Handreiking
Quickscan Information Security

versie 1.0 20 februari 2018

Inleiding

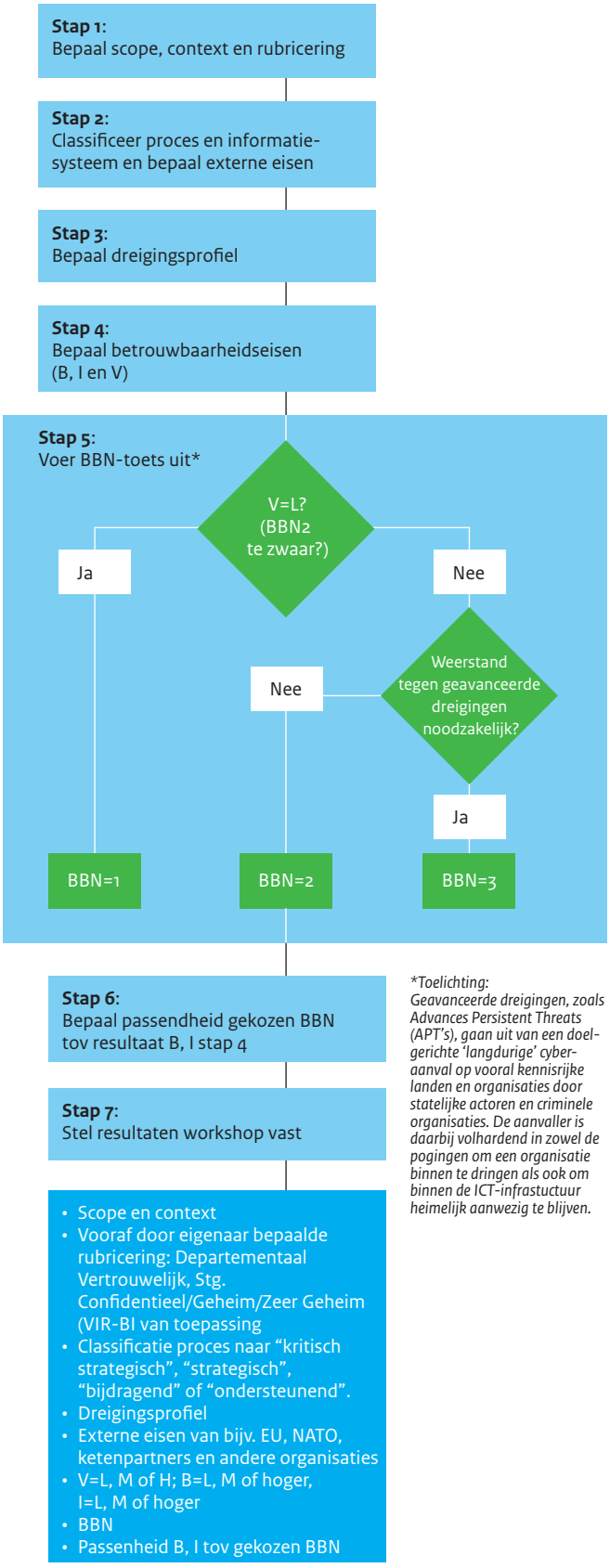
De Quickscan Information Security (QIS) is een handreiking die kan worden gebruikt om de toets voor het bepalen van het basis beveiligingsniveau (BBN-toets zoals beschreven in de BIR2017) in te vullen en om eventuele aanvullende vereisten te bepalen die noodzakelijk zijn om een informatiesysteem te beschermen gegeven het belang dat de eigenaar daar aan toekent. Behoudens de BBN-toets kunnen alle stappen in de QIS waar gewenst worden aangevuld en aangepast om de aansluiting van de QIS op de praktijk van de eigen organisatie te bevorderen.

De Quickscan start met een inventarisatie van de scope en context van het te beschermen informatiesysteem en de, door de eigenaar vastgestelde, rubricering van de daarin te verwerken informatie (stap 1).

Vervolgens wordt het belang van het proces en het ondersteunende informatiesysteem geclassificeerd en wordt bepaald of daar externe eisen van bijvoorbeeld de EU, de NAVO, ketenpartners of andere organisaties op van toepassing zijn (stap 2). De verwachte bedreigingen ten aanzien van het informatiesysteem en de (soort) actoren die deze veroorzaken worden, voor zover van toegevoegde waarde, vastgelegd in een dreigingsprofiel (stap 3).

