Quickscan Informatiebeveiliging

Handleiding workshop

Versie 3.0

Datum: 19 juni 2025

Documenthistorie

Versie	Datum	Toelichting	Review
1.99-a	29-03-2024	Voorstel voor een QuickScan IB in twee delen: 1. Een handleiding voor de deelnemers van de workshop 2. Verzamelstaat en tekenblad Versie 1.99-a vormt de basis voor beide delen In de handleiding en de verzamelstaat zijn teksten opgenomen voor de onderlinge verwijzingen.	Initiële versie
2.0	07-06-2024	Nieuwe versie, zonder inhoudelijke aanpassingen ter besluitvorming CISO board JenV en doorgeleiding naar CIO raad JenV	Definitief
2.1	31-12-2024	Versie 2.0 aangepast op basis van evaluaties gebruik: aanvullingen behoeven geen nadere besluitvorming – ter kennisname gemeld in CISO board en CIO raad.	Definitief
2.2	18-03-2025	Beoordeling van bedrijfskritische- en kritiek op genomen bij stap 4 Vervolgacties bij BBN3 bij stap 5 opgenomen Informatie noodzakelijk voor het juiste accreditatieproces is bij stap 1 opgenomen.	Definitief
3.0	14-05-2025	Aangepast tov Quickscan IB v3.0	Definitief
3.0	19-06-2025	CIO raad JenV ingestemd	Definitief JenV/AenM

Inhoud

Leeswijzer

Een QuickScan Informatiebeveiliging (QS-IB) bestaat uit twee documenten:

1. Een handleiding voor de deelnemers van de workshop
2. Verzamelstaat en tekenblad

Dit document is de handleiding voor de deelnemers van de workshop. Het bevat informatie over het gestructureerde verloop van de workshop, achtergrond informatie bij de verschillende kenmerken van het proces en informatiesysteem en verwijzingen naar achtergrond informatie en referenties.

Inleiding

De Quickscan Informatiebeveiliging (QS-IB) is een methodiek voor het bepalen van het basis beveiligingsniveau (BBN-toets) zoals beschreven in de BIO[1]. Voor JenV-onderdelen die onder het sturingsmodel vallen[2], geldt dat voor elk informatiesysteem periodiek ofwel een QS-IB ofwel een aanvullende risicoanalyse moet zijn uitgevoerd. geldt dat voor elk informatiesysteem een risicoanalyse in de vorm van een QS-IB moet zijn uitgevoerd. De QS-IB dient periodiek te worden getoetst op actualiteit (tenminste elke 3 jaar). De QS-IB wordt opnieuw uitgevoerd bij ingrijpende functionele en/of technische wijzigingen van het systeem of veranderingen in de context waarin het systeem wordt gebruikt of geconstateerde nieuwe (externe) dreigingen met mogelijke invloed op het systeem. De QS-IB is binnen JenV geëvolueerd van een technische systeemtoets naar een instrument voor het bepalen van risico's voor informatiebeveiliging in bredere zin. De QS-IB is in vorm en inhoud vastgesteld in de CISO Board JenV en van toepassing verklaard in de CIO-raad JenV

De uitgevoerde QS-IB biedt inzicht in de beveiligingsvereisten die vanuit de basisnorm voor IB JenV en/of verplichte bepalingen worden gesteld aan de inrichting, gebruik en beheer van het betreffende systeem of systemen. Dit gegeven het belang dat het systeem heeft voor het uitvoeren van een bedrijfsproces of -processen en de daarin verwerkte gegevens (informatieverwerking).

De uitvoering van een QS-IB is verdeeld in een aantal stappen:

Nr.	Omschrijving	Toelichting
1	Bepaal scope, context en rubricering	De QS-IB start met een inventarisatie van de scope en context van de te beschermen processen / informatie-systemen en de vastgestelde rubricering van de daarin te verwerken informatie. Het verwerken van internationaal verkregen informatie dient te worden gespecificeerd om redenen van de verplichting tot mogelijke accreditatie[3] van het systeem.
2	Classificeer proces en informatiesysteem en bepaal externe eisen	Vervolgens wordt het belang van de processen en ondersteunende informatiesystemen geclassificeerd en wordt bepaald of daar externe eisen van bijvoorbeeld de EU, de NAVO, ketenpartners of andere organisaties op van toepassing zijn.
3	Bepaal dreigingsprofiel	De verwachte bedreigingen ten aanzien van het informatiesysteem en de (soort) actoren die deze veroorzaken, worden vastgelegd in een dreigingsprofiel.
4	Bepaal wat de te stellen betrouwbaarheidseisen zijn voor het systeem (B,I en V) i.r.t. het proces waarvoor het systeem wordt ingezet: geef aan wat daarbij de risico' s zijn en te treffen passende maatregelen.	Op basis van een inschatting van de maximale schade die kan ontstaan voor het proces, wordt het niveau van "Beschikbaarheid", "Integriteit" en "Vertrouwelijkheid" bepaald. Dit wordt beargumenteerd op basis van vastgestelde risico's en (mogelijke) impact ervan voor het proces als het risico zich manifesteert.

[1] Baseline Informatiebeveiliging Overheid (BIO) versie 1.04vz

[2] Sui Generis en ZBO's kennen deze verplichting niet. ZBO's en Sui Generis worden ten zeerste aangeraden een risico analyse uit te voeren op de Informatie beveiliging waarbij deze QuickScan Informatie Beveiliging als handreiking gebruikt kan worden.

[3] Beleid accredidatie informatiesystemen JenV/AenM.

Nr.	Omschrijving	Toelichting
	Bepaal of er sprake is van een bedrijfskritisch of kritiek systeem.	In geval het systeem een bedrijfskritisch of kritiek systeem is dient dit te worden gemeld bij de departementale CISO. Het systeem wordt opgenomen in het departementale register van bedrijfskritische en kritieke systemen
5	Bepaal het passende BBN Stel vast of een aanvullende risico analyse nodig is.	Vervolgens wordt op basis van de eerder gedane keuzes in stappen 2, 3 en 4 het BBN gekozen op basis van een stroomschema. In geval van BBN3 is de BIO ontoereikend: er is een aanvullende risicoanalyse noodzakelijk om aanvullende te treffen maatregelen te bepalen (vervolgactie).
6	Samenvatting resultaten, beoordeling van de maatregelen en aandachtspunten.	De uitkomst van alle analyses en beoordelingen worden samengebracht in een overzicht voor de eigenaar. Vervolgens wordt bepaald welke basismaatregelen van toepassing zijn, welke additionele (cloud)risico's en bijbehorende maatregelen van toepassing zijn en/of er sprake is van een (rest)risico aanwezig is. Dit (rest)risico wordt vervolgens -waar mogelijk- afgezet tegen de risicobereidheid van de organisatie die verantwoordelijk is voor het onderhavige proces en de ondersteunende systemen. Het geheel wordt helder beargumenteerd.
7	Laat de QS-IB en het restrisico vaststellen door de eigenaar	Tenslotte verklaren de proces- en systeemeigenaar over hetgeen is vastgesteld het eens te zijn met de bepaling van de controls en maatregelen in de risicoafweging.

Het resultaat van de QS-IB is een rapportage die de keuze voor het toe te passen BBN en de eventueel aanvullend te implementeren maatregelen toelicht. Eventuele (rest)risico's worden – waar mogelijk- afgezet tegen de risicobereidheid van de proces eigenaar. De proces- en systeemeigenaar stelt deze rapportage formeel vast. Deze wordt vervolgens periodiek, minimaal eens per 3 jaar, herijkt of bij een significante wijziging van het proces of de systemen.

Werkwijze QS-IB

Waarvoor is deze QS-IB geschikt?

De QS-IB kan worden gebruikt om het basis beveiligingsniveau (BBN) te bepalen. Het is een efficiënte en laagdrempelige manier om vast te stellen of een proces en/of systemen voldoende beveiliging hebben aan BBN1 of BBN2 in de BIO. In dit proces wordt tevens gekeken naar toegepaste maatregelen. Bij de vaststelling van eventuele restrisico's wordt in stap 6 een beoordeling gevraagd van getroffen of nog te treffen maatregelen waardoor mogelijk een restrisico overblijft. Bij de inzet van cloud-technologie is het deployment model (bv. public, private, en hybride[4]) bepalend welke maatregelen getroffen moeten worden.

