Gereedschap voor Governance VIRBI implementatie

Dit document geeft gereedschap voor governance van gerubriceerde informatie. Het biedt ondersteuning bij de implementatie van het VIRBI 2025.

1. Inleiding

Governance is cruciaal voor het effectief implementeren van het VIRBI omdat het kaders en processen biedt voor het beheer van gerubriceerde informatie. Governance is geen “nice-to-have” bij security. Zonder governance blijft beveiliging fragmentarisch, reactief en afhankelijk van individuen in plaats van structureel geborgd. Het vormt de bestuurlijke laag die bepaalt wat beveiligd moet worden, waarom, en hoe consistent dat gebeurt.

Het omvat:

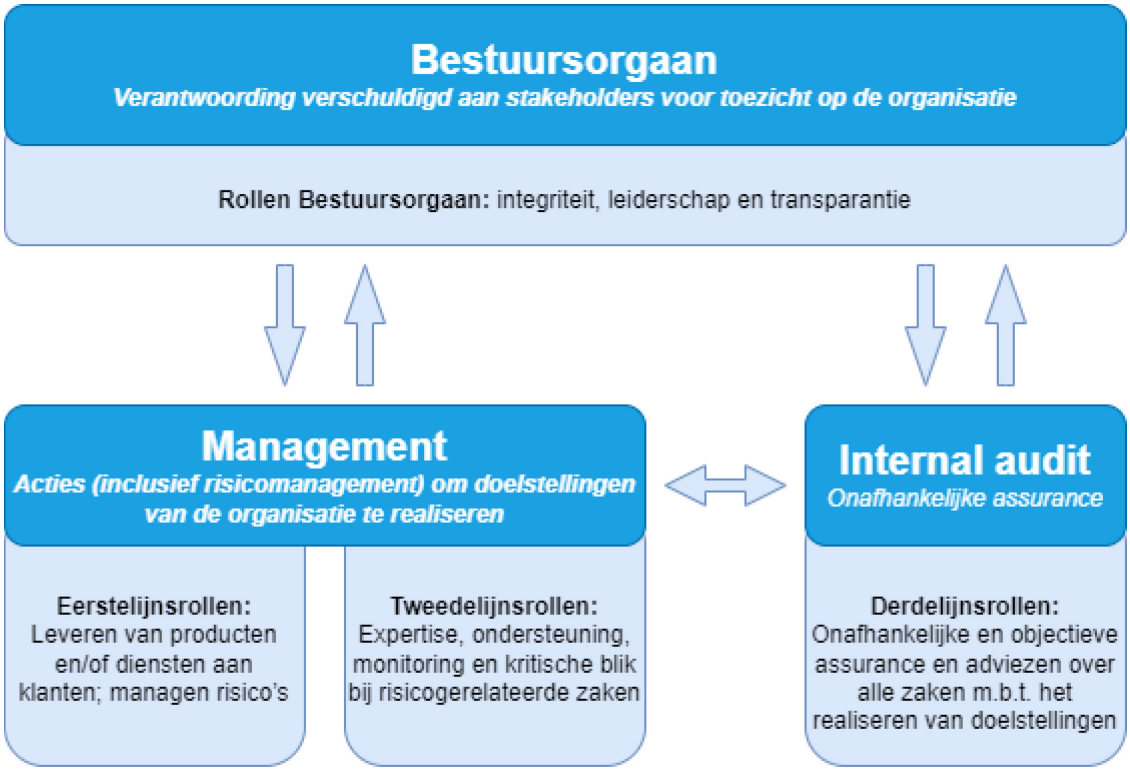
- Risicomanagement, waarbij risico's van onjuiste of onveilige behandeling van informatie worden geanalyseerd en gemitigeerd;
- Adequate maatregelen, zoals toegangscontrole en encryptie, moeten worden getroffen om de vertrouwelijkheid van de informatie te waarborgen;
- Besluitvorming rondom deze aspecten moet gestructureerd en helder zijn, zodat informatie op een verantwoorde en veilige manier wordt beheerd;
- Monitoring, (tactische) controle en rapportage.

Goede governance maakt het dus mogelijk om het VIRBI effectief te implementeren en voldoet aan de vereisten voor bescherming en compliance.

1.1. Het drielagenmodel

Voor een goede besturing zijn zowel bestuurders, verantwoordelijke lijnmanagers, specialisten, adviseurs en auditeurs belangrijk. Het is een samenspel van verschillende rollen. We nemen het drielagenmodel als uitgangspunt.

Onderstaand is dat schematisch weergegeven.