Op basis van een inschatting van de maximale schade die kan ontstaan op het gebied van "Beschikbaarheid", "Integriteit" en "Vertrouwelijkheid" (stap 4) wordt aan de hand van de BBN-toets het bijbehorende BBN gekozen (stap 5). Daarna wordt de passendheid van het gekozen BBN bepaald door te bezien welke extra – of juist minder – schade op het gebied van "Beschikbaarheid" en "Integriteit" aan de orde kan zijn ten opzichte van dit BBN (stap 6).

Tot slot worden de resultaten van de QIS vastgesteld door de eigenaar van het proces en/of het informatiesysteem (stap 7). Deze resultaten kunnen vervolgens worden gebruikt om – op basis van een risicoafweging – eventueel noodzakelijke aanvullende controls en maatregelen te bepalen[1].



*Toelichting:
Geavanceerde dreigingen, zoals Advances Persistent Threats (APT's), gaan uit van een doelgerichte 'langdurige' cyberaanval op vooral kennisrijke landen en organisaties door statelijke actoren en criminele organisaties. De aanvaller is daarbij volhardend in zowel de pogingen om een organisatie binnen te dringen als ook om binnen de ICT-infrastuctuur heimelijk aanwezig te blijven.

[1] BIR2017, par. 2.2: "Na de BBN-toets doorloopt het lijnmanagement alle toepasselijke controls uit de BIR. Op basis van een risicoafweging wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, rijksmaatregelen en/of operationaliseringen in handreikingen worden gebruikt."

Inhoudsopgave

Werkwijze Quickscan

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)
Stap 5: Voer BBN-toets uit
Stap 6: Bepaal passendheid gekozen BBN tov resultaat B, I stap 4
Stap 7: Stel resultaten workshop vast

Uitvoering

De Quickscan wordt in samenwerking met de direct betrokkenen uitgevoerd (gemiddeld 1 dagdeel). Ter voorbereiding stemt de Quickscan-begeleider de scope (welke processen en informatiesystemen), context en rubricering (stap 1) af met de opdrachtgever, zodat deze enkel gevalideerd hoeft te worden.

De Quickscan wordt uitgevoerd met de eigenaar van processen en informatiesystemen en een aantal representatieve gebruikers van de informatiesystemen. Deze ontvangen vooraf de resultaten van stap 1. Tijdens de Quickscan wordt per beveiligingsaspect onderzocht wat in het ergste geval ('worst case') het mogelijke gevolg zou kunnen zijn voor een organisatie, als gevolg van het optreden van een incident waarbij de informatie in een informatiesysteem en/of de werking van een informatiesysteem wordt aangetast.

Het resultaat van de Quickscan wordt verwoord in een rapportage waarin de keuze voor het toe te passen BBN wordt toegelicht. Deze rapportage wordt vastgesteld door de opdrachtgever.

Een handleiding voor het uitvoeren van de Quickscan door het organiseren van een workshop is opgenomen als bijlage 1.

Stap 1: Bepaal scope, context en rubricering

De uitvoering van de Quickscan vereist resources vanuit de organisatie. Het is derhalve essentieel deze zo efficiënt mogelijk uit te voeren. Dit vereist voorbereiding en afstemming met de opdrachtgever en de te betrekken functionarissen. Stap 1 van de Quickscan beschrijft de wijze waarop de scope en de context worden bepaald en biedt ruimte om de door de eigenaar vastgestelde rubricering vast te leggen.

Deze stap wordt ter voorbereiding van de workshop uitgevoerd door de procesbegeleider en de eigenaar van het proces en het informatiesysteem. De resultaten daarvan worden vooraf naar de deelnemers verzonden.

Scope

Bepaal de scope van de Quickscan: welk (deel van het proces) en welke informatiesystemen betreft het?
De scope kan uitgaan van een proces met één of meerdere ondersteunende systemen of één informatiesysteem dat meerdere processen ondersteunt. Geef in onderstaande tabel aan welke processen met ondersteunende systemen tot de scope van de analyse behoren.

