jaar) te worden ingevuld. Indien geen datum staat ingevuld, wordt ervan uitgegaan dat de actie / maatregel per eind van het volgende kwartaal gereed is.

7 Rapportage van de risico's

Onderscheid wordt gemaakt tussen het rapporteren van de corporate, tactische en operationele risico's.

7.1.1 Opstellen van corporate risico dashboard

IRC stelt op basis van de vastgestelde 16 risicogebieden een corporatie risicodashboard samen. Dit dashboard geeft inzicht in de belangrijkste risico's van de hele ProRail organisatie. Dit corporate risico dashboard heeft als doel om inzicht te geven in en sturing aan de belangrijkste risico's voor het behalen van de bedrijfsdoelstellingen.

7.1.2 Rapportage van de corporate risicodashboard

Per risicogebied wordt op basis van de input van de risico-eigenaar elk kwartaal een dashboard opgesteld en gerapporteerd. Dit dashboard bevat de belangrijkste risico's, beheersmaatregelen en planning hiervan.

Deze dashboards worden geagendeerd voor de prestatiedialoog tussen RvB en risico-eigenaar en biedt daarmee de mogelijkheid om te sturen op de risico's. De dashboards worden naar aanleiding van dit gesprek aangepast en vervolgens worden de belangrijkste risico's daaruit opgenomen in een managementrapportage die wordt gezonden naar de ExCo. In de ExCo vindt een risico assessment sessie plaats op basis waarvan de managementrapportage wordt aangepast. Vervolgens wordt deze vastgesteld door de RvB en ter informatie gezonden naar de Audit Commissie en de RvC.

De kwartaalrapportage risicomanagement geeft inzicht in:

1. de positie van het risico in de risicomatrix. Dit geeft daarmee de ernst van het risico weer. Bij de inschatting van het risico wordt gebruik gemaakt van de ProRail risicomatrix. Hierin is af te lezen (op de verticale as) welke kans van optreden bij het risico hoort en wat de impact (op de horizontale as) is per gebeurtenis. Voor meer details wordt verwezen naar bijlage 3 waar het gebruik van de risicomatrix in meer detail wordt uitgelegd;
2. de aanvullende beheersmaatregelen voor alle risico's buiten het groene deel op basis van de inschatting van een risico en de adequaatheid van de maatregelen door de risico-eigenaar;
3. de belangrijkste mitigerende maatregelen per risico;
4. de status van de maatregel en hierbij terugkijken naar vorige kwartaal (zie onder 8). Achter iedere maatregel wordt de status vermeld. Bij de maatregelen die nog niet gereed zijn wordt een stapsgewijze aanpak gehanteerd: formuleer een maatregel (actie) en een deadline en kom daarna met een vervolgactie en een volgende deadline;
5. de werking van de maatregel. Per geïmplementeerde maatregel wordt vermeld wat de werking hiervan is: werkt de maatregel naar behoren of niet. Indien niet, dan dient dit te worden toegelicht in de management reactie;
6. eventuele voorstellen voor aanvullende maatregelen. Dit dient te worden toegelicht in de management reactie;
7. de richting waarin een risico in de matrix zich ontwikkelt ten opzichte van het vorige kwartaal en wat de prognose is voor de toekomst;
8. bij de maatregelen moet als eerste worden weergegeven welke maatregelen het komende kwartaal getroffen worden.

7.2 Opstellen rapportage op tactisch en uitvoerend niveau

Afdelingen zoals asset management, capaciteitsmanagement en veiligheid hebben een rapportagesysteem met risico's van de business. Management bepaalt zelf de manier en frequentie van rapporteren op tactisch niveau (MT-niveau) en uitvoerend niveau. Vervolgens kunnen de afdelingen de belangrijkste risico's overnemen in het dashboard van het ProRailbrede risicosysteem. Het is van belang dat het dashboard wordt gebruikt in de rapportage van de prestatiedialoog, alsook in discussies over prestaties en risico's, zoals bij de ExCo.