Een QS-IB wordt in principe uitgevoerd voor één informatiesysteem dat één of meer bedrijfsprocessen ondersteunt. Zo blijft de scope overzichtelijk. Wanneer processen en/of systemen nauw gerelateerd zijn aan elkaar en voldoende onderscheiden kunnen worden, dan kan de QS-IB ook worden toegepast op meerdere processen en systemen tegelijkertijd. Het uitgangspunt is dan wel dat de zwaarste beveiligingseisen bepalend zijn voor de onderzochte set van systemen en/of processen binnen de scope. In die situatie kan overal in de QS-IB waar de termen 'informatiesysteem' en het daaraan gerelateerde 'proces' zijn gebruikt, ook het meervoud daarvan gelezen worden.
Andersom kan er ook een QS-IB worden uitgevoerd op slechts één of enkele gedeeltes van één informatiesysteem.

Na uitvoering van de QS-IB wordt een uitgebreide risicoanalyse (bv. op basis van IRAM) uitgevoerd wanneer er sprake is van één of meer van de volgende situaties:

- BBN2 geeft onvoldoende weerbaarheid voor het gekozen dreigingsbeeld;
- Departementaal Vertrouwelijke informatie waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threats (APT's), die uitgaat van statelijke actoren en beroepscriminelen;
- Staatsgeheime informatie, dus vanaf STG Confidentieel.

Stappenplan

Stap 1: Bepaal scope, context en rubricering;
Stap 2: Classificeer proces en informatiesysteem en bepaal externe eisen;
Stap 3: Bepaal dreigingsprofiel;
Stap 4: Bepaal betrouwbaarheidseisen (B, I en V) en het belang van het systeem;
Stap 5: Bepaal het passende BBN;
Stap 6: Leg resultaten en aandachtspunten vast, beoordeel de maatregelen en stel eventuele risico's vast;
Stap 7: Laat de QS-IB en het restrisico vaststellen door de eigenaar.

Uitvoering

Idealiter wordt de QS-IB uitgevoerd in de vorm van één of meerdere workshops.
In voorbereiding op de QS-IB is het verstandig om te beschikken over het uitgewerkte procesmodel van het proces binnen scope en de (infra)technische architectuur van het systeem binnen scope. Deze worden gedeeld met de deelnemers aan de workshop i.c. de uitwerking van de QS-IB.

Het is hierom dat ter voorbereiding de workshop-begeleider de scope (welke processen en informatiesystemen zijn binnen scope van de QS-IB), context en rubricering (stap 1) afstemt met de opdrachtgever, zodat deze enkel gevalideerd hoeft te worden in de workshop. Zie ook bijlage 1.

[4] Een compleet overzicht van verschillende cloud deployment modellen:
https://en.wikipedia.org/wiki/Cloud_computing#Deployment_models

De QS-IB wordt uitgevoerd met de eigenaren van het (de) business proces(sen) en het (de) bijbehorende informatiesyste(m)en, materiedeskundigen op het gebied van het (de) business proces(sen) en van het (de) informatiesyste(m)en.
Deze ontvangen vooraf de resultaten van stap 1.

Tijdens de QS-IB wordt per beveiligingsaspect geschat wat de maximale impact (‘worst case’) van een incident is voor een organisatie, als door dat incident de informatie in - of de werking van - een informatiesysteem wordt aangetast.

Een handleiding voor het uitvoeren van de QS-IB door het organiseren van een workshop is opgenomen als bijlage 1. Beperk u in de definitieve versie tot de feitelijke relevante informatie. Indien bijvoorbeeld gekozen wordt voor Hoog, verwijder dan de rijen voor Laag en Midden. Beargumenteer gemaakte keuzes altijd duidelijk zodat er achteraf, bijvoorbeeld bij periodieke herijking van de QS-IB, daarover geen discussie ontstaat en helder is waarom een bepaalde keuze is gemaakt.

Stap 1: Bepaal scope, context en rubricering

Stap 1 van de QS-IB beschrijft de wijze waarop de scope en de context worden bepaald en biedt ruimte om de door de proces- of systeemeigenaar vastgestelde rubricering vast te leggen. In deze stap gaan de procesbegeleider en de eigenaren van het proces en het informatiesysteem de workshop voorbereiden. Tevens dienen zij vooraf de soorten gegevens met bijbehorende rubricering voorlopig te inventariseren. Hierbij moet in ieder geval het resultaat van de eerder uitgevoerde DPIA meegenomen worden, zie ook bijlage 2. De resultaten van stap 1 worden vooraf naar de deelnemers verzonden, zodat de deelnemers die tijdens de QS-IB workshop kunnen valideren.
De resultaten van de rubricering zijn input voor het bepalen van het BBN in stap 5.

Scope

Bepaal de scope van de QS-IB: welk (deel)processen en welke informatiesystemen betreft het?
De scope kan uitgaan van:
- Eén proces met een of meerdere ondersteunende systemen,
- Eén informatiesysteem dat één of meerdere processen ondersteunt, of
- Meerdere gerelateerde informatiesystemen die meerdere soortgelijke processen ondersteunen.

Geef in tabellen 1a en 1b in de verzamelstaat aan welke (deel)processen met ondersteunende systemen tot de scope van de analyse behoren.

Context

Vul **per proces** dat tot de scope behoort, tabel 1c in. Vallen meerdere processen onder de scope dan dient per proces een tabel ingevuld te worden. In stap 3 worden proces gerelateerde dreigingen en (mogelijke) risico's nader uitgewerkt.

Vul **per informatiesysteem,** dat tot de scope behoort, tabel 1d in. Als er meerdere informatiesystemen onder de scope vallen dan dient per informatiesysteem een tabel ingevuld te worden. In stap 3 worden systeem technische dreigingen en (mogelijke) risico's nader uitgewerkt.

Rubricering en privacy classificatie

Geef in tabel 1e **per informatiesysteem** het rubriceringsniveau aan zoals in het VIR-BI is gegeven. Als hulpmiddel kan hier de *Handleiding Rubricering*[5] worden gebruikt. Als er meerdere soorten informatie in de informatiesystemen worden verwerkt, dan dient per soort informatie het rubriceringsniveau te worden vermeld. Geef ook hier een duidelijke argumentatie voor het gekozen niveau. N.B. de hoogste privacy classificatie bepaald de uiteindelijke rubricering van het systeem.

Gebruik de informatie uit de eerder uitgevoerde DPIA[6] [7] [8] [9]voor tabel 1f.

[5] https://rijksportaal.overheid-i.nl/organisaties/rijksbreed/nieuws/2024/01/omgaan-met-vertrouwelijke-info.html

[6] Let op: naast de AVG zijn (mogelijk) meerdere wetten van toepassing (Wpg, Wjsg, etc.).

[7] Gegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gezondheid, en seksueel gedrag of seksuele gerichtheid, alsmede genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon.

[8] Gegevens over de financiële situatie van de betrokkene; gegevens die betrekking hebben op kwetsbare groepen; gegevens die kunnen worden misbruikt voor (identiteits)fraude; gebruikersnamen, wachtwoorden en andere inloggegevens; (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene; en communicatie- en locatiegegevens.

[9] Burgerservicenummer (BSN), BIG-nummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer, kenteken.

NB: wees zorgvuldig bij het duiden van de soorten gegevens. Deze duiding wordt in stap 3 gebruikt om de dreigingen (al of niet van statelijke actoren) in beeld te brengen. Denk bijvoorbeeld aan statelijke actoren die geïnteresseerd zijn in seksuele geaardheid, geloofsovertuiging, familiaire achtergrond, etc.

Internationaal verkregen informatie
Gebruik tabel 1g om internationaal verkregen informatie te duiden die verwerkt wordt in de informatiesystemen. Zie voetnoot 18 en 19 voor een duiding van de verschillende soorten internationaal verkregen informatie.

NB: wees zorgvuldig bij het duiden van internationaal verkregen informatie. Deze duiding bepaalt hoe de accreditatie van het informatiesysteem moet verlopen. Niet duiden van internationaal verkregen en gebruikte informatie kan leiden tot een eenzijdig stoppen van uitwisseling van informatie. De rubricering van internationaal verkregen of gedeelde informatie is een verantwoordelijkheid van de eigenaar de informatie. De rubricering van de internationale informatie is altijd vermeld op het document of bekend gemaakt bij de uitwisseling.

Classificatie overige gevoelige gegevens
NB: in geval er aanvullende gegevens/data worden vastgesteld die niet eerder in de DPIA zijn meegenomen dan dient dit te worden vermeld. Gebruik tabel 1h om overige nog niet geïdentificeerde gevoelige gegevens te benoemen.
Geadviseerd wordt om deze tabel te toetsen bij de privacy officer (PO) om redenen van mogelijk aanvullende eisen te stellen aan het systeemgebruik of -beheer vanuit privacy wetgeving.

