Gereedschap risicoanalyse van gerubriceerde informatie:

1. Inleiding

Dit document is een hulpmiddel dat bedoeld is om je op weg te helpen bij de risicoanalyse van gerubriceerde informatie, zoals benoemd in het VIRBI 2025.

Een onderdeel van VIRBI 2025 is de bijlage, waarin de uitgangspunten en het vereiste beveiligingsniveau zijn vastgelegd voor de bescherming van de vertrouwelijkheid van bijzondere informatie en de verwerking daarvan in informatiesystemen.

De te nemen maatregelen ter bescherming van de vertrouwelijkheid van bijzondere informatie worden bepaald op basis van een risicoanalyse. Het VIRBI gaat over vertrouwelijkheid maar in de praktijk neem je betrouwbaarheid en integriteit ook mee bij de risicoanalyse van informatie.

De te nemen maatregelen omvatten in ieder geval de uitgangspunten en maatregelen zoals weergegeven in de tabellen van de bijlage in het VIRBI 2025. Indien wordt afgeweken van deze voorgeschreven maatregelen, moet dit in de risicoanalyse gemotiveerd worden vastgelegd, inclusief eventueel aanvullende mitigerende maatregelen. Een eventuele afwijking voor Dep.V vereist minimaal goedkeuring door een lijnmanager of directeur, en voor STG ten minste door een DG.

1.1. Implementatie van het VIRBI

Implementatie van het VIRBI 2025 omvat de beheersing van risico's t.a.v. de exclusiviteitseisen van de verwerking van gerubriceerde informatie. Dat gaat door middel van het treffen van een beheerst risicogestuurd stelsel van passende mitigerende integrale beveiligingsmaartregelen. Deze maatregelen die de onderkende risico's reduceren tot aanvaardbare proporties en recht doen aan de compliance vereisten zoals deze zijn opgelegd door ketenpartners. Daarmee is de risicoanalyse die vanuit het VIRBI 2025 wordt voorgeschreven een onlosmakelijk deel van de risicoanalyse met de bijbehorende scope (te weten betrouwbaarheid) die vanuit het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) wordt voorgeschreven.

1.2. Rubriceren:

In het VIRBI wordt gesproken over bijzondere informatie of gerubriceerde informatie. Deze informatie moet extra goed worden beveiligd om de vertrouwelijkheid te waarborgen. Dat betekent dat deze informatie niet in handen mag komen van ongeautoriseerde personen.

Ook hier geldt: Het VIRBI gaat over vertrouwelijkheid maar in de praktijk neem je betrouwbaarheid en integriteit ook mee bij de risicoanalyse van informatie. Dat geldt dus voor dit hele document.

Voor uitleg over hoe je informatie kunt rubriceren, verwijzen we naar het document uit de toolkit:

'Gereedschap rubriceren'. Daarin wordt ingegaan op:

- Een eventueel rubriceringsbesluit van jouw organisatie;
- Procedures en uitleg over hoe medewerkers informatie moeten rubriceren;
- Verwijzingen naar aanvullende documenten en voorbeelden.

2. Risicoanalyse:

Het doel van een risicoanalyse is om inzicht te krijgen in potentiële bedreigingen en risico's zodat je gepaste maatregelen kunt nemen om de vertrouwelijkheid van gerubriceerde informatie te waarborgen.

Bij een risicoanalyse bepaal je de risico's voor gerubriceerde informatie aan de hand van een gekozen methode. Het is daarom belangrijk om binnen je organisatie af te stemmen welke analysemethode wordt gehanteerd.

Als er binnen de organisatie nog geen vaste methode is vastgesteld, vormt het kiezen van een passende methode een eerste stap. Het advies is om in dat geval te beginnen met een eenvoudige methode.

Voorbeelden van methoden voor risicoanalyse zijn: MAPGOOD, SWOT, FMEA, IRAM, MASKER en RAVIB. Eventueel kan je een eigen (afgeleide) aanpak kiezen vanuit de eigen professionaliteit. Kern is dat je aan risicoanalyse en risicomanagement doet op een gestructureerde en professionele wijze.

Heb je weinig kennis van een methode? Dan kun je een workshop of training volgen om ermee aan de slag te gaan. Vanuit het ondersteuningsprogramma faciliteert CIO Rijk eventueel een workshop risicoanalyse. Neem daarvoor contact op met: CIORijk-IB&P@minbzk.nl

2.1. Reikwijdte:

Om de vertrouwelijkheid van gerubriceerde informatie te kunnen waarborgen, hanteren we een brede definitie van een informatiesysteem: Een informatiesysteem is een samenhangend geheel van gegevensverzamelingen, de daarbij behorende personen, procedures, processen en programmatuur, evenals de getroffen voorzieningen voor opslag, verwerking en communicatie.

Verder is het van belang om te noemen dat implementatie van het VIRBI niet alleen gaat over digitale informatiebeveiliging maar juist gaat over integrale beveiliging. Het doel daarbij is 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.