De aansturing en beheersing van organisaties kunnen volgens het bovenstaande drie-lagen-model beschreven worden. Dat betreft:

- Een eerste lijn, het bevoegd gezag, die de acties uitvoert of delegeert, die invulling geven aan de realisatie van de organisatiedoelen en de beheersing van de gerelateerde risico's;
- Een tweede lijn, die adviseert en kaders stelt en die de eerste lijn daarin faciliteert;
- Een derde lijn die de kwaliteit van de risicobeheersing door de eerste lijn en de samenwerking tussen de eerste en tweede lijn onafhankelijk beoordeelt en adviezen geeft ter verbetering.

Zowel het management als internal audit leggen verantwoording af aan en rapporteren naar het bestuur. Het bestuur geeft opdracht en richting, delegeert taken, voorziet in benodigde middelen en houdt toezicht op de organisatie. Het management en internal audit zorgen voor een goede onderlinge afstemming, communicatie, coördinatie en samenwerking.

1.2. Voorbeeld RASCI-tabel

Om te komen tot een effectieve samenwerking maken we gebruik van een voorbeeld RASCI-tabel met daarin taken, bevoegdheden en verantwoordelijkheden in een helder overzicht.

Onderstaand: Voorbeeld RASCI-tabel voor besturing van gerubriceerde informatie:

	Responsible	Accountable	Supporting	Consulted	Informed
Identificatie van vertrouwelijke informatie					
Bestuur		X			X
Lijnmanager/Informatie-eigenaar	X				
RA-procesbegeleider			X		
CISO/BVA			X	X	
Adviseur & specialist				X	

Risicoanalyse van gerubriceerde informatie					
Lijnmanager/Informatie-eigenaar		X		X	
RA-procesbegeleider	X				
CISO/BVA			X		
Accepteren van risico's buiten de risicobereidheid					
Bestuur		X		X	
Lijnmanager/Informatie-eigenaar	X				
CISO/BVA			X		
Overdragen van de maatregelen naar een maatregeleigenaar					
Bestuur		X			X
Lijnmanager/Informatie-eigenaar	X				
Maatregeleigenaar				X	X
Beveiligingsmaatregelen implementeren					
Bestuur					X
Lijnmanager/Informatie-eigenaar		X			
CISO/BVA			X		
Maatregeleigenaar	X				
Adviseur & specialist				X	
Opstellen van de risicoanalyserapportage					
Lijnmanager/Informatie-eigenaar		X			
RA-procesbegeleider	X				
CISO/BVA				X	
Bestuur					X
Monitoren en rapporteren van compliance					
Bestuur		X			X
CISO/BVA	X				
Toezicht op implementatie van het VIRBI					
Bestuur		X			X
Lijnmanager/Informatie-eigenaar			X	X	
CISO/BVA	X			X	

Hieronder geven we uitleg van taken, bevoegdheden en verantwoordlijkheden (TBV) van de bovenstaande RASCI-tabel:

- R (Responsible): Degene die verantwoordelijk is voor de uitvoering van een taak of activiteit. Deze persoon voert het werk uit;
- A (Accountable): Degene die eindverantwoordelijk is voor de taak en ervoor zorgt dat het correct wordt uitgevoerd. Er kan maar één accountable persoon per taak zijn;
- S (Supportive): Personen die ondersteuning bieden bij het uitvoeren van de taak, bijvoorbeeld door middelen, expertise of assistentie;
- C (Consulted): Personen die geconsulteerd moeten worden voor advies of input tijdens het proces. Dit zijn vaak experts of belanghebbenden wiens feedback waardevol is;
- I (Informed): Personen die op de hoogte moeten worden gehouden van de voortgang of uitkomsten van de taak, maar die niet direct betrokken zijn bij de uitvoering.

De bovenstaande RASCI-tabel is een voorbeeld en is bedoeld om er zelf mee aan de slag te gaan om het geschikt te maken voor de eigen organisatie. Het doel is om samen afspraken te maken zodat er een duidelijke en effectieve governance van gerubriceerde informatie ontstaat. Daarbij kent iedere betrokkene zijn of haar rol, en is er een gezamenlijke verantwoordelijkheid voor het beveiligen en beheren van gevoelige gegevens.

2. Stappenplan governance

Om de governance van gerubriceerde informatie duidelijk, transparant en helder te maken geven we een kort stappenplan.

Stappenplan voor het adequaat inregelen van governance van gerubriceerde informatie:

2.1. Bepaal de doelstellingen van de governance

- Doelen vaststellen zoals het waarborgen van de vertrouwelijkheid van gerubriceerde informatie, naleving van het VIRBI en het optimaliseren van het gebruik van deze informatie;
- Specificeer wat er nodig is op het gebied van risicomanagement, compliance en informatiebeveiliging. Gebruik daarvoor ook bijlage 1 van het VIRBI 2025 om tenminste een basisset van maatregelen te nemen.