Is het VIR-BI van toepassing, dan moeten de bij het rubriceringsniveau behorende maatregelen uit dit voorschrift worden geïmplementeerd. Kortheidshalve wordt hier verwezen naar de tekst van het VIR-BI[10] en de *Handleiding Rubricering*. Indien gebruik wordt gemaakt van een Cloud leverancier, dienen tevens de eisen voortkomend uit het *Cloud Afwegingskader* in overweging te worden genomen.

De Autoriteit Persoonsgegeven (AP) geeft op de eigen website een duidelijke uiteenzetting van de verschillende soorten persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens

[10] https://wetten.overheid.nl/BWBR0033507/2013-06-01

Stap 2: Classificatie en externe eisen van de processen en informatiesysteem

De resultaten van deze stap zijn input voor het bepalen van het belang van het informatiesysteem in stap 4. Classificatie van processen

Voor het realiseren van de doelstellingen van de organisatie moeten de bedrijfsprocessen goed functioneren. Ieder proces wordt geclassificeerd naar de mate van belang. In onderstaande tabel worden de classificaties weergegeven.

Classificatie: Ondersteunend	**Taak: Voorwaardenscheppend**
De activiteiten waaraan de typering 'handig om te hebben' kan worden toegekend. Deze activiteiten hebben geen directe relatie met het voortbrengen van de producten / diensten waaraan de instelling haar bestaansrecht ontleent. In de meeste gevallen is hier sprake van een ondersteunende rol naar de lijn. De activiteiten vormen een waardevolle support van het primaire proces.	

Classificatie: Bijdragend	**Taak: Subtaak**
Er is slechts sprake van een indirecte relatie met de hoofdactiviteiten van de organisatie. Het ontbreken echter van het 'bijdragende proces' heeft echter wel effectiviteits- en efficiencyverliezen binnen het primaire proces tot gevolg.	

Classificatie: Strategisch	**Taak: Afgeleide kerntaak**
Het proces heeft een directe relatie met het realiseren van de doelstellingen van organisatie en heeft een of meer van de volgende kenmerken: - Een aanzienlijk deel (50% - 80%) van het te besteden budget komt ten goede aan dit proces. - Het proces heeft te maken met de uitvoering van wettelijke taken (het betreft hier primaire processen met wettelijk / contractueel vastgelegde termijnen). - Het proces wordt in de toekomst strategisch door voorzienbare veranderingen in de strategische doelstellingen van de organisatie.	

Classificatie: Kritisch strategisch	**Taak: Kerntaak**
In relatie tot de doelstellingen van de organisatie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop de organisatie direct kan worden aangesproken. De organisatie ontleent haar bestaansrecht aan het uitvoeren van deze taken. Het proces heeft een of meer van de volgende kenmerken: - Het betreft een maatschappelijk vitaal proces. Deze vitale belangen zijn als volgt gedefinieerd: a. territoriale veiligheid: het ongestoord functioneren van Nederland als onafhankelijke staat, en in het bijzonder de territoriale integriteit van het grondgebied en de internationale positie of; b. fysieke veiligheid: het ongestoord kunnen functioneren als mens in Nederland; c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie of; d. ecologische veiligheid: het beschikken over voldoende zelf herstellend vermogen van de leefomgeving bij aantasting of; e. sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden. - De instelling krijgt 80% of meer van de inkomsten uit dit proces, c.q. het budget van de organisatie wordt voor meer dan 80% uitgeput door dit proces of: - Als de activiteit langer dan één week stilvalt of niet goed verloopt, heeft dit ernstige gevolgen voor het voortbestaan van de organisatie.	

De gekozen classificatie van processen wordt samen met een onderbouwing beschreven in tabel 2a.

Inventarisatie en classificatie van informatiesystemen

Om een proces goed te kunnen laten functioneren zijn er een of meer informatiesystemen die dat proces ondersteunen. De onderstaande tabel biedt een overzicht van de classificatie van een informatiesysteem die aangeeft hoeveel waarde men hecht aan dat informatiesysteem als ondersteuning van het proces.

Typering	Waardering
Nuttig (N)	- Het informatiesysteem geeft support bij de activiteiten binnen het bedrijfsproces en i 'handig om te hebben'.
Belangrijk (B)	Het informatiesysteem heeft een of meer van de volgende kenmerken: - Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en / of de levering van de producten of diensten of; - Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk of; - Inzet van het informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie of; - Het informatiesysteem wordt door veel (interne / externe) medewerkers / burgers gebruikt of; - Het systeem is onderdeel van processen in een keten.
Vitaal (V)	Het informatiesysteem heeft een of meer van de volgende kenmerken: - Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten / diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem of; - Inzet van het informatiesysteem is essentieel voor een goede uitvoering van het bedrijfsproces of; - Het systeem is essentieel voor uitvoering van processen in een keten.

Geef in tabel 2b **per informatiesysteem** (IS) aan in hoeverre het bedrijfsproces afhankelijk is van het ondersteunende informatiesysteem / de informatiesystemen.

Bepaal externe beveiligingseisen

Geef in tabel 2c **per informatiesysteem** aan welke (externe) beveiligingseisen[11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24]externe partijen daar aan stellen (denk bv. aan inschaling op BBN3). Houd hierbij ook rekening met informatiesystemen die in de Cloud worden gehost door externe partijen. De eisen kunnen betrekking hebben op het proces, de informatiestromen of de ondersteunende systemen. De eisen worden per informatiesysteem toegepast.

NB: Vermeld in deze tabel (2c) ook de voorgenomen maatregelen uit de DPIA van het informatiesysteem!

---

[11] https://www.forumstandaardisatie.nl/open-standaarden is een overzicht van alle standaarden waar rijksoverheden aan gehouden zijn.

[12] Min JenV - Cloud afwegingskader JenV v1.2.pdf (samenwerkruimten.nl)

[13] Cloud Security and Privacy Framework - Alle documenten (samenwerkruimten.nl)

[14] wetten.nl - Regeling - Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) - BWBR0033507 (overheid.nl)

[15] https://www.nbu.cz/download/AC_35-D_2002_REV5_znackaNBU.pdf

[16] https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/

[17] https://bio-overheid.nl/

[18] https://eur-lex.europa.eu/eli/dir/2022/2555. Een vertaling naar de Nederlands wet en regelgeving is op het moment van verschijnen van de QS-IB nog in de maak.

[19] https://wetten.overheid.nl/BWBR0040940/2021-07-01

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[21] https://wetten.overheid.nl/BWBR0022463/2023-11-01

[22] https://wetten.overheid.nl/BWBR0014194/2023-11-01

[23] https://www.forumstandaardisatie.nl/open-standaarden is een overzicht van alle verplichte en aanbevolen standaarden voor de rijksoverheden.

[24] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

Stap 3: Dreigingsprofiel

De resultaten van deze stap zijn input voor het bepalen van het BBN in stap 5.

Opgetreden beveiligingsincidenten[25]

Om het dreigingsprofiel te bepalen is het nuttig informatie te verzamelen over eventueel opgetreden beveiligingsincidenten. Kijk vooral naar 'ernstige' incidenten. Dit kan door een lijst met recente (beveiligings)incidenten samen te stellen (o.a. bij de Servicedesk op te vragen) en deze te analyseren op de volgende punten:

- Media exposure (belang van het incident);
- Hoe is het incident ontstaan (bijv. niet eerder onderkende dreiging en maatregelen niet aanwezig of ineffectief);
- Welke gegevens verwerkt het ondersteunde proces / ondersteunende systeem (bijvoorbeeld financiële gegevens, persoonsgegevens)
- Hoe interessant zijn die gegevens voor specifieke doelgroepen en zijn die te identificeren als (be)dreiging.

Beschrijf in tabel 3a de verschillende opgetreden beveiligingsincidenten.

Dreigingsprofiel

*Sluit bij het opstellen van het dreigingsprofiel **geen** dreigingen uit waarvoor een mitigerende maatregel al eerder binnen JenV is geïmplementeerd, of waarvoor de organisatie voornemens is om een mitigerende maatregelen te treffen. Immers ook deze dreigingen zijn opportuun voor het profiel.*

*Ga tevens uit van **welbewuste, intentionele**[26] dreiging.*

[25] Deze subparagraaf is vanzelfsprekend alleen relevant bij reeds bestaande systemen

[26] Intentioneel in die zin dat het hier niet gaat om toevallige "bijvangst" van een kwaadwillende actor, maar dat deze actor welbewust het betreffende systeem wil compromitteren.

