Gereedschap: Te Beschermen Belangen (TBB) systematiek

1. Hoofdstuk 1 Inleiding en stappenplan

Dit document is bedoeld om je praktisch op weg te helpen bij de implementatie van het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere informatie (VIRBI). Je moet immers belangen beschermen. Voor het VIRBI gaat het om het borgen van de vertrouwelijkheid van gevoelige of gerubriceerde informatie. Dit document beschrijft de systematiek van de Te Beschermen Belangen oftewel de TBB's.

1.1. Voor wie is dit document?

Dit document richt zich op TBB-eigenaren en medewerkers die verantwoordelijk zijn voor het in kaart brengen en beveiligen van Te Beschermen Belangen (TBB's), binnen alle departementen en organisaties.

1.2. Wat is het doel van dit document?

Dit document helpt diensten en directies door een methode en stappenplan te geven die ze kunnen hanteren om TBB's vast te stellen en adequaat te beveiligen.

1.3. Wat is een TBB?

Een organisatie wil haar eigen organisatiedoelen behalen (niveau 1). Om deze doelstellingen te realiseren wordt er informatie verwerkt, en zijn processen ingericht (niveau 2). Deze processen worden ondersteund door netwerk- en informatiesystemen (niveau 3). Te Beschermen Belangen hebben betrekking op alle onderstaande niveaus.

Je hanteert een indeling van drie niveaus:

- Niveau 1: Organisatiedoelen
- Niveau 2: Processen
- Niveau 3: Netwerk- en informatiesystemen

Onder Te Beschermen Belangen wordt verstaan: informatie, informatiesystemen, materieel, goederen, (bewinds)personen en objecten waarbij compromittering ernstige gevolgen kan hebben.

Dat geldt voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid. En ook voor delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries. Een TBB bevat één of meerdere van deze componenten.

Kennisname, aantasting of verlies van deze belangen door onbevoegden, zoals statelijke actoren of criminele organisaties kan leiden tot maatschappelijke ontwrichting, economische schade of het verlies van politieke legitimiteit. Bij het bepalen van het TBB staan de primaire processen centraal.

Tip: Voor implementatie van het VIRBI gaat het specifiek over het borgen van de vertrouwelijkheid van gerubriceerde informatie. Als je breder kijkt neem je ook Integriteit en beschikbaarheid mee.

1.4. Waarom is dit belangrijk?

Kennisname door niet-geautoriseerden kan (zeer ernstige) schade toebrengen aan een van de vitale belangen van Nederland of van zijn bondgenoten.

Het goed in beeld hebben en adequaat beveiligingen van TBB's is daarom noodzakelijk om aantasting, kennisname en/of verstoring van de primaire processen van de ministeries zoveel mogelijk te voorkomen en/of te beperken.

Verschillende wet-, regelgeving en normenkaders hanteren de TBB's als basis voor de implementatie. Denk daarbij aan het Normenkader Beveiliging Rijkskantoren (NkBR), Voorschrift Informatie Beveiliging Rijksdienst Bijzondere Informatie (VIRBI) en Algemene Beveiligingseisen voor Rijksoverheidsopdrachten(ABRO).

Tip: Het in beeld hebben en beschermen van TBB's is dus niet alleen noodzakelijk, maar ook verplicht!

1.5. Wat is het wettelijk kader van de TBB's?

De basis voor het vaststellen en beschermen van de TBB's is vastgelegd in het Besluit BVA-stelsel Rijksdienst 2021[1].

In het Besluit BVA-stelsel is opgenomen dat de secretaris-generaal (SG) eindverantwoordelijk is voor de inrichting en werking van integrale beveiliging van haar organisatie (onderdeel), evenals de zorg voor en de beveiliging van de TBB's van het departement.

De SG is ook eindverantwoordelijk voor het treffen van maatregelen voor de integrale beveiliging van het Te Beschermen Belang op basis van risicoanalyse. De SG stelt, binnen de rijksbrede kaders, het departementale integrale beveiligingsbeleid vast.

Ook wijst de SG een beveiligingsautoriteit aan. De exacte rolverdeling kan per departement verschillen. In de "Toolkit ondersteuning implementatie VIRBI" is gereedschap beschikbaar voor het inregelen van Governance. Een goede governance is essentieel voor effectieve beveiliging[2].