2.2. Identificeer betrokkenen en rollen

- Betrek alle relevante spelers: bestuurders, informatie-eigenaren, BVA, CISO, adviseurs en specialisten;
- Stel vast welke rol elke betrokkene heeft in het proces van werken met en beveiligen van gerubriceerde informatie.

2.3. Stel een RASCI-tabel op

- Maak aan de hand van de voorbeeld-RASCI-tabel een concrete invulling en definieer de verantwoordelijkheden van de betrokkenen duidelijk in het overzicht. Voeg concrete namen en functienamen toe per rol.

2.4. Organiseer bijeenkomsten of workshops

- Plan een reeks bijeenkomsten of workshops met de betrokkenen zoals: bestuurders, informatie-eigenaren, BVA, CISO, adviseurs en specialisten;
- Doelen van de workshops zijn:
    - Het verduidelijken van de rollen en verantwoordelijkheden;
    - Het bespreken van de benodigde maatregelen om gerubriceerde informatie veilig en effectief te beheren;
    - Het maken van een impacttabel rubriceren, toegespitst op de organisatie;
    - Het gezamenlijk vaststellen van procedures voor het classificeren, beveiligen en controleren van gerubriceerde informatie.

2.5. Discussieer en leg de verantwoordelijkheden vast

- Tijdens de sessies, bespreek per activiteit of taak wie verantwoordelijk (R), verantwoordelijk voor de eindbeslissing (A), ondersteunend (S), geconsulteerd (C) en geïnformeerd (I) is;
- Zorg ervoor dat iedereen het eens is over de gemaakte keuzes en de invulling van hun rollen;
- Leg de governance-structuur schriftelijk vast en zorg voor goedkeuring van het bestuur.

2.6. Stel een actieplan op en implementeer

- Na de workshops, stel je een concreet actieplan op met duidelijke mijlpalen en deadlines;
- Begin met de implementatie van de governance-structuur door de gedefinieerde rollen en verantwoordelijkheden in de dagelijkse processen te integreren.

2.7. Monitor en rapporteer de compliance

- Verzamel gegevens over de compliance t.a.v. de vertrouwelijkheid van gerubriceerde informatie;
- Analyseer de verzamelde gegevens om te bepalen of hoe het staat met: voortgang van maatregelen en waar compliance onvoldoende is en waar bijsturing nodig is;
- Deel de compliance-rapportage op gezette tijden met de stakeholders.

Tip: Gebruik de "Three Lines of Defense"- aanpak en voer (tactische) reviews uit

om te waarborgen dat beveiligingsmaatregelen effectief zijn geïmplementeerd en nageleefd.

2.8. Evalueren en stuur zo nodig bij

- Evalueer na een bepaalde periode de effectiviteit van de governance en pas deze aan waar nodig;
- Organiseer periodieke updates en trainingen om de betrokkenen up-to-date te houden over veranderingen in beleid of technologie.

Tip: Implementatie van het VIRBI gaat niet alleen over digitale informatiebeveiliging maar betreft in essentie integrale beveiliging om de vertrouwelijkheid van gerubriceerde informatie te waarborgen. Het gaat dus naast digitale zaken ook over fysieke zaken zoals toegang, gebouwen en ruimtes, kasten en kluizen en de daarbij horende rollen en processen.

2.9. Uitkomst

Na deze bovenstaande stappen ontstaat er een duidelijke en effectieve governance van gerubriceerde informatie. Alle betrokkene kennen hun rol en er is een gezamenlijke verantwoordelijkheid voor het beveiligen en beheren van gevoelige gegevens.

Je beschikt nu over concrete producten zoals;

- Een RASCI-tabel passend op je eigen organisatie;
- Vastgestelde doelen;
- Een voor de organisatie specifiek gemaakte impacttabel;
- Een overzicht van de namen en contactinformatie van alle betrokkenen;
- Een overzicht van (mogelijke) maatregelen per rubriceringsniveau;

- Een actieplan voor implementatie van de governance-structuur door de gedefinieerde rollen en verantwoordelijkheden in de dagelijkse processen te integreren;
- Afspraken over monitoring en rapportage om de voorgang inzichtelijk te maken;
- Afspraken over evaluatie en bijsturen.

3. Colofon

Wil je reageren, mail dan naar: CISORijk@minbzk.nl

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

Sponsoren van deze gereedschapskist zijn de BVA Rijk en de CISO Rijk.