Bijlage 1: Risicogebieden

Bijlage 2: Risicomanagement Dashboard - voorbeeld

16) Compliance & Integriteit * — * Integriteit heeft raakvlakken met risicogebied 1, Cultuur & Organisatie — **Risico-eigenaar: Diederick Slijkerman (1/2)**

Doelstellingen

- A. Het professionaliseren van compliance binnen ProRail. Het bevorderen en verbeteren van integriteit, compliance en privacy binnen ProRail
- B. Verbeteren op het compliance-volwassenheidsniveau (van 3 naar 4) zoals aangegeven in het ACM cultuuronderzoek
- C. Verkrijgen van overzicht van wet- en regelgeving en gebruik daarvan in de spoorse wereld
- D. Vergroten van bewustzijn en begrip omtrent compliance en integriteit in de spoorse wereld

Legenda prognose

- ↑ = Risico wordt groter
- ↓ = Risico wordt kleiner
- = = Risico blijft gelijk
- ? = Ontwikkeling risico onzeker

Belangrijkste risico's	Mitigerende maatregelen	Taakhouder	Deadline	Q3 2022	Q4 2022	Prog
1. Het risico dat door stikstofdepositie projecten vertraging oplopen en dat dieselactiviteiten op emplacementen wordt stilgelegd. (Doelstelling A en C) Oorzaken: (1) Sommige emplacementen beschikken niet over een vergunning in het kader van de Wnb en deze wordt minder afgegeven door strengere wetgeving; (2) Gebruikelijke instrumenten zoals ecologische onderbouwing zijn nauwelijks toepasbaar; (3) Geen geld voor extra maatregelen. Gevolgen: Stilleggen van dieselactiviteiten op emplacementen zal leiden tot ontwrichting van de dienstregeling en hogere kosten.	Opstellen per project van ecologische onderbouwingen nabij Natura 2000-gebieden. Strategie, communicatie en escalatiemodel opstellen. Wetgevingsbeïnvloeding, overleg LNV-I&W. Impactanalyse van vernietiging bouwvrijstelling door Raad van State wordt opgesteld; komende uitspraak Raad van State VIA15 wordt afgewacht. Overzicht opstellen van toekomstige projecten waarbij mogelijk geen vergunning verkregen kan worden. Verduurzaming bouwplaats en bouwlogistiek: aanbesteding PGA-contracten waarvan inzetten van elektrisch materieel op locaties nabij Natura 2000-gebieden onderdeel is.		Ongoing Gereed Ongoing Update feb-23 Gereed Incidenteel	[illegible]	[illegible]	=
2. Het risico op niet voldoen aan wet- en regelgeving op het gebied van natuur, milieu en omgevingsveiligheid. (Doelstelling A) Oorzaken: niet voldoende en tijdig contractering en handhaving, onvoldoende borgen van know-how, en het niet voldoende oppakken van de regierol. Gevolgen: infra en veiligheid zijn niet op orde; goederentreinen vallen uit; problemen voor besturing en bijsturing; betrouwbaarheid en reputatie zijn in het geding; boetes en andere sancties kunnen worden opgelegd. Bij niet tijdig contractering willen de aannemers gecompenseerd worden of dienen claims in.	[illegible]		Q2-23 1-07-23 Ongoing 1-07-23 Gereed Ongoing ASAP ASAP Q2-23	7	7	=
3. Het risico dat ProRail een tekort heeft aan ballast omdat voorgeschreven wordt vanuit SZW om enkel kwartsloze ballast te gebruiken. Oorzaken: niet tijdig voldoende kwartsloze ballast beschikbaar hebben. Er zijn nog geen groeves gecertificeerd op basis van de nieuwste productspecificatie SPC00383. Gevolgen: het niet uit kunnen voeren van projecten waar ProRail dit type spoorwegballast wil toepassen.	[illegible]		Update bij uitspraak Gereed 2024 Q4 2023		[illegible]	=
4. Het risico dat personeel (eigen en inhuur) zich niet houdt aan wet- en regelgeving en ProRail regels en -procedures. (Doelstelling A, B, C en D) Oorzaken: medewerkers zijn onbekend met deze regels en procedures. Gevolgen: fouten, boetes en imagoschade.	Programma onboarding nieuwe medewerkers. Pre-employment screening. E-learning Gedragscode en Dilemmaworkshops over o.a. belangenverstrengeling. Spel over omgaan met informatie, van cyber security tot sociale veiligheid. Herziening van de Gedragscode waaronder Regeling en proces nevenwerkzaamheden. Regelmatig publiceren van gedragsthema's op focus, zoals terugkoppeling over vragen en meldingen over de Gedragscode.		Q3-23 Ongoing Ongoing 2022-23 Q4-22 Q4-23	6	6	= ↑