Actor / actie / informatie	**Score dreigingsprofiel**[27]

• Systeem / proces bevat maximaal DepV informatie en/of
• Activiteiten zoals hacken, malware aanval:
  ○ Kwaadwillende medewerker, burger, actiegroepen
  ○ Crimineel opportunist (bv. kleine partijen die ransomware-aanvallen uitvoeren)
  ○ Contractor / inhuurkracht
  ○ Gelegenheidscriminelen, script kiddies en/of
• Activiteiten door Statelijke actoren of Beroepscriminelen zoals phishing, doch niet per se gericht op JenV en/of
• De toegang tot het systeem (in de Cloud of on premise) is beperkt tot medewerkers van de leverancier van de dienst, of wel vanaf een managed device van een IDVG-dienstverlener (waaronder JIO of SSC-ICT), of wel vanaf een unmanaged device vanuit een virtual desktop (waaronder Citrix) en/of
• Indien het systeem wordt afgenomen als SAAS oplossing en de proceseigenaar beschikt over een dekkende Assuranceverklaring (ISAE3402 / SOC2 / ISAE3000 rapportage[28] [29]).
	'Normaal'

• Systeem / proces bevat STG-Confidentieel informatie of hoger en/of
• *Advanced Persistent Threat*s
  ○ Terreurgroep
  ○ Inlichtingendienst
  ○ Georganiseerde criminaliteit
  ○ Specifiek op JenV gerichte aanvallen door Statelijke actoren of Beroepscriminelen en/of
• Het systeem draait in de cloud, en heeft de volgende kenmerken:
  ○ bevat Dep-V informatie of hoger en
  ○ draait niet conform vastgestelde generieke dienstverlening van een Shared Service Center, dan wel is niet afgenomen in afstemming met Strategisch Leveranciers Management Rijk voor de betreffende cloud provider en/of
• Toegang tot de beheerfuncties van het systeem is mogelijk via internet, of in ieder geval niet beperkt tot Justitienet.
	'Hoog'

- *Bronnen van dreigingen: Over de bedreiging die mogelijke actoren vormen, kan actuele informatie worden gehaald uit bijvoorbeeld het Cyber Security Beeld Nederland (CSBN) dat het NCSC jaarlijks publiceert.*
- *Specifiek voor dreigingen in de cloud: zie het Cloud Security en Privacy Framework*[30]

Onderbouw in tabel 3b de gekozen dreigingen en dreigers.

[27] De score is afgeleid van de definitie BBN's, zie bijlage 2 van de BIO
[28] https://isae3402.nl/
[29] https://www.tuv.nl/nl/diensten/isae-3000/
[30] Cloud Security and Privacy Framework - Alle documenten (samenwerkruimten.nl)

Stap 4: Eisen aan Betrouwbaarheid, Integriteit en Vertrouwelijkheid

In deze stap worden ten aanzien van het proces de betrouwbaarheidseisen "Beschikbaarheid", "Integriteit" en "Vertrouwelijkheid", bepaald aan de hand van de schadescenario's uit bijlage 2 van de BIO. Als voor de aspecten "Beschikbaarheid" en "Integriteit" ernstigere schade dan de bij "Midden" beschreven schadescenario's aan de orde kan zijn, dan wordt daarvoor de waarde "Hoog" toegekend.

Tevens worden in deze stap de RTO (Recovery Time Object) en de RPO (Recovery Point Object) vastgesteld. RTO geeft de doelstelling aan wat de maximale hersteltijd is na uitval (hoe snel moet de dienst weer beschikbaar zijn?). RPO geeft de doelstelling aan van het herstelpunt; het maximaal toelaatbare dataverlies na uitval (hoeveel uren/dagen aan data mag er verloren gaan?).

De resultaten van deze stap zijn input voor het bepalen van het BBN in stap 5.

NB.: Als een systeem uit meerdere onderdelen bestaat die uiteenlopende betrouwbaarheidsniveaus kennen, vul dan één tabel per onderdeel in!

Beschikbaarheid

Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen) (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Categorie	Maximale schade
Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie; leidt nog niet uit het niet verkrijgen van een accountants verklaring; en/of - beperkt verlies van management control; en/of - irritatie en ongemak bij burgers geventileerd in de media; en/of - interne negatieve publiciteit (imagoschade). Beschikbaarheid Laag wordt als volgt gekwantificeerd in bijlage 2 van BIO: - Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden - een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. - Maximaal dataverlies 28 uur. - Maximale hersteltijd in geval van incidenten is binnen 40 werkuren - (vijf werkdagen van 8 uur) in 85% van de gevallen.

Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; en/of - diplomatieke schade te herstellen door ambtelijke opschaling; en/of - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie; geen accountantsverklaring afgegeven; en/of - belangrijk verlies van management control; en/of - verlies van publiek respect; klachten van burgers; en/of - Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. Beschikbaarheid Midden wordt als volgt gekwantificeerd in bijlage 2 van de BIO: - Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; - maximaal dataverlies 24 uur; - maximale hersteltijd bij incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Hoog	Significant ernstigere schade dan het bij "Midden" beschreven schadescenario. De beschikbaarheidseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken.

Gebruik tabel 4a voor een beschrijving van het gekozen beschikbaarheidsniveau.

Integriteit

Integriteit betreft het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan. De juistheid en volledigheid van de informatie is een directe verantwoordelijkheid van de eigenaar van het informatiesysteem (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Categorie	Maximale schade
Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen. Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie; leidt nog niet tot het niet verkrijgen van een accountants verklaring; en/of - beperkt verlies van management control; en/of - irritatie en ongemak bij burgers geventileerd in de media; of interne negatieve publiciteit (imagoschade).
Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; en/of - diplomatieke schade te herstellen door ambtelijke opschaling; en/of - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie; en/of - geen accountantsverklaring afgegeven; en/of - belangrijk verlies van management control; en/of - verlies van publiek respect; klachten van burgers; en/of - Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.

Hoog	• Ernstigere schade dan het bij "Midden" beschreven schadescenario. De integriteitseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken. • Wijzigen van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3.

Gebruik tabel 4b voor een beschrijving van het gekozen beschikbaarheidsniveau

Vertrouwelijkheid

Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de gebouwen, de informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, trojan horses). En het gaat ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Categorie	Maximale schade
Laag	Kennisname van informatie door ongeautoriseerde medewerkers en buitenstaanders is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: - financiële gevolgen: op te vangen binnen de begroting van de organisatie; en/of - irritatie en ongemak bij burgers geventileerd in de media; en/of - interne negatieve publiciteit (imagoschade).
Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst[31], waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; en/of - diplomatieke schade te herstellen door ambtelijke opschaling; en/of - financiële gevolgen: niet meer op te vangen binnen de begroting van de organisatie; geen accountantsverklaring afgegeven; en/of - verlies van publiek respect; klachten van burgers of significant verlies van - motivatie van medewerkers; en/of - bindende aanwijzing van de AP in verband met schending van de privacy; en/of - directe imagoschade, bijvoorbeeld door negatieve publiciteit.
Hoog	- Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; - informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); en/of - aansluiting op een infrastructuur vereist BBN3 om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen); en/of - weerstand tegen statelijke actoren is noodzakelijk.

Gebruik tabel 4c voor een beschrijving van het gekozen vertrouwelijkheidsniveau.

Gebruik tabel 4d voor een samenvatting van de beoordeling van de BIV eisen.