1.6. Stappenplan TBB-aanpak

De voorgestelde TBB-aanpak bestaat uit vier stappen zoals ook het NCSC[3] aangeeft:

1. Schep de randvoorwaarden;
2. Verkrijg mandaat en draagvlak;
3. Breng TBB's in kaart
4. Onderneem de vervolgstappen

Voor deze vier stappen geven we hieronder een toelichting op hoofdlijnen. In de volgende hoofdstukken 2 en 3 geven we meer gedetailleerde informatie.

1.6.1. Stap 1: Schep de randvoorwaarden

Voordat je aan de slag gaat met het in kaart brengen van jouw Te Beschermen Belangen is het belangrijk om de juiste randvoorwaarden te scheppen. In deze stap schrijf je een beknopt plan van aanpak. Dit plan helpt je om draagvlak bij collega's te creëren en is het uitgangspunt om mandaat te verkrijgen van het bestuur van jouw organisatie.

In het plan beschrijf je o.a.:

- Jouw definitie van een TBB, dit helpt bij het inventariseren van TBB's en het voeren van de dialoog over hoe belangrijk een bepaalde TBB is ten opzichte van een andere TBB;
- Concrete doelstelling(en) van jouw organisatie en definieer daarbij op hoofdlijnen welke categorieën[4] belangen hiermee gemoeid gaan;

[1] wetten.nl - Regeling - Besluit BVA-stelsel Rijksdienst 2021 - BWBR0044617

[2] The NIST Cybersecurity Framework (CSF) 2.0

[3] Hoe breng ik mijn te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum

[4] Denk hierbij aan financiële-, juridische-, reputatie- en veiligheidsbelangen.

- Welke organisatieprocessen essentieel zijn ten aanzien van de hierboven genoemde categorieën van belangen;
- Een procesvoorstel met de verschillende processtappen in volgorde. Denk daarbij aan: een overzicht van stakeholders, een eerste inventarisatie van informatie die reeds aanwezig is op het gebied van organisatiedoelstellingen en processen. In workshops en/of tabeltops bespreek je deze zaken met collega's waarin je belangen inventariseert en met elkaar prioriteert, de resultaten in een referentietabel gaat samenvatten en deze referentietabel aan het bestuur oplevert en eventuele vervolgstappen toelicht en toetst.

1.6.2. Stap 2: Verkrijg mandaat en draagvlak

In stap 1 heb je de randvoorwaarden geschept om de Te Beschermen Belangen van jouw organisatie in kaart te brengen. De volgende stap in dit proces is het verkrijgen van mandaat bij het bestuur van jouw organisatie en het betrekken van de stakeholders. Om dit mandaat te verkrijgen ga je in gesprek en leg je het door jou opgestelde procesvoorstel voor.

1.6.3. Stap 3 Breng TBB's in kaart

In de voorgaande stappen heb je de voorbereidingen getroffen en mandaat verkregen. Het is nu tijd om echt aan de slag te gaan! In deze stap ga je de TBB's van jouw organisatie in kaart brengen en vervolgens waarderen en prioriteren. Deze resultaten verwerk je in een referentietabel.

Wanneer je de TBB's van jouw organisatie in kaart gaat brengen is het nuttig om éérst te inventariseren welke informatie er al beschikbaar is. Dit houdt in dat je praat met stakeholders binnen verschillende afdelingen.

Denk ook aan Leveranciersinformatie zoals contracten, service level agreements en compliancestandaarden. risicoanalyses die zijn gemaakt voorafgaand aan het inkopen van een dienst of product en evaluaties van bestaande diensten waarin potentiële risico's worden genoemd.

Dergelijke informatie helpt je een eerste beeld te krijgen van de TBB's van jouw organisatie. Samen met stakeholders binnen je organisatie ga je de dialoog aan om de TBB's verder te inventariseren, concretiseren en prioriteren.

Organiseer gesprekken, dialoogsessies en workshops waarin je na afloop gezamenlijke conclusies kan trekken en nog steeds met ruwe resultaten werkt. Verwerk deze resultaten in de referentietabel. Zie deze gesprekken en ruwe resultaten als stappen op weg naar het beschermen van de TBB's van je organisatie.