16) Compliance & Integriteit * — **Risico-eigenaar: Diederick Slijkerman (2/2)**

Belangrijkste risico-indicatoren	Norm KRI	Status KRI	Belangrijkste risico-indicatoren	Norm KRI	Status KRI
1. Compliance-volwassenheidsniveau zoals aangegeven in het ACM cultuuronderzoek *(ACM heeft informeel aan ProRail aangegeven dat we van trede 3 naar trede 4 zijn gestegen. Dit wordt nog officieel gecommuniceerd.)*	3	4	3. Aantal meldingen lekken persoonsgegevens aan Autoriteit Persoonsgegevens		
2. Aantal gevallen overtreding aanbestedingsregels. Dit heeft voorspellende waarde voor de kans dat mededingingswet wordt overtreden en ACM optreedt			4. Tijdige implementatie van en compliant zijn aan Wet- en regelgeving		

Toelichting op de belangrijkste risico's en de prognoses

Toelichting K. te Boome: Risico 1: Voor de taskforce stikstof is een strategie, een handelingskader en ook een interne website opgesteld.
Risico 2:

- Met name voor milieu-compliance wordt nu door Programma Ketenversterking Natuur en Milieu gewerkt aan structurele verbeteringen. Programma is afgerond en opgeleverd aan de lijn - LCM (Landelijk Committee Milieu). Vanwege capaciteitstekort bij AM worden LOD's onvoldoende opgelost. Daarnaast is er geen tijd om te werken aan het nieuwe milieusysteem.
- Er wordt gewerkt aan het op orde krijgen van de infra op de Rotterdamse havenemplacementen.
- De activiteiten worden door het Bevoegd Gezag bekeken door een vergrootglas.
- Er wordt vooruitgang geboekt, het aantal LOD's neemt voorzichtig af. We hebben derden niet aan een lijntje en kunnen slechts indirect invloed uitoefenen, maar het IPT spant zich daar maximaal in. Waar veel gewerkt wordt, gaat gemakkelijk iets fout, bijv. door de haast of onbekendheid met het terrein.

Dit alles in ogenschouw nemend durf ik de stelling aan dat er wel degelijk forse verbeteringen plaatsvinden, al zijn we er nog lang niet. Maar ook daar is het IPT zich van bewust.
Daarnaast staat IPT niet op zichzelf en bestaat mede uit mensen vanuit de organisatie, zodat er op hoofdlijnen aansluiting is met de verschillende afdelingen.
Daarbij dienen we ons bewust te zijn van het feit, dat ook elders het bevoegd gezag "strenger" kan gaan worden en daar soortgelijke issues kunnen optreden.

Toelichting R. Warnar Risico 2: Zorgen zijn geuit omtrent het opzetten van de staande organisatie. Om dit te doorgronden wordt in Q1'23 een Governance onderzoek gestart door Corporate Audit.