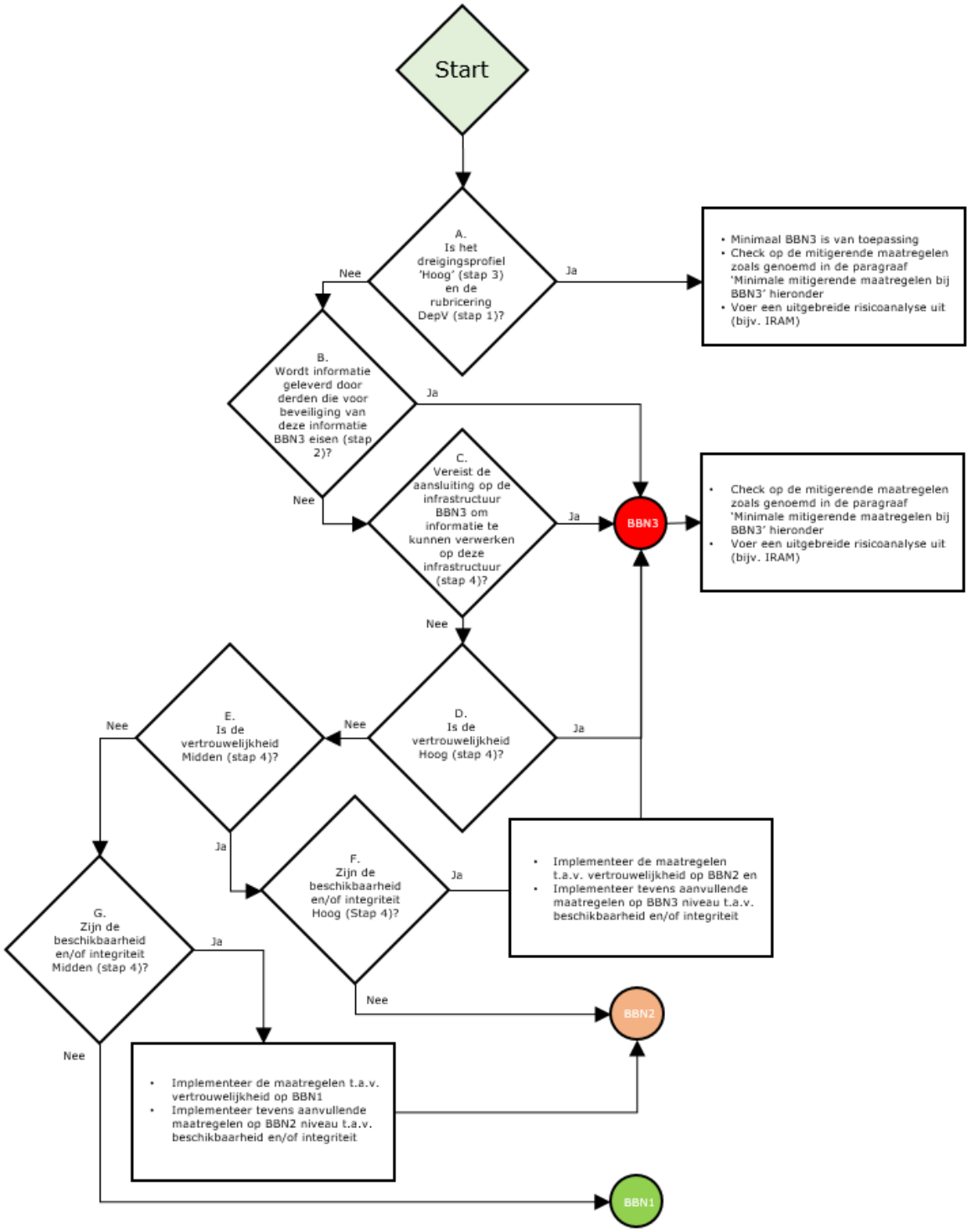
Gebruik tabel 4e voor het bepalen van het belang van het informatiesysteem aan de hand van eerder in de QS-IB bepaalde meta data

Gebruik de informatie uit tabellen 2a, 2b, 4a, 4b, 4c en 4d om te beoordelen of een informatiesysteem bedrijfskritisch of kritiek is. Gebruik tabel 4e om de beoordeling vast te leggen.

[31] In de zin van de VIR-BI

Stap 5: Basis Beveiligingsniveau (BBN)

In deze stap worden het BBN-niveau en eventuele vervolgacties bepaald aan de hand van de volgende flowchart:



Gebruik tabel 5 voor de uitkomst

Minimale mitigerende controls en maatregelen bij BBN3[32]

Als BBN3 van toepassing is, moet er altijd een uitgebreide risicoanalyse worden uitgevoerd. Maak bij deze risico analyse ook gebruik van de BBN3 Aanpak JenV[33]. Onderstaand volgt het overzicht van maatregelen die bij BBN3 feitelijk dienen te worden geïmplementeerd of tenminste dienen te worden getoetst op van toepassing zijnde. Dit zijn maatregelen die bij BBN3 nog belangrijker worden dan bij BBN2: waar *comply or explain* bij BBN2 kan worden toegepast geldt voor deze maatregelen dat bij BBN3 de mogelijkheid van *explain* ten zeerste wordt onraden.

Control-/ Maatregelnr.	Soort maatregel	Omschrijving
BIO-8.1.1	Beheer van bedrijfsmiddelen	Inventariseren van bedrijfsmiddelen: Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.
BIO-9.1.2/1	Toegangsbeveiliging	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
BIO-9.1.2/2	Toegangsbeveiliging	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.
BIO-11.1.4/1	Fysieke beveiliging	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.
BIO-11.1.4/2	Fysieke beveiliging	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.
BIO-12.2.1/3	Beveiliging bedrijfsvoering	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
BIO-12.2.1/5	Beveiliging bedrijfsvoering	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.
BIO-12.3.1/3	Beveiliging bedrijfsvoering	In het back-upbeleid staan minimaal de volgende eisen: a. Dataverlies bedraagt maximaal 28 uur. b. Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.
BIO-12.3.1/4	Beveiliging bedrijfsvoering	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
BIO-12.3.1/5	Beveiliging bedrijfsvoering	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.
BIO-12.6.2/1	Beveiliging bedrijfsvoering	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).

[32] Gebaseerd op expert inschatting JenV/DII/IB zomer 2022.

[33] https://www.samenwerkruimten.nl/teamsites/cisoteamjenv/Documenten/WG%20BBN3/BBN3%20aanpak%20JenV%20v1.1.docx?d=w61d503f4160e4ce0807caf29c552af21

Control-/ Maatregelnr.	Soort maatregel	Omschrijving
BIO-13.1.3	Communicatiebeveiliging	Scheiding in netwerken: Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
BIO-14.2.8	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Testen van systeembeveiliging: Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
BIO-15.2.1/1	Leveranciersrelaties	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.
BIO-17.1.1	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Informatiebeveiligingscontinuïteit plannen: De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.
BIO-17.1.2	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Informatiebeveiligingscontinuïteit implementeren: De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
BIO-17.1.3/1	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.
BIO-17.1.3/3	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.
BIO-18.2.1/1	Naleving	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.

Mogelijk aanvullende mitigerende maatregelen bij BBN3[34]

Hieronder staan maatregelen die bij BBN3 aanvullend genomen kunnen worden t.o.v. de hierboven genoemde maatregelen. De lijst maatregelen hieronder is primair bedoeld als keuzelijst en bedoeld om reeds geïmplementeerde maatregelen te versterken en/of noodzakelijk geacht gezien de eerder in de quickscan onderkende specifieke dreigingen en risico's voor proces en/of systeem in scope.

Maatregelnr.	Soort maatregel	Omschrijving
RKJV-A3	Management van bedrijfsmiddelen en -informatie	Alle middelen om gerubriceerde informatie mee te verwerken en de personen aan wie deze zijn uitgereikt staan geregistreerd.
RKJV-A4	Management van bedrijfsmiddelen en -informatie	De locatie/standplaats van alle middelen en de toewijzing aan een eigenaar zijn geregistreerd.
RKJV-A7	Management van bedrijfsmiddelen en -informatie	Thuiswerken met staatsgeheimen is alleen toegestaan op apparatuur die na goedkeuring door de BVA ter beschikking gesteld is. Het is verboden privéapparatuur voor verwerking van staatsgeheime informatie te gebruiken.
RKJV-A10	Management van bedrijfsmiddelen en -informatie	Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.
RKJV-A11	Management van bedrijfsmiddelen en -informatie	Alleen apparatuur die door de BVA zijn goedgekeurd mogen een ruimte waar staatsgeheime informatie worden verwerkt/besproken betreden.
RKJV-A12	Management van bedrijfsmiddelen en -informatie	Thuiswerken met Departementaal Vertrouwelijke informatie is alleen toegestaan op door de BVA's geaccrediteerde voorzieningen zoals Citrix.
RKJV-A17	Management van bedrijfsmiddelen en -informatie	Via telewerkvoorzieningen mogen geen staatsgeheimen verwerkt worden en de voorzieningen zijn zodanig ingericht dat er geen toegang tot staatsgeheimen mogelijk is.
RKJV-B4	Personele beveiligingsmaatregelen	Personen die frequent te maken hebben met bijzondere informatie dienen tevens te beschikken over een passende verklaring.
RKJV-B5	Personele beveiligingsmaatregelen	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn minimaal in het bezit van een VGB op B-niveau niet ouder dan 5 jaar.
RKJV-B6	Personele beveiligingsmaatregelen	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op minimaal C-niveau niet ouder dan 5 jaar.
RKJV-C2	Fysieke beveiligingsmaatregelen	Het compartiment met een Te Beschermen Belang (TBB) bevindt zich in een zone die met toegangscontrole is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.
RKJV-C5	Fysieke beveiligingsmaatregelen	Fysieke toegang tot het compartiment met een TBB is tot op individueel niveau controleerbaar.
RKJV-C8	Fysieke beveiligingsmaatregelen	Toegang tot het TBB of compartiment is alleen door middel van Two-factor Authenticatie verleend.
RKJV-C9	Fysieke beveiligingsmaatregelen	Alleen een geautoriseerd persoon kan zelfstandig toegang krijgen tot een TBB of tot een compartiment waarin zich een TBB bevindt.
RKJV-C11	Fysieke beveiligingsmaatregelen	Bezoekers worden begeleid wanneer zij ruimten, waarin bijzondere informatie aanwezig is, betreden.