1.6.4. Stap 4 Onderneem vervolgstappen

Wanneer je de bovenstaande stappen hebt gevolgd ben je in het bezit van een (ruwe) lijst met TBB's van jouw organisatie op procesniveau. Je kan nu een aantal vervolgstappen zetten. Dat betreft op hoofdlijnen:

Werk de tabel uit naar het niveau van netwerk- en informatiesystemen. Daarbij begin je bij de zeer grote belangen en werkt vanuit daar omlaag in de tabel. Je maakt in deze stap een eerste overzicht van kritieke elementen binnen (digitale) infrastructuur in relatie tot de Te Beschermen Belangen op procesniveau.

Incidenten met gevoelige informatie kunnen een grote gevolgen hebben. Daarom is het noodzakelijk om deze risico's te beheersen. Wijs voor informatie een 'eigenaar' aan. De lijst met TBB's kan helpen om binnen de geïdentificeerde categorieën een eigenaar aan te wijzen. Een NCSC -factsheet[5] biedt handvatten om grip te krijgen op de beheersing van risico's bij het werken met gevoelige informatie.

[5] risico's beheersen: de waarde van informatie als uitgangspunt

Op basis van een risicoanalyse kun je vervolgens bepalen wat de juiste maatregelen zijn om deze belangen te beschermen. Bijlage 1 van het VIRBI 2025 geeft een concreet overzicht van mogelijke maatregelen.

1.7. PDCA-cyclus:

Het in kaart brengen van de TBB's van de organisatie is geen eenmalige exercitie. Zaken zoals veranderde bedrijfsdoelstellingen, nieuwe wetgeving of risico's kunnen er voor zorgen dat de TBB's veranderen. Richt in samenspraak met het bestuur een proces en/of beleid in, waarin je afspreekt hoe het overzicht van TBB's actueel gehouden kan worden. Je kunt bijvoorbeeld vaststellen dat de referentietabel elke X aantal maanden herzien moet worden. Een tactisch team kan periodiek evalueren of het overzicht van TBB's nog actueel is of dat je het moet actualiseren.

We hebben nu de vier stappen op hoofdlijnen besproken hoe je de TBB's voor je organisatie in kaart kan brengen en passende maatregelen kan nemen op basis van risicoanalyse. Tevens dien je aan de hand van een PDCA-cyclus, periodiek te evalueren en zo nodig bij te sturen om het overzicht van TBB's actueel te houden en blijvend de risico's' te kunnen beheersen.

2. Hoofdstuk 2 - Indeling in vier categorieën TBB's

Om de TBB op het juiste niveau te beschermen is het noodzakelijk om te komen tot een afgewogen geheel aan organisatorische, bouwkundige, elektronische en digitale beveiligingsmaatregelen.

2.1. Vaststellen categorieën

Voor het vaststellen van de noodzakelijke beveiligingsmaatregelen is het van belang om een beeld te hebben van de dreiging waaraan een TBB is blootgesteld en de impact die aantasting van een TBB kan hebben.

Verder dient duidelijk te zijn wat het belang is van de betreffende TBB voor het ongestoord functioneren van het departement en/of de Rijksoverheid.

Voor wat betreft dit laatste worden de Te Beschermen Belangen op basis van impactcriteria ingedeeld in vier categorieën, waarbij de hoogte van de categorie afhankelijk is van de schade die kan ontstaan of de consequenties voor de continuïteit van het functioneren van één of meerdere ministeries.

Deze categorie indeling geldt als hulpmiddel voor prioritering bij de toewijzing van middelen en helpt bij het maken van keuzes ten aanzien van de inzet van beveiligingsmaatregelen ter bescherming van de TBB.

Om te komen tot een categorie-indeling van de TBB dient onder andere rekening te worden gehouden met:

- het rubriceringsniveau van de informatie of van het informatiesysteem;
- de kwetsbaarheid, vervangbaarheid (schaarste) en reparatiemogelijkheden van het materieel en/of object in geval van (moedwillige) vernieling;
- de hoogte van de vervangingskosten van het materieel en/of object;
- de (imago)schade voor een (bewinds)persoon, een departement, of in extreme gevallen voor de Rijksoverheid, Nederland of bondgenoten, in geval de TBB is gecompromitteerd;
- de schade aan het milieu.

De categorieën zijn in termen van te nemen beheersmaatregelen ingedeeld van de lichtste TBB-categorie 4 in een drietal stappen naar de zwaarste categorie 1. Per TBB dient er een inschatting te worden gemaakt van impact aan de hand van de volgende drie aspecten: (Voor het VIRBI kijken we slechts/vooral naar Vertrouwelijkheid.)