Prognoses:
Risico 1: Het risico blijft ongewijzigd vanwege de impact van de uitspraak Raad van State en komende uitspraak over VIA15. Op dit moment worden er geen vergunningen gegeven.
Risico 2: Gelet de verwachte impact van de huidige LOD's kan dit risico op termijn groter worden. Dit is inmiddels onder de aandacht van de desbetreffende BE's/afdelingen en de RvB. Zorgen zijn geuit omtrent de overgang naar de staande organisatie. Om dit te doorgronden wordt in Q1'23 een onderzoek gestart door Corporate Audit.
Risico 3: Het is nog onvoldoende duidelijk hoe de inbedding van IPT in de organisatie wordt gerealiseerd. De vraag is in hoeverre er bij IPT rekening wordt gehouden met bestaande normen, betaalbare oplossingen en integratie in bestaande systemen en processen. Hierdoor gaat het risico omhoog. Dit is inmiddels onder de aandacht van de desbetreffende BE's/afdelingen en de RvB. IRC adviseert om hier een audit op te laten uitvoeren door Corporate Audit.

Impactcategorie risicomatrix:
Risico 1: Score kans = regelmatig (5): 10 x per jaar tot maandelijks. Score impact =groot (5). Score is 8, rood.
Relevante Impactcategorie "Prestatie railinfrastructuur en beschikbaarheid" = het risico kan impact hebben op trein en goederenverkeer, namelijk > 100 treinen die uitvallen of gelijkwaardig.
Risico 2: Score kans = regelmatig (5): 10 x per jaar tot maandelijks. Score impact =aanzienlijk (4). Score is 7, oranje.
Relevante Impactcategorie "Compliance (wet- en regelgeving)" = overtreding van de wettelijke (milieu/gedrags) normen. Bevoegd gezag legt dwangsom of bestuursdwang op.
Risico 3: Score kans = zeer regelmatig (6): meer dan 100 keer per jaar of dagelijks. Score impact =groot (5). Score is 9, rood.
Relevante Impactcategorie "Prestatie railinfrastructuur en beschikbaarheid" = het risico kan impact hebben op trein en goederenverkeer, namelijk > 100 treinen die uitvallen of gelijkwaardig.

Bijlage 3: Toelichting gebruik van de ProRail risicomatrix

Toepassingsgebied

De risicomatrix moet worden gebruikt voor alle risico's die de realisatie van de ProRail doelstellingen bedreigen. Dit betreft zowel strategische als de operationele doelstellingen. Indien je van mening bent dat de risicomatrix niet van toepassing zou zijn, neem dan contact op met de afdeling IRC. Tevens dient contact opgenomen te worden met IRC in geval van voorstellen tot wijziging van de parameters en/of indien men een andere versie van de matrix wil gebruiken. De risicomatrix is niet geschikt voor extern gebruik.

Beschrijving van de matrix

De risicomatrix bestaat uit de y-as en de x-as. De y-as toont de kansverdeling van het optreden van de risicogebeurtenis op een schaal van 1 t/m 6. De x-as toont de verdeling van het gevolg (impact) voor als de risicogebeurtenis optreedt op een schaal van 1 t/m 6. De impactscore geeft de impact weer per gebeurtenis. Als de kans 10 keer per jaar is met een impact van 50 per gebeurtenis, dan moet bij de impactschaal gezocht worden naar 50 en niet naar 500 (10 x 50). De risico-eigenaar bepaalt op basis van welke methode het risico wordt ingeschat. Indien historische gegevens beschikbaar zijn, dan wordt het risico onder andere daarop gebaseerd. Ook is mogelijk om het risico in te schatten op basis van expert judgement.