[34] De maatregelnummering verwijst naar het *Rubriceringskader Ministerie van Justitie en Veiligheid*, dd. 26-07-2021 (afgekort RKJV).

Maatregelnr.	Soort maatregel	Omschrijving
RKJV-C13	Fysieke beveiligingsmaatregelen	Bezoekers (en de 'bezoek-verantwoordelijke') worden geregistreerd indien zij toegang (kunnen) hebben tot bijzondere informatie in ruimten die zij betreden, als de toegang tot die informatie niet op andere wijze kan worden voorkomen (bv kast/kluis/etc.). Aanwezigen zonder zichtbare pas worden behandeld als bezoekers (i.r.t. medewerkers die hun medewerkerspas niet zichtbaar dragen).
RKJV-C16	Fysieke beveiligingsmaatregelen	Er zijn voorzieningen getroffen om elektronische apparatuur die niet strikt noodzakelijk zijn voor het uitvoeren van werkzaamheden buiten de compartimenten te houden.
RKJV-C18	Fysieke beveiligingsmaatregelen	De sterkte van het opbergmiddel is gerelateerd aan de rubricering en de interventietijd
RKJV-C19	Fysieke beveiligingsmaatregelen	Opbergmiddelen tot 1000 kilogram zijn chemisch veranker
RKJV-C20	Fysieke beveiligingsmaatregelen	Opbergmiddelen zijn voorzien van een sleutelslot en een cijfercombinatieslot
RKJV-C22	Fysieke beveiligingsmaatregelen	Locaties waar zich een opeenstapeling van staatsgeheimen bevinden en waar sprake is van enige concrete dreiging, worden na instemming van de BVA's bij KB aangewezen als verboden plaats. De aanwijzing wordt met redenen omkleed en gaat vergezeld met kadastrale omschrijving van het perceel. Bij de ingangen zijn borden geplaatst waarop vermeld wordt dat de locatie een verboden plaats is, alsmede dat de toegang voor onbevoegden en opnameapparatuur verboden is.
RKJV-D2	Bouwkundige beveiligingsmaatregelen	Daar waar bestaande bouwkundige normeringen niet bekend zijn, moet de uitsteltijd worden vastgesteld aan de hand van beproevingen c.q. analyses om het weerstandsvermogen (in tijd) tegen door potentiële daders gebruikte aanvalsmethoden en -middelen te toetsen.
RKJV-D3	Bouwkundige beveiligingsmaatregelen	Ramen en gevelopeningen die open kunnen, zijn voorzien van braak werend glas, hang- en sluitwerk, sponningen enzovoorts.
RKJV-D4	Bouwkundige beveiligingsmaatregelen	Toepassing van gecertificeerde sleutels.
RKJV-E1	Elektronische beveiligingsmaatregelen	Het compartiment waarin een opbergmiddel met een TBB is geplaatst, is voorzien van een 'indringen detectie signaleringssysteem' (IDSS).
RKJV-E2	Elektronische beveiligingsmaatregelen	De aanliggende compartimenten van het compartiment met een TBB zijn voorzien van IDSS of een opbergmiddel met een TBB is zelf voorzien van IDSS.
RKJV-E3	Elektronische beveiligingsmaatregelen	Het activeren en deactiveren van een IDSS kan alleen door middel van een Two-factor Authenticatie.
RKJV-E4	Elektronische beveiligingsmaatregelen	Een alarm van een IDSS leidt tot een effectieve alarmopvolging binnen de in gestelde interventie tijd.
RKJV-E5	Elektronische beveiligingsmaatregelen	Bewegingsmelders beschikken bij voorkeur over anti-masking maatregelen.
RKJV-E6	Elektronische beveiligingsmaatregelen	In een ruimte met een TBB zijn zonder goedkeuring van de BVA geen camera's, smartphones, microfoons of andere opnameapparatuur aanwezig.
RKJV-E7	Elektronische beveiligingsmaatregelen	De bewaartermijnen voor camerabeelden worden gehanteerd conform Rijksbeleid cameratoezicht.
RKJV-E8	Elektronische beveiligingsmaatregelen	Een ETS (Elektronische Toegangssysteem) is uitgerust met een Anti Pass Back (APB) systeem.

Maatregelnr.	Soort maatregel	Omschrijving
RKJV-E9	Elektronische beveiligingsmaatregelen	Een ETS is voorzien van Logging, waarbij de logs minimaal een jaar worden bewaard.
RKJV-E10	Elektronische beveiligingsmaatregelen	Meldingen uit het IDSS en het ETS moeten leiden tot tijdige Interventie.
RKJV-E11	Elektronische beveiligingsmaatregelen	Tempestmaatregelen conform Beleidsadvies Compromitterende straling (VBV 32000).
RKJV-F1	Logische toegangsbeveiliging	Toegang tot een account wordt na een aantal direct achtereenvolgende foutieve inlogpogingen geblokkeerd.
RKJV-F2	Logische toegangsbeveiliging	Toegang tot bijzondere informatie wordt op individueel niveau bepaald.
RKJV-F3	Logische toegangsbeveiliging	Toegang tot systemen kan op groepsniveau worden bepaald.
RKJV-F4	Logische toegangsbeveiliging	Toegangsrechten van de gebruikers zijn periodiek, minimaal zesmaandelijks, geëvalueerd.
RKJV-F5	Logische toegangsbeveiliging	Toegangsrechten van de gebruikers zijn periodiek, minimaal driemaandelijks, geëvalueerd.
RKJV-F7	Logische toegangsbeveiliging	Een geblokkeerd account kan worden vrijgegeven door tussenkomst van de leidinggevende en eventueel aangevuld is consultatie met de CISO.
RKJV-F8	Logische toegangsbeveiliging	Naast niet-succesvolle loginpogingen worden van succesvolle loginpogingen de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit e/o misbruik van het besturingssysteem.
RKJV-F9	Logische toegangsbeveiliging	Two-factor authenticatie in aanvulling op wachtwoorden is gebruikt.
RKJV-G4	ICT-voorzieningen	Onderhoud vindt plaats onder direct toezicht van gescreende personen.
RKJV-G5	ICT-voorzieningen	Van de gepleegde onderhouds- en reparatiewerkzaamheden wordt een administratie bijgehouden.
RKJV-G6	ICT-voorzieningen	Apparatuur waarop gerubriceerde informatie wordt verwerkt mag niet worden gekoppeld aan apparatuur van externen. Tenzij deze apparatuur van externen beveiligd wordt conform de eisen voor de betreffende TBB.
RKJV-G7	ICT-voorzieningen	Functiescheiding: niemand in de organisatie mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen. Dit i.v.m. het risico dat hij/zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Uitgangspunt: 4-ogen principe.
RKJV-H1	Informatiebeveiliging	De CISO houdt toezicht op de registratie van locatie, uitgifte, inname en herkomst van alle door de organisatie in ontvangst of in beheer genomen digitale TBB.
RKJV-H2	Informatiebeveiliging	Een TBB dat is opgeslagen op mobiele apparatuur is alleen toegestaan met toepassing van door het Rijk goedgekeurde procedures en middelen zoals: vercijfering, alleen hoogstnoodzakelijke hoeveelheid informatie in opslag en mag niet gebruikt worden in publieke ruimten.
RKJV-H3	Informatiebeveiliging	Telewerken is niet toegestaan.

