Van start met Implementatie VIRBI 2025

1. Inleiding

Om van start te gaan met de implementatie van het VIRBI 2025 is het handig om een kort en bondig plan van aanpak op te stellen. Dit voorliggende document helpt om een compact maar volledig plan van aanpak op te stellen. De structuur is gebaseerd op de overzichtsplaat “Implementatie VIRBI 2025 – Helicopterview”.

Dit document maakt deel uit van de gereedschapskist Implementatie VIRBI 2025. Het is een hulpmiddel en geen verplicht kader.

2. Doorloop de volgende stappen

In dit hoofdstuk doorlopen we de stappen om te komen tot een kort en bondig plan van aanpak met relevante onderwerpen. De zeven inhoudelijke stappen (paragraaf 2.1 t/m 2.7) zie je ook terug in de overzichtsplaat. Daarnaast geven we een samenvatting (paragraaf 2.8) en noemen we belangrijke uitgangspunten (paragraaf 2.9).

2.1. Bepaal doel, scope en aanpak

Allereerst is het belangrijk doel, scope en aanpak te bepalen.

2.1.1. Wat organiseer daarvoor:

- Doelstelling van de implementatie.
- Scope van systemen, processen en organisatieonderdelen.
- Afbakening van gerubriceerde informatie.
- Projectstructuur en globale planning.
- Stuurgroep en opdrachtgeverschap.
- Vaststellen van beleid en uitgangspunten.

2.1.2. Wat is het resultaat:

- Duidelijk implementatieaanpak.
- Bestuurlijke sturing en draagvlak.

2.2. Governance en samenwerking

Governance en samenwerking zijn essentiële voorwaarden voor een effectieve implementatie van het VIRBI 2025 en maken het mogelijk om op een gestructureerde en beheerste wijze het gewenste betrouwbaarheidsniveau voor de verwerking van gerubriceerde informatie te realiseren.

2.2.1. Wat organiseer je daarvoor:

- Three lines of defense.
- Rollen, taken en verantwoordelijkheden.
- RASCI-tabel.
- Overlegstructuren.

- Rapportagelijnen.
- Gebruik het gereedschap uit de gereedschapskist.
- Samenwerking tussen:
    - CISO;
    - BVA;
    - proceseigenaren;
    - IV/ICT;
    - securityarchitect;
    - privacy/functioneel beheer;
    - audit/compliance.

2.2.2. Wat is het resultaat:

- Heldere verantwoordelijkheden.
- Structurele samenwerking en besluitvorming.

2.3. Breng TBB's in kaart

Het is belangrijk om de Te Beschermen Belangen (TBB's) te identificeren en te analyseren, zodat passende maatregelen kunnen worden getroffen om deze effectief en risicogestuurd te beschermen.

2.3.1. Wat organiseer je daarvoor:

- Inventarisatie van Te Beschermen Belangen (TBB's).
- Start bij kritieke processen.
- Gebruik het gereedschap uit de gereedschapskist.
- Vaststellen van:
    - gevoelige informatie;
    - kritieke processen en systemen;
    - afhankelijkheden;
    - ketens;
    - externe partijen.

2.3.2. Wat is het resultaat:

- Inzicht in wat beschermd moet worden.
- Prioritering van kritieke belangen.

2.4. Voer risicoanalyse uit op TBB's

Het uitvoeren van een risicoanalyse op Te Beschermen Belangen (TBB's) is belangrijk om inzicht te krijgen in dreigingen, kwetsbaarheden en risico's, zodat gerichte en proportionele beveiligingsmaatregelen kunnen worden genomen.

2.4.1. Wat organiseer je daarvoor:

- Analyse van dreigingen en kwetsbaarheden.
- Kans x impact-beoordeling.
- Risicoclassificatie.
- Prioritering van risico's.
- Risicobehandelplan.
- Vastlegging van restrisico's.
- Gebruik het gereedschap uit de gereedschapskist.

2.4.2. Wat is het resultaat:

- Inzicht in belangrijkste risico's.
- Onderbouwing voor maatregelen.

2.5. Implementeer maatregelen en bouw architectuur

Het is belangrijk om een samenhangende set van maatregelen te nemen, zodat organisatorische, technische, fysieke en procedurele beveiligingsmaatregelen elkaar versterken en gezamenlijk bijdragen aan een effectief en beheerst beveiligingsniveau.

2.5.1. Wat organiseer je daarvoor:

- Overzicht van alle maatregelen.
- Samenhang tussen organisatorische, technische, fysieke en procedurele maatregelen.
- Eigenaarschap per maatregel.
- Roadmap en planning.
- Securityarchitectuur.
- Logging, monitoring en toegangsbeveiliging.
- Need-to-know-principe.
- Awareness en opleidingen.
- Gebruik het gereedschap uit de gereedschapskist.

2.5.2. Wie betrek je daarbij:

- Securityarchitect.
- CISO/BVA.
- ICT-architectuur en beheer.

2.5.3. Wat is het resultaat:

- Samenhangend stelsel van beveiligingsmaatregelen.
- Duurzaam beveiligingsontwerp.

2.6. Richt PDCA-cyclus en tactisch team in

Het organiseren van een PDCA-cyclus is belangrijk om de effectiviteit van beveiligingsmaatregelen periodiek te toetsen, tijdig bij te sturen en de beveiliging structureel te blijven verbeteren en borgen.

2.6.1. Wat organiseer je daarvoor:

- Periodieke controles.
- KPI's en managementrapportages.
- Audits en evaluaties.
- Tactisch overleg/team.
- Escalatieproces.
- Continue verbetering.
- Actualisatie van risico's en maatregelen.
- Gebruik de PDCA-checklist uit de gereedschapkist.

2.6.2. Wat is het resultaat:

- Continue borging en verbetering.
- Aantoonbaar "in control".

2.7. Rubriceer

Rubriceren is van belang om vast te stellen welke mate van vertrouwelijkheid bescherming vereist, zodat passende beveiligingsmaatregelen kunnen worden toegepast op gerubriceerde informatie.

2.7.1. Wat organiseer je daarvoor:

- Gebruik van het rubriceringsbesluit van je eigen organisatie.
- Toepassing van de handreiking in gereedschapskist.
- Hanteer een uniforme werkwijze voor rubriceren.
- Aansluiting op processen en informatiestromen.
- Bewustwording en instructie voor medewerkers.

2.7.2. Resultaat:

- Eenduidige rubricering van informatie.
- Duidelijkheid over vertrouwelijkheidseisen.

2.8. Samenvatting inhoud plan van aanpak

Hieronder geven we een samenvattende tabel met een opsomming van onderwerpen die je minimaal in het plan van aanpak kunt opnemen:

Samenvattende tabel: beknopt plan van aanpak:

Onderdeel	**Inhoud**
Doel en scope	Wat en waarom
Governance	Rollen, overleg en verantwoordelijkheden
TBB's	Wat moet beschermd worden
Rubriceren	Vertrouwelijkheid en bescherming
Risicoanalyse	Belangrijkste risico's
Maatregelen	Wat wordt ingevoerd
Planning	Prioriteiten en roadmap
Architectuur	Samenhang en ontwerp
Borging	PDCA, audits en monitoring

2.9. Wat zijn belangrijke uitgangspunten

Beschrijf niet alleen losse maatregelen, maar vooral:

- de samenhang;
- prioriteiten;
- verantwoordelijkheden;
- afhankelijkheden;
- borging van de maatregelen.

Juist die integraliteit maakt aantoonbaar dat de organisatie beheerst en risicogestuurd werkt conform het VIRBI 2025.

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.

12-5-2026