- Beschikbaarheid (B)

Processen, informatiesystemen en informatie moeten beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen (de impact) als deze belangen niet beschikbaar zijn;

- Integriteit (I)
  Het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Classificatie gaat in op de mogelijke gevolgen (de impact) wanneer informatie onjuist, onvolledig is of niet actueel is;
- Vertrouwelijkheid (V)
  De bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke gevolgen (de impact) wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

Per onderwerp B, I en V dient de impact te worden ingeschat, met keuze uit vier 'scores', te weten Zeer Hoog (**ZH**), Hoog (**H**), Midden (**M**) en Laag (**L**).

De hoogste score bepaalt vervolgens de indeling in een TBB categorie.

Als voorbeeld : Bij compromittering van een Te Beschermen Belang waar er op korte of middellange termijn geen alternatieven of adequate tegenmaatregelen zijn, dan zou de schade in beginsel onacceptabel kunnen zijn. De impact kunnen we dan als HOOG inschatten. Hiermee komt de TBB in categorie 2.

2.2. Tabel A - indeling Te Beschermen Belangen (TBB)

In onderstaande tabel geven we een overzicht van de Te Beschermen Belangen op basis van impactniveau, beschikbaarheid, integriteit en vertrouwelijkheid.

TBB-categorie	**Impactniveau**	**Beschikbaarheid & integriteit (B/I)**	**Vertrouwelijkheid (V)**	**Gevolg bij compromittering**
TBB 1	Zeer hoog	Zeer ernstige schade voor de Staat. Geen alternatieven beschikbaar. Schade is onacceptabel.	Staatsgeheim ZEER GEHEIM (of equivalent)	Zeer ernstige schade aan vitale belangen van de Staat of bondgenoten. Herstel is niet of alleen met zeer grote inspanning mogelijk.
TBB 2	Hoog	Ernstige schade voor de Staat. Beperkte alternatieven beschikbaar. Schade is in beginsel niet acceptabel.	Staatsgeheim GEHEIM (of equivalent)	Ernstige schade aan vitale belangen. Herstel alleen mogelijk met grote investeringen.
TBB 3	Midden	Schade voor de Staat. Alternatieven beschikbaar. Schade moet zoveel mogelijk worden voorkomen.	CONFIDENTIEEL (of equivalent)	Nadelige impact op het functioneren van de Rijksoverheid. Herstel mogelijk met beperkte inspanning.

TBB 4	Laag	Beperkte schade voor één departement. Alternatieven beschikbaar. Schade is ongewenst.	Departementaal VERTROUWELIJK of ongerubriceerd (met merking)	Beperkt nadelig effect op het functioneren van de Rijksoverheid.

3. Hoofdstuk 3: Toelichting op context van de kwetsbaarheid m.b.t. spionage (onderdeel van risicoanalyse)

Kernvraag is in hoeverre processen en informatie(systemen) van een dienstonderdeel interessant (lees: waardevol en daarmee aantrekkelijk) zijn voor buitenlandse inlichtingendiensten of de georganiseerde criminaliteit.

Naar analogie van de TBB-bepaling geldt een zelfde indeling naar 'zwaarte' van impact in geval van compromittering, namelijk in oplopende zwaarte van LAAG, MIDDEN, HOOG tot ZEER HOOG. Waarbij deze vierpuntsschaal overeenkomt met de gangbare indeling in niveaus van vertrouwelijkheid op basis van het VIRBI 2025 en (uiteraard) de TBB inschaling.

3.1. Tabel B - Indeling TBB-categorieën

In onderstaande tabel is de relatie tussen impactniveau, TBB-categorie en rubricering weergegeven:

Impactniveau	**TBB-categorie**	**Rubriceringsniveau**	**Gevolg bij kennisname door niet-geautoriseerden**
Zeer hoog	TBB 1	Staatsgeheim ZEER GEHEIM (of equivalent)	Zeer ernstige schade aan vitale belangen van de Staat of bondgenoten.
Hoog	TBB 2	Staatsgeheim GEHEIM (of equivalent)	Ernstige schade aan vitale belangen van de Staat of bondgenoten.
Midden	TBB 3	Staatsgeheim CONFIDENTIEEL (of equivalent)	Schade aan een van de vitale belangen van de Staat of bondgenoten.
Laag	TBB 4	Departementaal vertrouwelijk (of ongerubriceerd met merking)	Schade aan de belangen van één of meerdere ministeries.