2.2. Stappen risicoanalyse:

Hieronder geven we een voorbeeld van de te doorlopen stappen van de risicoanalyse:

a) Identificatie en bewustwording: Een eerste stap is identificatie en bewustwording in de organisatie. Je wilt inzicht krijgen over hoe je risico's kan beperken van systemen, processen, personen, componenten, data en andere hulpmiddelen en welke maatregelen je daarbij kan inzetten. Deze eerste stap is cruciaal en randvoorwaardelijk om risico's effectief te kunnen beheersen. Ook compliance neem je hierbij mee, je moet immers voldoen aan wet en regelgeving.

b) Analyse van de Te Beschermen Belangen (TBB): Identificeer deze TBB's en prioriteer de bescherming daarvan. Daarbij bepaal je eerst wat de benodigde betrouwbaarheid moet zijn van de TBB's;
c) Inzicht krijgen in dreigingen, kwetsbaarheden en risico's: Dreiging kan je zien als dader profiel met gewogen onderbouwing van capabiliteit en intentie. Wat kan er misgaan? Waar zitten de kwetsbaarheden? Hanteer een brede scope en kijk naar: de boze buitenwereld, personeel, processen en systemen als geheel. Deze stap heeft een relatie met de gestelde betrouwbaarheidseisen. Kans en impact inschatten maakt deel uit van deze stap: Hoe waarschijnlijk is het risico? Wat is het gevolg als het zich voordoet?;
d) Prioriteiten stellen: Welke risico's vragen directe actie? Wat kan eventueel worden geaccepteerd?;
e) Maatregelen bepalen: (Kijk hiervoor ook naar de Bijlage van het VIRBI 2025). Welke acties kun je nemen om risico's te verminderen of te beheersen?
f) Voorbereid zijn: Voorkomen dat je wordt verrast. Plannen klaar hebben, incl. het testen van de plannen, voor als er toch iets gebeurt. Denk daarbij aan een calamiteitenplan, een back-upstrategie of herstelstrategie.

Risicoanalyse helpt je om bewust keuzes te maken en grip te houden op onzekerheden. Dat doe je door het realiseren van het gewenste betrouwbaarheidsniveau door het treffen van een stelsel van informatiebeveiligingsmaatregelen.

2.3. Risicobehandelplan

Als de 'te nemen maatregelen' zijn bepaald moet je deze toekennen aan eigenaren van de maatregelen die er mee aan de slag gaan om uit te (laten) voeren. Maatregelen kunnen groot of klein zijn en er is meestal een plan van aanpak nodig voor de uitvoering. Stel een 'risicobehandelplan' op waar alle risico's, eigenaren en de te nemen maatregelen zijn opgenomen.

3. Verbetercyclus:

Eenmalig maatregelen nemen is onvoldoende. Je moet blijven opletten en verbeteren om het gewenste betrouwbaarheidsniveau te kunnen behouden. Om te kunnen verbeteren moet je de voortgang regelmatig monitoren. Ook wil je weten of de genomen maatregelen effectiviteit zijn.

3.1. Risicoregister:

Je moet de bepaalde risico's en maatregelen vastleggen in een systeem of register. Dat heet dan een risicoregister. Meestal is dat belegd bij de CISO en afdeling IT. Bespreek in je organisatie of dat er al is? Soms is het geïntegreerd in een Information Security Management System (ISMS). Als er niets is kan je beginnen met een spreadsheet. Strikt genomen is het beheer van maatregelen onderdeel van risicomanagement en hoort het niet bij risicoanalyse zelf.

We geven nog een tip: Let op bij registratie van TBB- of STG-info in een risicoregister of ISMS. Hier hoort een bepaalde terughoudendheid bij, de informatie die je registreert mag namelijk niet hoger zijn dan de rubricering van het informatiesysteem waarin de registratie plaatsvindt. Anders gezegd, het is in strijd met het VIRBI om STG info op te nemen in een informatiesysteem die daar niet geschikt voor is. Een voorbeeld daarvan is een STG-C document inscannen en opnemen in een

managementsysteem van een departement dat slechts Dep V is gerubriceerd. Dat is dus niet de bedoeling.

3.2. Monitoren en rapporteren

Benoem een tactisch team die op gezette tijden monitort en rapporteert waar je staat. Hierbij worden onder andere (tactische) reviews uitgevoerd om te waarborgen dat beveiligingsmaatregelen correct zijn geïmplementeerd en worden nageleefd. Het monitoren, verbeteren en zo nodig verbeteracties in gang zetten is onderdeel van de PDCA-cyclus. Er is een PDCA-checklist beschikbaar in de gereedschapskist.

3.3. Governance:

Er is gereedschap beschikbaar met de titel "Governance VIRBI-implementatie". Gebruik dit hulpmiddel om, aan de hand van een voorbeeld RASCI-tabel, duidelijke afspraken te maken over rollen en verantwoordelijkheden met betrekking tot het uitsplitsen van de implementatierollen. Dus: wie is verantwoordelijk voor risicoanalyse opstellen en vaststellen, wie voor uitvoering van maatregelen, monitoring / toezicht op risicoanalyse en implementatie en effectiviteit van getroffen maatregelen, wie rapporteert aan wie, etc.

4. Colofon:

Wil je reageren? Dat kan naar: CISORijk@minbzk.nl

Dit gereedschap is tot stand gekomen met een brede werkgroep en maakt deel uit van: Toolkit ter ondersteuning implementatie van het VIRBI 2025. Sponsoren van dit traject zijn de BVA Rijk en de CISO Rijk.