Het nemen van samenhangende mitigeren maatregelen

1. Inleiding

Implementatie van het VIRBI 2025 omvat het beheersen van risico's ten aanzien van de exclusiviteitseisen voor de verwerking van gerubriceerde informatie. Dit gebeurt door het treffen van een beheerst en risicogestuurd stelsel van passende, integrale beveiligingsmaatregelen. Deze maatregelen reduceren de onderkende risico's tot aanvaardbare proporties en doen recht aan de geldende compliance-eisen.

2. Plan opstellen

Om effectief mitigerende maatregelen te nemen, is het belangrijk om niet alleen losse acties te beschrijven, maar ook de samenhang, prioriteit, verantwoordelijkheid en borging. Dit voorliggende document helpt om een compact maar volledig plan op te stellen waarmee je aantoonbaar "in control" bent en kan voldoen aan het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie, het VIRBI 2025.

Maak een bondig plan en neem de volgende zaken op:

2.1. Doel en scope bepalen

Beschrijf kort:

- Wat je wilt beschermen;
- Aan welke eisen of normen je wilt voldoen;
- Welke organisatieonderdelen, processen, systemen of informatie binnen scope vallen.

Enkele voorbeelden:

- Implementatie VIRBI 2025;
- Bescherming van gerubriceerde informatie;
- Voldoen aan het VIRBI 2025.

2.2. Governance organiseren

In het gereedschap governance is een voorbeeld RASCI-tabel opgenomen die je op je eigen organisatie kan aanpassen. Voor het nemen van maatregelen gaat het erom dat alle deelnemers weten wat je van elkaar kan verwachten en wie welke rol heeft zodat je elkaar daarop effectief kan aanspreken.

Goed ingeregelde governance is een essentieel onderdeel van het organiseren van adequate beveiligingsmaatregelen.

We geven hieronder een overzichtstabel wat je minimaal moet organiseren voor het nemen van maatregelen:

Onderdeel:	Wat organiseer je:
Opdrachtgever	Bestuurlijke eigenaar
Stuurgroep	Besluitvorming en prioritering
Projectleider/coördinator	Dagelijkse aansturing
CISO/BVA	Inhoudelijke beveiligingskaders
Eigenaren van maatregelen	Uitvoering van maatregelen
Three lines of defense	Beheer, controle en audit
Rapportagestructuur	Periodieke voortgang en escalatie

Deze governance moet duidelijk maken:

- wie maatregelen uitvoert;
- wie controleert;
- wie accepteert dat restrisico's blijven bestaan.

2.3. Mitigerende maatregelen in samenhang bepalen

Maak een overzicht van alle te nemen maatregelen en deel deze in categorieën. Organiseer maatregelen per categorie zodat ze elkaar versterken. Betrek daarbij ook vooral een security architect.

Hieronder geven we in een tabel enkele voorbeelden van samenhangende maatregelen:

Categorie	Voorbeelden
Organisatie	Governance, rollen, beleid
Mens	Awareness, opleiding, gedrag
Proces	Procedures, controles, logging
Techniek	MFA, encryptie, segmentatie
Fysiek	Toegangsbeveiliging
Juridisch	Contracten, afspraken
Monitoring	Audits, KPI's, dashboards

Het is belangrijk om een aantal aspecten in acht te nemen:

- voorkom losse maatregelen zonder onderlinge afstemming;
- koppel maatregelen aan risico's;
- beschrijf afhankelijkheden.

2.4. Plannen & prioriteren

Niet alles kan tegelijk dus maak een planning en prioriteer.

Voor de bepaling van prioriteiten kijk je naar meerdere aspecten zoals:

- risico en impact;
- wettelijke verplichtingen;

- haalbaarheid;
- beschikbare capaciteit;
- afhankelijkheden.

Voor je planning werk je met:

- korte termijn;
- middellange termijn;
- lange termijn.

2.5. Roadmap

Maak van de planning een compacte roadmap. Als voorbeeld geven we onderstaand overzicht:

Activiteit	**Eigenaar**	**Prioriteit**	**Deadline**
Vaststellen beveiligingsbeleid	BVA	Hoog	Q2
Awareness campagne	HR/CISO	Midden	Q3
Workshops rubriceren	BVA	Hoog	Q3
Technische maatregelen (hoog)	IB/IT	Hoog	Q3
Technische maatregelen (midden)	IB/IT	Midden	Q4

Een roadmap is een goed middel om te rapporteren en te gebruiken om samen het gesprek aan te gaan.

2.6. Middelen en capaciteit organiseren

Om maatregelingen te kunnen nemen zijn middelen en is capaciteit nodig. Beschrijf in je plan de volgende zaken:

- benodigde expertise;
- budget;
- capaciteit;
- tooling;
- externe ondersteuning.

Zonder middelen en capaciteit blijft een plan alleen papier.

2.7. Monitoring en PDCA organiseren

Het eenmalig uitvoeren van maatregelen is niet genoeg. Werk aan het borgen van continue verbetering. Dat kan je doen door de volgende zaken te organiseren:

- KPI's;
- periodieke controles;
- managementrapportages;
- audits;
- lessons learned;
- actualisatie van risico's.

Gebruik de PDCA-cyclus:

1. Plan
2. Do
3. Check
4. Act

2.8. Restrisico's en besluitvorming vastleggen

Niet alle risico's verdwijnen. Het kan zijn dat er restrisico's overblijven als je maatregelen hebt getroffen. Leg daarom vast:

- welke restrisico's overblijven;
- wie deze accepteert;
- welke maatregelen later volgen;
- welke uitzonderingen bestaan.

2.9. Compacte structuur voor een kort plan

Een praktisch kort plan kan bestaan uit:

1. Doel en scope
2. Governance en verantwoordelijkheden
3. Uitkomst risicoanalyse en TBB-analyses
4. Overzicht mitigerende maatregelen in samenhang, incl. security architectuur
5. Planning en prioriteiten
6. Monitoring en borging
7. Restrisico's en besluitvorming

Dat is meestal voldoende voor bestuurlijke besluitvorming én operationele uitvoering.

3. Colofon:

Wil je reageren? Dat kan naar het volgende e-mailadres: CISORijk@minbzk.nl.

Dit gereedschap is tot stand gekomen met een brede werkgroep en maakt deel uit van de gereedschapskist ter ondersteuning van implementatie van het VIRBI 2025.

De BVA Rijk en de CISO Rijk zijn sponsoren van deze gereedschapskist.

11-5-2026