Maatregelnr.	Soort maatregel	Omschrijving
RKJV-H4	Informatiebeveiliging	Na beëindiging van de opdracht worden de gegevensdragers fysiek vernietigd. Een proces-verbaal van vernietiging is opgesteld.
RKJV-H5	Informatiebeveiliging	Beheer op afstand is niet toegestaan.
RKJV-H6	Informatiebeveiliging	Gegevens op verwijderbare media moet vercijferd worden opgeslagen om hun vertrouwelijkheid te waarborgen.
RKJV-H7	Informatiebeveiliging	Groepsaccounts zijn niet toegestaan.
RKJV-H8	Informatiebeveiliging	Systemen waarop zich een grote concentratie van TBB van STG-C bevindt, zijn geplaatst in een ruimte die op TBB 2 niveau is beveiligd.
RKJV-H9	Informatiebeveiliging	Systemen waarop zich een grote concentratie van TBB van STG-G bevindt, zijn geplaatst in een ruimte die op TBB 1 niveau is beveiligd.
RKJV-H10	Informatiebeveiliging	Hergebruik van ICT-middelen is toegestaan mits het dezelfde TBB betreft en is gewist door gebruik te maken van de door het Rijk goedgekeurde middelen. Een proces verbaal van vernietiging (wissen) is opgesteld.
RKJV-H11	Informatiebeveiliging	Een werkplek is voor (TBB1 en 2 na: 5, TBB3 na: 10 en TBB4 na: 15 minuten) inactiviteit automatisch geblokkeerd.
RKJV-H12	Informatiebeveiliging	Het gebruik van draadloze communicatie is niet toegestaan zonder daarvoor goedkeurde voorzieningen.
RKJV-H13	Informatiebeveiliging	Het gebruik van draadloze communicatie is toegestaan met toepassing van door het Rijk goedgekeurde middelen en procedures.
RKJV-H14	Informatiebeveiliging	Een netwerk waarop TBB zijn opgeslagen, heeft geen verbinding met een ander netwerk, tenzij door het Rijk goedgekeurde procedures en middelen zijn toegepast.
RKJV-H15	Informatiebeveiliging	Netwerkapparatuur en -bekabeling wordt fysiek beschermd met een dusdanige vertragingstijd dat detectie van ongeautoriseerde toegang en pogingen daartoe plaatsvindt op een tijdstip dat interventie mogelijk maakt.
RKJV-H16	Informatiebeveiliging	Netwerkapparatuur en -bekabeling wordt fysiek beschermd dat detectie van ongeautoriseerde toegang en pogingen daartoe mogelijk is.
RKJV-H17	Informatiebeveiliging	Netwerkapparatuur en -bekabeling wordt fysiek beschermd dat detectie van ongeautoriseerde toegang mogelijk is.
RKJV-H18	Informatiebeveiliging	Gerubriceerde systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische toegangsmethoden.
RKJV-I1	Verzending gerubriceerde informatie	Digitale verzending van bijzondere informatie dient met ministerieel goedgekeurde crypto grafische middelen te geschieden.
RKJV-I2	Verzending gerubriceerde informatie	Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
RKJV-I3	Verzending gerubriceerde informatie	Fysieke verzending geschiedt door (1) ofwel een geautoriseerde medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens transport, ofwel (2) een

Maatregelnr.	Soort maatregel	Omschrijving
		ministerieel goedgekeurde koerier, ofwel (3) door een militaire, overheids- of diplomatieke koerier.
RKJV-I4	Verzending gerubriceerde informatie	Nationale verzending uitsluitend via een overheidskoerier.
RKJV-I5	Verzending gerubriceerde informatie	Internationale verzending uitsluitend als diplomatieke koerier zending of militair transport.
RKJV-I6	Verzending gerubriceerde informatie	Zowel digitaal als niet digitaal is er een onweerlegbare bevestiging van ontvangst.
RKJV-I7	Verzending gerubriceerde informatie	Verzending vindt plaats in dubbele enveloppe of door de BVA's goedgekeurde sealbag. De enveloppe of sealbag wordt zodanig gesloten dat openen zonder verbreken van de sluiting of beschadigingen niet mogelijk is.
RKJV-I8	Verzending gerubriceerde informatie	Indien gebruik wordt gemaakt van dubbele enveloppen draagt de binnen enveloppe de rubricering welke ook het document als geheel draagt. De buitenenveloppe draagt geen rubricering.
RKJV-I9	Verzending gerubriceerde informatie	Voor verzending worden zodanige enveloppen gebruikt dat met behulp van een technisch middel kennis nemen van de inhoud zonder openen van de enveloppen niet mogelijk is.
RKJV-I11	Verzending gerubriceerde informatie	Van alle exemplaren van bijzondere documenten worden de volgende gegevens vastgelegd: Exemplaarnummer, Maker, Ontvanger.
RKJV-J1	Fysieke opslag, verwerking, vernietiging en ontwikkeling	Geregistreerd is wie werkzaamheden aan bijzondere informatie heeft uitgevoerd of bijzondere informatie heeft ingezien.
RKJV-J3	Fysieke opslag, verwerking, vernietiging en ontwikkeling	De reproductie van Informatie geschiedt alleen met toestemming van degene die de rubricering heeft vastgesteld. Gemaakte reproducties zijn geregistreerd.
RKJV-J4	Fysieke opslag, verwerking, vernietiging en ontwikkeling	Het maken van reproducties is voorbehouden aan daartoe aangewezen geautoriseerd personeel dat ook zorgdraagt voor de registratie hiervan.
RKJV-J5	Fysieke opslag, verwerking, vernietiging en ontwikkeling	Reproducties kennen dezelfde rubricering als het origineel, ook als slechts delen van het origineel is gebruikt.
RKJV-J6	Fysieke opslag, verwerking, vernietiging en ontwikkeling	Er worden niet meer reproducties van bijzondere informatie gemaakt dan strikt noodzakelijk.
RKJV-J7	Fysieke opslag, verwerking, vernietiging en ontwikkeling	In geval van vernietiging wordt door een aangewezen medewerker met de juiste Autorisatie een proces-verbaal van vernietiging opgemaakt.

Bijlage 1: Handleiding workshop QS-IB

Inleiding

Deze bijlage biedt een handleiding die de workshopleider ondersteunt bij de voorbereiding en uitvoering van de QS-IB.

Workshopleider

Per workshop worden (bij voorkeur) een tweetal senior adviseurs ingezet: één adviseur richt zich op verslaglegging van hetgeen in de workshop wordt besproken en registreert hetgeen is vastgesteld in het format van de quickscan. De andere adviseur begeleidt het workshop proces en stuurt op voldoende diepgang van de risico analyse.
De beide adviseurs samen moeten over de volgende kennis bezitten:

- Kennis van de quickscan;
- Kennis van de business en de organisatie;
- Kennis van de betreffende systemen en de bijbehorende SLA's;
- Kennis van informatiebeveiliging in het algemeen en van de BIO;
- Ervaring met het uitvoeren van QS-IB workshops (training gevolgd).

Voorbereiding

Inventariseren benodigde informatie voor scoping

Bron voor het bepalen van de informatiebeveiliging is de BIO: de BIO is van toepassing op een proces, informatiesysteem of een combinatie hiervan. Tijdens de intake voor het uitvoeren van de quickscan wordt bepaald wat de scope is van het proces en het systeem waarop de quickscan wordt uitgevoerd. M.a.w. welk proces, informatiesysteem of combinatie van processen met systemen wordt onderzocht? Van belang is dat de scope niet te groot wordt gekozen. Veelal wordt uitgegaan van één proces met ondersteunende systemen of één systeem dat meerdere processen ondersteunt.

Om een goed inzicht te verkrijgen in de betrouwbaarheidseisen is het raadzaam om voorafgaand aan de QS-IB de DPIA uit te voeren. De inzichten uit de DPIA worden meegenomen in de QS-IB. Daarnaast is de volgende documentatie van belang:

- Procesbeschrijvingen;
- Systeembeschrijvingen / systeemdocumentatie;
- Bekende classificaties;
- Bekende incidenten;
- Documentatie van eerder uitgevoerde risicoafwegingen, QS-IB, audits, of BIA's ;
- Documentatie van Leverancier(s), derde partijen of ketenpartners;
- Reeds eerder uitgevoerde afwegingen voor de transitie naar de Cloud (Afwegingskader Cloud).
- Eerder geïdentificeerde risico's en daaraan gekoppelde mitigerende maatregelen uit het Governance, Risk and Compliance system (GRC).

Voorafgaand aan de workshop is de scope (welk proces, systeem(en)) vastgesteld met de proces- en systeemeigenaar (combineer dit met de hiervoor genoemd intake). Bij de start van de workshop wordt dit nog wel getoetst c.q. gevalideerd.

Selectie deelnemers workshop

De QS-IB wordt in een workshop bestaande uit twee of drie dagdelen uitgevoerd met diverse functionarissen. In de QS-IB worden de eisen die gesteld moeten worden aan processen en systemen vastgesteld. Een vertegenwoordiging in de workshop van de proces- en systeemeigenaar is daarom vereist. Immers de proces / systeemeigenaar bepaald uiteindelijk welke eisen er gesteld worden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van het proces / systeem. Laat gebruikers / afnemers van het proces en systeem deelnemen aan de workshop. Zij

kunnen als materiedeskundigen een inschatting maken van de werking en werkbaarheid van vastgestelde maatregelen. Hiernaast is het van belang dat bij het selecteren van de functionarissen voor de workshop kennis van de bron voor de informatiebeveiliging (BIO) afdoende aanwezig is: laat de (C)ISO deelnemen aan de workshop i.p.v. toetsing achteraf van de quickscan.