De y-as meetpunten (kans) zijn:

1. Zeer onwaarschijnlijk, minder dan 1x in 100 jaar
2. Onwaarschijnlijk,1x in 100 jaar tot 1x in 10 jaar (1/100- 1/10)
3. Incidenteel, 1x in 10 jaar tot 1x per jaar (1/10- 1)
4. Waarschijnlijk, 1x per jaar tot 10x per jaar (1-10)
5. Regelmatig, 10x per jaar of maandelijks tot 100x per jaar of dagelijks (10-100)
6. Zeer regelmatig, meer dan 100 keer per jaar of dagelijks (100+)

De x-as meetpunten (impact) zijn:

1. Geen tot zeer gering (A)
2. Gering (B)
3. Beperkt (C)
4. Aanzienlijk (D)
5. Groot (E)
6. Zeer groot (F)

De gevolgen op de x-as zijn onderverdeeld in zogenaamde impactcategorieën. Deze staan in de matrix als volgt weergegeven:

- **Fysieke veiligheid**: de mate waarin de activiteiten / bedrijfsvoering van ProRail veilig zijn voor mensen onder wie reizigers, baanwerkers en bedienend personeel. Dit betreft ook ARBO-veiligheid en systeemveiligheid;
- **Impactvolle storingen op de infra**: de mate, waarin storingen impact hebben op de infra;
- **Compliance: wet- en regelgeving**: de mate, waarin ProRail zich houdt aan vigerende wet- en regelgeving;
- **Duurzaamheid**: de mate, waarin ProRail haar bedrijfsactiviteiten duurzaam uitvoert;
- **Reputatie / Stakeholders (bijvoorbeeld overheden en vervoerders)**: de mate waarin ProRail waarde hecht aan haar positie in de maatschappij / bij de stakeholders;
- **Financiële schade / kosten**: de mate waarin ProRail efficiënt omgaat met haar financiële middelen.

De risico-eigenaar kiest op welke bedrijfswaarde het risico de meeste impact heeft. Het is mogelijk dat het risico impact heeft op meerdere impactcategorieën. De bedrijfswaarde waar het hoogst op gescoord wordt, bepaalt de positie op de impactschaal. De impact neemt van links naar rechts in ernst toe.

Invullen van de matrix

De risico-eigenaar houdt bij de inschatting van het risico rekening met de maatregelen en de status hiervan. Bij het invullen dienen de volgende stappen genomen te worden:

- Maak een inschatting van de kans van optreden van het risico;
- Maak een inschatting van de impact indien het risico optreedt;
- Bepaal op basis van de kans en impact wat de positie is op de matrix. Ieder vak heeft een nummer en een kleur en een risicoclassificatie Laag, gemiddeld, hoog en zeer hoog;
- De risicoclassificatie bepaalt of actie genomen dient te worden volgens onderstaand schema.

Kleur	Toelichting risicoclassificatie
	Beheersingsmaatregelen zijn nodig
	Beheersingsmaatregelen zijn nodig
	Beheersingsmaatregelen zijn nodig
	Geen aanvullende beheersingsmaatregelen zijn nodig

Verantwoordelijkheid

IRC is verantwoordelijk voor het beheer van de risicomatrix. Vragen en/of opmerkingen kunnen geadresseerd worden aan de afdeling IRC.

Begrippenlijst

Hieronder volgt een overzicht van de belangrijkste termen die gehanteerd worden voor risicomanagement binnen ProRail.

Risicomanagement
Gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's.

Risicomanagement beleid
Verklaring van de algemene bedoelingen en richting van een organisatie met betrekking tot risicomanagement.

Risicomanagementproces
Systematische toepassing van beleidslijnen, procedures en werkwijzen op de activiteiten met betrekking tot de communicatie, overleg, vaststelling van de context, en het identificeren, analyseren, evalueren, behandelen, monitoren en beoordelen van risico's.

Risico(gebeurtenis)
Een onzekere gebeurtenis of situatie in de toekomst die de realisatie van de doelstellingen bedreigen. Risico's zijn conform de COSO-ERM methodiek als volgt onderverdeeld:

- **Strategische risico's**: "Doen we de juiste dingen". Hier is besluitvorming nodig door de RvB. Strategische risico's zijn risico's die direct de strategische doelstelling van de organisatie in gevaar kunnen brengen;
- **Operationele risico's**: "Doen we de dingen op de juiste manier". Operationeel risico betreft het risico dat ontstaat als gevolg van het falen of tekortschieten van interne processen, menselijke en technische tekortkomingen, en onverwachte externe gebeurtenissen;
- **Financiële risico's**: Dit betreft risico's betreffende activiteiten en beslissingen m.b.t. de effectieve beheersing van de financiën;
- **Compliance risico's**: Risico's ontstaan door het niet voldoen aan wet- en regelgeving.