	<Proces A>	**<Proces B>**
	Korte beschrijving van het proces	Korte beschrijving van het proces
<Informatie-systeem 1>	Beschrijving van de ondersteunende functie van het informatie-systeem voor het proces	Beschrijving van de ondersteunende functie van het informatie-systeem voor het proces
<Informatie-systeem 2>	Beschrijving van de ondersteunende functie van het informatie-systeem voor het proces	Beschrijving van de ondersteunende functie van het informatie-systeem voor het proces

Context

Vul per proces dat tot de scope behoort onderstaande tabel in. Vallen meerdere processen onder de scope dan dient per proces een tabel ingevuld te worden.

<Naam van het proces>	
Proceseigenaar	<naam van de proceseigenaar>
De klant van het proces	De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt: • <wie is de interne klant?> • <wie is de externe klant?>
De output van het proces	<De output is het resultaat van handelen in het proces>
Koppelvlakken met andere processen	• <aanleverende processen/ organisaties> • <afnemende processen/organisaties>
Gebruikte systemen	De informatiesystemen die worden gebruikt bij de activiteiten in het proces: • <informatiesysteem>

Vul per informatiesysteem dat tot de scope behoort onderstaande tabel in. Als er meerdere informatiesystemen onder de scope vallen dan dient per informatiesysteem een tabel ingevuld te worden.

<Naam van het Informatiesysteem>	
Informatiesysteem-eigenaar	<naam van de informatiesysteemeigenaar>
De gebruikers van het informatiesysteem	Degene die werkzaam zijn met het informatiesysteem • <wie is de interne gebruiker / klant?> • <wie is de externe gebruiker / klant?> • <aantal gebruikers / burgers>
De output van het informatiesysteem	
Koppelvlakken met andere informatiesystemen	Een architectuurplaatje kan verhelderend werken
Het informatiesysteem ondersteunt de volgende processen	
Kritische momenten	Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes

Rubricering

Geef aan of het informatiesysteem gerubriceerde informatie verwerkt. Als er meerdere soorten informatie in het informatie-systemen worden verwerkt dan dient per soort informatie het rubriceringsniveau te worden vermeld.

<Naam van het Informatiesysteem waarop rubricering wel/niet van toepassing is>	
Soort informatie	**Rubricering**
<soort informatie: persoonsgegevens, etc>	Niet/Departementaal Vertrouwelijk, Stg. Confidentieel/Geheim/Zeer Geheim (VIR-BI van toepassing)

Als informatie is gerubriceerd dan is het VIR-BI van toepassing en moeten de bij het rubriceringsniveau behorende maatregelen uit dit voorschrift worden geïmplementeerd. Kortheidshalve wordt hier verwezen naar de tekst van het VIR-BI[2].

[2] http://wetten.overheid.nl/BWBR0033507/2013-06-01

Stap 2: Classificeer proces en informatiesysteem en bepaal externe eisen

Classificatie van het proces

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 naar 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 het ministerie/kerndepartement of uitvoeringsorganisatie. Het ontbreken echter van het 'bijdragende proces' heeft echter wel effectiviteits- en efficiencyverliezen binnen het primaire proces effectiviteit- en efficiencyverliezen tot gevolg.

Classificatie: Strategisch **Taak: Afgeleide kerntaak**

Het proces heeft een directe relatie met het uitvoeren van de doelstellingen van het ministerie/ kerndepartement of uitvoerings-organisatie. Het betreft het primaire proces van de directie, agentschap, raad, etc.

- Aan het proces kan een ontwikkelpotentieel worden toegekend. Met andere woorden, het wordt in de toekomst belangrijker in verband met mogelijke veranderingen in de strategische doelstellingen van het ministerie / kerndepartement of uitvoerings-organisatie.
- Een aanzienlijk deel van de omzet (50% - 80%) wordt gegenereerd met dit proces of 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).

Classificatie: Kritisch strategisch **Taak: Kerntaak**

In relatie tot de doelstellingen van het ministerie/ kerndepartement of uitvoeringsorganisatie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop het ministerie / kerndepartement of uitvoeringsorganisatie direct kan worden aangesproken.
Het ministerie / kerndepartement of uitvoeringsorganisatie ontleent haar bestaansrecht aan het uitvoeren van deze taken.