Let wel, wanneer een te beschermen belang ingedeeld is in categorie TBB 2, hoeft dit niet te betekenen dat het proces of informatiesysteem gegevens verwerkt of bevat op het niveau van STG GEHEIM. Er kunnen andere redenen zijn waarom een proces of informatiesysteem een dergelijke TBB classificering heeft gekregen.

Andersom geldt dit echter wel. Indien een proces of informatiesysteem gegevens verwerkt of bevat op het niveau van STG GEHEIM, dan is automatisch sprake van indeling in categorie TBB 2.

3.2.In de context van kernbelangen:

Beide analyses (TBB en KWAS[6]) worden uitgevoerd om inzicht te krijgen in de Te Beschermen Belangen van het onderdeel en (geaggregeerd) de Te Beschermen Belangen van het ministerie.

Bovenstaande tabel in is prima bruikbaar als kapstok maar heeft als nadeel dat de interpretatieruimte tussen 'schade', 'ernstige schade' en 'zeer ernstige schade' vrij groot is. Ook ontbreekt het aan goede voorbeelden die een nadere duiding van vertrouwelijkheid en impact zouden kunnen vergemakkelijken.

Hieronder volgt daarom een nadere toelichting met voorbeelden van (kern)belangen. De voorbeelden zijn ter illustratie en derhalve niet limitatief:

3.2.1. Kernbelang Democratische rechtsorde

Bescherming van gegevens van bewindspersonen en topambtenaren en het democratisch besluitvormingsproces met het oog op voorkennis, oneigenlijke beïnvloeding, chantage of bedreiging.

- Gegevens m.b.t. de Ministerraad en Onderraden (notulen, excerpten, besluitenlijst)
- Politieke advisering en verantwoording
- Informatie m.b.t. bewindspersonen (persoonlijke gegevens, reizen, gesprekken)
- Externe aanwezigheid bewindspersonen (optredens, evenementen, reizen)

3.2.2. Kernbelang Internationale betrekkingen

Bescherming van de positie van Nederland –voor zover het onderwerpen van het ministerie betreft– ten opzichte van andere landen in het Koninkrijk, in de EU en daarbuiten.

- Vertrouwelijke informatie van en over internationale verdragsorganisaties (EU, NATO)
- Internationale betrekkingen, bilateraal overleg met andere landen
- Gegevensuitwisseling in en met Caribisch Nederland

3.2.3. Kernbelang Veiligheid

Bescherming van gegevens die van belang zijn voor de staatsveiligheid.

- Gegevens van en over inlichtingendiensten (inlichtingenpositie, verbindingsbeveiliging, veiligheidsonderzoeken)
- Dossiers m.b.t. terrorisme, polarisatie, radicalisering, buitenlandse beïnvloeding
- Gegevens m.b.t. het Koninklijk Huis
- Gegevens over objecten met een verhoogd risico

3.2.4. Kernbelang Gevoelige beleidszaken

Bescherming van gegevens over onderwerpen die op een bepaald moment politiek (zeer) gevoelig zijn, voordat een definitief besluit is genomen, tegen voorkennis of oneigenlijke beïnvloeding.

- Persoonlijke beleidsopvattingen van de politieke en ambtelijke top;
- Politiek gevoelige beleidsdossiers (afhankelijk van de aard en actualiteit);
- Politiek gevoelige wetgevingstrajecten;
- Begrotingsvoorbereiding.

[6] Kwetsbaarheidsanalyse+spionage+20100401.pdf

3.2.5. Kernbelang Betrouwbare dienstverlening

Bescherming van de publieke dienstverlening van het ministerie waarvoor zij verantwoordelijk is en de eigen bedrijfsvoering uit oogpunt van onkreukbaarheid en betrouwbaarheid:

- Personeelsgegevens medewerkers van het ministerie en rijksbreed;
- Gegevens m.b.t. veiligheid en beveiliging van medewerkers, gebouwen en informatievoorziening;
- Gegevens over de kritieke processen, systemen en structuren (ICT infrastructuur en systemen, beveiligingsmaatregelen, cryptoverbindingen)

Deze bijlage is gebaseerd op: kwetsbaarheidsanalyse spionage – KWAS - 2014

4. 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: Toolkit ter ondersteuning implementatie van het VIRBI 2025.

20260606 v1.0