ProRailbrede risico's
Dit betreft de risico's voor ProRail op corporate of strategisch niveau (voormalige toprisico's). Daarnaast heb je risico's op management of tactisch niveau (MT van afdeling) en uitvoerend niveau (operationele risico's).

Risicogebied
De dashboards waarin de belangrijkste risico's beschreven staan, zijn verdeeld over risicogebieden. De risicogebieden zijn afgeleid van de strategische doelstellingen van ProRail. Hierbinnen zijn sub-risico's bepaald die de realisatie van de doelstellingen kunnen bedreigen.

Risicobeoordeling
Gehele proces van risico-identificatie, risicoanalyse en risico-evaluatie.

Mitigerende maatregelen
Mitigerende maatregelen zijn maatregelen die op basis van de risicobereidheid worden gedefinieerd om het risico te mitigeren. De maatregelen kunnen betrekking hebben op de kans van optreden en/of op de impact van het risico.

Restrisico
Restrisico is het risico waarbij rekening wordt gehouden met de maatregelen. De risico-eigenaar bepaalt welk restrisico nog aanwezig is en of dit acceptabel is.

Risicomatrix
De risicomatrix dient als maatstaf voor het meten van risico's. Het meten gebeurt door te bepalen hoe groot de kans van optreden is van het risico en hoe groot het gevolg is bij optreden van het risico. De grootte wordt bepaald door de kans te vermenigvuldigen met het gevolg.

Risico-eigenaar
Persoon die eindverantwoordelijk is om het risico te managen De risico-eigenaar is '*accountable*' voor het risico en bepaalt daarmee welke maatregelen getroffen moeten worden. Degene die de acties daadwerkelijk uitvoert is de 'responsible person' en daarmee degene die verantwoordelijk is voor het uitvoeren van de maatregel (zie hierna).

Taakhouder
De taakhouder is verantwoordelijk voor het correct uitvoeren van de maatregelen die nodig zijn om het risico te beheersen en of te mitigeren.

Oorzaak (van een risico(gebeurtenis)
Gebeurtenis of situatie waardoor een risico optreedt.

Gevolg van een risico(gebeurtenis)
Uitkomst van een (risico)gebeurtenis waardoor doelstellingen worden beïnvloed.

Waarschijnlijkheid
Kans dat iets gebeurt.

Risicoanalyse
Proces dat tot doel heeft de aard van het risico te analyseren en het risiconiveau vast te stellen.

Risicocriteria
Referentiekader aan de hand waarvan de belangrijkheid van een risico wordt beoordeeld.

Risico-evaluatie
Proces waarin de resultaten van een risicoanalyse worden vergeleken met de risicocriteria om vast te stellen of het risico en/of de omvang ervan aanvaardbaar of tolereerbaar is.

Monitoring
Voortdurend controleren van, toezicht houden op, kritisch waarnemen of vaststellen van een toestand om eventuele wijzigingen ten opzichte van het vereiste of verwachte prestatieniveau te identificeren.

Beoordeling (review)
Activiteit die wordt ondernomen om de geschiktheid, toereikendheid en doeltreffendheid van het desbetreffende onderwerp voor het behalen van vastgestelde doelstellingen te bepalen.

Expert judgement
Risico's worden beoordeeld op basis van expert judgement. Dit betekent dat het oordeel door een deskundige gebaseerd wordt op kennis, vaardigheid, ervaring en of gespecialiseerde kennis binnen een specifiek gebied (risico).