- 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;
  b. fysieke veiligheid: het ongestoord functioneren van de mens in Nederland en zijn omgeving;
  c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie;
  d. ecologische veiligheid: het beschikken over voldoende zelf herstellend vermogen van de leefomgeving bij aantasting;
  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.
- Als de activiteit langer dan één week stilvalt of niet goed verloopt, heeft dit ernstige gevolgen voor het voortbestaan van de organisatie, c.q. het brengt het ministerie / kerndepartement of uitvoeringsorganisatie in een hachelijke positie.

Argumentatie van de gekozen classificatie voor het proces

Beschrijf hier de keuze die is gemaakt voor de classificatie. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen classificatie.

Inventarisatie en classificatie van de informatiesystemen

Om het proces goed te kunnen laten functioneren wordt gebruik gemaakt van een aantal ondersteunende informatiesystemen. In onderstaande tabel is een overzicht gegeven van mogelijke classificaties van het informatiesysteem. De classificaties geven een waarde aan die men hecht aan het informatiesysteem ter ondersteuning van het proces.

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

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

Argumentatie van de gekozen classificatie voor het informatiesysteem		
Informatiesysteem	**Belang (N, B, V)**	**Argumentatie**
Naam Informatiesysteem		Beschrijf hier de keuze die is gemaakt voor de classificatie van het informatiesysteem. Het is van belang dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen classificatie.

Bepaal externe eisen

Geef in onderstaande tabel per informatiesysteem aan welke eisen externe partijen daar aan stellen.

Argumentatie externe eisen voor het informatiesysteem		
Informatiesysteem	**Externe eis**	**Herkomst eis**
Naam		NAVO, EU, ketenpartner, andere organisatie, AVG

Stap 3: Bepaal dreigingsprofiel

In de BIR2017 zijn op basis van de generieke schades en dreigingen voor de Rijksoverheid basis basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. In aanvulling daarop is het van belang om vast te stellen van of en van welke (soort) specifieke dreigingen het te analyseren proces met ondersteunende informatiesystemen doelwit kan zijn.

Beveiligingsincidenten

Om het dreigingsprofiel te bepalen kan het van toegevoegde waarde zijn om inzicht te hebben in eventueel opgetreden beveiligingsincidenten. Maak in dat geval een inventarisatie van de belangrijkste relevante opgetreden beveiligingsincidenten. Dit kan bijvoorbeeld door (beveiligings)incidenten van de Servicedesk op te vragen en te analyseren.

Belangrijkste beveiligingsincidenten		
Informatie-systeem	**Incident**	**Datum**
<soort informatie: naam informatie-systeem>	Incident: de beschikbaarheid, integriteit en/of vertrouwelijkheid van het informatiesysteem en/of de daarin verwerkte informatie zijn in het geding geweest door de volgende voorvallen: ... Dit is als volgt hersteld: ... Om herhaling te voorkomen zijn de volgende maatregelen genomen: ...	

Dreigingsprofiel

Actor	**Bedreigingen**
Denk bijvoorbeeld aan: • De onbetrouwbare medewerker • Wraakzuchtige medewerker • De verontruste burger • Actiegroep • Crimineel opportunist • Contractor/inhuurkracht • Georganiseerde internet crimineel • Statelijke actoren • Criminele organisaties	Denk bijvoorbeeld aan: • Infiltratie light • Publiek benaderbare sociale netwerken • Verhoor (fysiek geweld tegen personen) • Hacking op afstand • Malware (met en zonder remote control) • Crypto kraken • Draadloze netwerken interceptie • Draadloze netwerken actief benaderen • Beproeving van fysieke, technische en elektronische weerstand • Advanced Persistent Threats (APT's) • Onopzettelijk menselijk handelen • Opzettelijk menselijk handelen • Onbeïnvloedbare externe factoren • Technisch falen

Daarnaast met betrekking tot mogelijke actoren en dreigingen inspiratie worden gehaald uit bijvoorbeeld het Cyber Security Beeld Nederland (CSBN) dat het NCSC jaarlijk publiceert.