Resumerend is het van belang dat tenminste de volgende functionarissen betrokken zijn:

- proces- / systeemeigenaar
- de eindgebruiker / key-user / representatieve gebruiker in het proces / van het ondersteunende systeem
- functioneel systeem beheerder
- technisch systeem beheerder
- de Functionaris Gegevensbescherming (FG) of de Privacy Officer (PO) van het onderdeel indien verwerking van persoonsgegevens aan de orde is.
- De (Chief) Information Security Officer (C)ISO) van het onderdeel
- optioneel:
    - vertegenwoordiger van de leverancier
    - projectleider
    - informatiebeveiligingsfunctionaris
    - informatiemanager
    - architect

Niet altijd zal het mogelijk zijn om de workshops zo te plannen dat alle vereiste functionarissen aanwezig zijn. Om die reden biedt de quickscan de mogelijkheid om de workshops in te delen naar een meer op het proces gerichte sessie en een sessie waarin meer het systeem-technische aspect aan de orde komt. In plaats van een workshop aanpak kan de keuze worden gemaakt om op basis van individuele interviews de vereiste informatie in te winnen. Hierbij is het van groot belang dat de argumentatie van de gemaakte keuzes goed wordt gedocumenteerd en gedeeld met de andere functionarissen. Een groot kwalitatief nadeel bij individuele interviews is het ontbreken van de groepsdiscussies. (hybride)Workshops verdienen de aanbeveling.

Uitnodigen deelnemers QS-IB workshop

De deelnemers aan de QS-IB workshop kunnen volstaan met een minimale voorbereiding.
Stuur voorafgaand aan de workshop, met de uitnodiging voor de bijeenkomst, de deelnemers de quick scan IB toe. Geef daarbij aan dat de workshop m.b.v. de quick scan tot doel heeft om een risicoanalyse uit te voeren op de informatieveiligheid van het betreffende proces en systeem. De voorafgaand aan de workshop bepaalde (voorlopige) scope van het proces wordt met de deelnemers gedeeld.
Meer in detail kan de uitnodiging het volgende omvatten:

- Inleiding over waarom de QS-IB workshop wordt gehouden en het doel van de workshop: In kaart brengen welke eisen gesteld worden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid voor het te onderzoeken proces / informatiesysteem.
- Het beoogde resultaat van de QS-IB workshop is een verantwoorde afweging om het basis beveiligingsniveau (BBN) te bepalen dat minimaal noodzakelijk is om het proces en de bijbehorende ondersteunende informatiesystemen te beschermen, gegeven het belang dat de proces- en systeemeigenaar daaraan toekent.
- Korte beschrijving van wat er in de QS-IB workshop gaat gebeuren:
    - Uitvraag van eisen die aan de processen en systemen worden gesteld op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid.
      Neem in de uitnodiging een aantal voorbeelden van vragen op die gesteld worden zoals:
        - Hoe lang mag het proces / systeem eruit liggen voordat er grote processchade optreedt?
        - Welke impact op het proces heeft het wanneer de informatie in het proces/ systeem niet volledig of niet correct is?
        - Wordt er met vertrouwelijke informatie gewerkt en hoe erg is het als deze informatie ‘op straat komt te liggen’ i.c. door niet bevoegden kan worden ingezien of ge(mis)bruikt?

- De tijdsbesteding: op basis van de scope en de documentatie vooraf samen met de opdrachtgever de tijdbesteding inschatten en nagaan wat te doen als de geplande tijd niet voldoende blijkt. Als richtlijn kan een tijdsduur van twee dagdelen genomen worden van elek ca. 4 uren.
- Wat er van de deelnemers verwacht wordt:
  - Vooraf doornemen van de meegestuurde scopebeschrijving
  - Input leveren tijdens de workshop
  - Review van het eindresultaat

N.B.: Biedt ruimte om vragen stellen over de toegestuurde informatie bijvoorbeeld door een 'spreek uurtje' te plannen. Hiermee voorkom je dat veel tijd van de workshop opgaat in het stellen en beantwoorden van vragen.

De QS-IB workshop

Voor een snel en soepel verloop van de workshop is het verstandig dat de adviseur aan het begin van de QS-IB een algemene inleiding geeft op het gebied van informatiebeveiliging, waarbij ook de gehanteerde definities worden verduidelijkt. Hierbij gaat het in ieder geval om:
- Rubricering;
- VIR, VIR-BI;
- Baseline informatiebeveiliging Overheid (BIO);
- Basis beveiligingsniveau (BBN);
- BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid);
- Classificeren;
- Indien van toepassing: het gebruik van de Cloud.

Voor het samenstellen van deze inleiding kan geput worden uit deel 1 van de BIO. Advies is om de inhoud en diepgang van de inleiding zoveel als mogelijk af te stemmen op de kennis en ervaring van de workshopdeelnemers

Nadat de introductie is gedaan, en de deelnemers zich hebben voorgesteld, kan begonnen worden met de workshop. Van belang is dat de scope – eerder toegezonden – wordt gevalideerd. Gebruik hiervoor de invulformulieren in de QS-IB.

N.B.: je kunt de keuze maken om het voorgaande als informatie vooraf te sturen (zie voorbereiding workshop). Echter dit vergt een flinke belasting van de deelnemers voorafgaand aan de workshop. Wij raden dit af om deze reden maar vooral ook omdat met deze start van de workshop een ieder op dat moment hetzelfde basis kennisniveau aangereikt krijgt.

Vervolg na de QS-IB workshop

Wanneer alle processtappen zijn doorlopen en de voorlopige conclusie is getrokken, is het aan de procesbegeleider om de ingevulde QS-IB aan de workshopdeelnemers voor te leggen voor een finale review. Bij de review is het van belang dat er goed gekeken wordt naar de argumentatie die is gegeven waarom bepaalde keuzes zijn gemaakt. Deze hebben immers effect op de additionele mitigerende maatregelen om de risico's te mitigeren.

Het vervolg op de uitkomst van de quick scan IB wordt vastgelegd in een plan van aanpak. Dit plan van aanpak wordt na vaststelling ervan door de proces- en systeemeigenaar toegevoegd aan de quick scan IB.
Afhankelijk van de uitkomst van de quick scan (het bepaalde BBN) omvat het plan van aanpak tenminste het volgend:

1. **BBN1:**
   Met de formele ondertekening van de rapportage staan de te nemen maatregelen in het vervolgtraject vast. Daarbij moet de systeem/proceseigenaar opdracht geven een implementatieplan op te stellen om de benodigde maatregelen in te voeren. Het implementatieplan moet bevatten:

- een selectie van de BIO BBN1-maatregelen en eventuele extra maatregelen, bij voorbeeld uit de ISO27001:2013 (Annex A);
- per maatregel de actor en gewenste datum van invoering.

2. **BBN2:**
   Aan het implementatieplan moeten de VIR-BI maatregelen voor Departementaal vertrouwelijke informatie worden toegevoegd.
3. **BBN3:**
   Om adequate beveiligingsmaatregelen te bepalen is de BIO ontoereikend en is een uitgebreide risicoanalyse sterk aanbevolen. Als methode wordt daarvoor IRAM aanbevolen.
4. **Indien gebruik wordt gemaakt van de Cloud:**
   Bij het implementatieplan moeten tevens de maatregelen uit de Implementatierichtlijn Cloud worden toegevoegd in aanvulling op het gekozen BBN.

Vanuit het oogpunt van risicomanagement moet een organisatie met beperkte resources de prioriteit leggen bij de beheersing van de grootste risico's. Overweeg daarom of een BBN3-systeem moet worden gelabeld als "kritiek systeem" op basis van de volgende voorwaarden:[35]

- het proces wordt aangemerkt als kritisch strategisch (afgeleide kerntaak) of valt in TBB categorie 2 of 1;
- het informatiesysteem is vitaal voor dit proces en
- één of meer betrouwbaarheidseisen (B, I, V) scoren hoog.

Na verwerking van de reviewcommentaren wordt de resultaten van de QS-IB aangeboden voor ondertekening aan de betrokken proces / systeemeigenaar.

---

[35] Zie Toelichting Model In Control Verklaring 2018 (BZK) ven Leidraad Te Beschermen Belangen (TBB = mensen of objecten waarvan de primaire taak van rijksoverheid afhankelijk is);

Bijlage 2: Samenhang QS-IB en DPIA

Inleiding

De QS-IB overlapt met de DPIA voor verwerkingen van persoonsgegevens: de context, procesbeschrijving, verantwoordelijkheden en beoordeling van risico's komen in beide voor. Het uitvoeren van een QS-IB kan daarom pas plaatsvinden nadat een DPIA is uitgevoerd. Zie de DPIA Rijksdienst of de Cloud specifieke DPIA.

Volgordelijkheid DPIA en workshop QS-IB