Argumentatie van de van toepassing zijnde dreigingen en dreigers
Bepaal welke specifieke aanvullende dreigingen van toepassing zijn op het proces met ondersteunende systemen. Dit kunt u doen door bijv. te kijken naar hoeveel exposure het proces heeft. Is het bijvoorbeeld een proces / dienstverlening dat veel in de media is (geweest) of worden er in het proces / ondersteunende systeem- gegevens verwerkt die interessant kunnen zijn voor specifieke doelgroepen (bijvoorbeeld financiële gegevens, persoonsgegevens). Daarnaast kunnen eerdere incidenten helpen dreigingen en dreigers te identificeren.

Stap 4: Bepaal betrouwbaarheidseisen

In deze stap worden de betrouwbaarheidseisen “Beschikbaarheid”, “Integriteit” en “Vertrouwelijkheid”, bepaald aan de hand van de schadescenario’s uit bijlage 2 van de BIR2017.
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 “Hoger dan midden” toegekend.
De resultaten van deze stap worden gebruikt in de BBN-toets in stap 5 en bij het bepalen van de passendheid van het gekozen BBN in stap 6.

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 het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet • krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: • Kantoorautomatisering en dienstspecifieke 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 (5 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; of • diplomatieke schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of • uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en dienstspecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Hoger dan midden	Ernstigere schade dan het bij “Midden” beschreven schadescenario. De beschikbaarheideis 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.

Argumentatie van de gekozen beschikbaarheidsniveau
Beschrijf hier de keuze die is gemaakt voor de gekozen waardering van de beschikbaarheid. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn. • Beschrijf bijvoorbeeld de minimale eisen die gesteld worden aan de beschikbaarheid (ook in de piekperiodes). Komt dit overeen met de afgesloten SLA? • Welke eisen worden gesteld aan bijvoorbeeld het weer beschikbaar hebben van de data bij verlies? • Zijn er wettelijke termijnen die gehaald moeten worden? • Zijn er contractuele verplichtingen qua beschikbaarheid afgesproken naar burgers? • Zijn er politieke processen die een bepaalde beschikbaarheid / response tijd vereisen? • Zijn er resultaten van andere Quickscans die leiden tot hogere beschikbaarheidseisen? • Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.

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 en de hem ondersteunende managers en medewerkers (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Categorie	Maximale schade
Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden totbeperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; 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; of • diplomatieke schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Hoger dan midden	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.

Argumentatie van de gekozen integriteitsniveau
Beschrijf hier de keuze die is gemaakt voor de gekozen waardering van integriteit. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn. • Beschrijf waarom welke integriteitseisen aan de informatie worden gesteld. • Zijn er workarounds, is er bijvoorbeeld een papieren schaduwdossier, worden fouten snel herkend, wordt het vier ogen principe gehanteerd, wordt functiescheiding toegepast?, etc. • Zijn er fouttoleranties afgesproken met burgers / afnemers? • Zijn er resultaten van andere Quickscans die leiden tot hogere integriteitseisen? • Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.

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 ongeautoriseerden (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 het ministerie of uitvoeringsorganisatie; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst, 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; of • diplomatieke schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of • bindende aanwijzing van de AP in verband met schending van de privacy; 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); of • aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of • weerstand tegen statelijke actoren is noodzakelijk.

Argumentatie van de gekozen integriteitsniveau
Beschrijf hier de keuze die is gemaakt voor de gekozen waardering van vertrouwelijkheid. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn. • Beschrijf wat voor soort informatie in het proces en informatiesysteem wordt verwerkt. Is dit privacy gevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie en welke belangen worden geschaad bij het openbaar worden van deze informatie? • Worden er wettelijke eisen aan de vertrouwelijkheid gesteld (bijv. AVG)? • Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naar burgers? • Zijn er resultaten van andere Quickscans die leiden tot hogere vertrouwelijkheidseisen? • Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.

Samenvatting betrouwbaarheidseisen			
	Beschikbaarheid	**Integriteit**	**Vertrouwelijkheid**
Betrouwbaarheidseisen	L, M of hoger dan M	L, M of hoger dan M	L, M of H

Stap 5: Voer BBN-toets uit

Bepaal het gewenste BBN aan de hand van de volgende afwegingen.

Stap 1: Is BBN2 voldoende?

Meestal is BBN2 van toepassing op een specifiek informatiesysteem. Het kan echter zijn dat BBN2 niet voldoende is. BBN2 is onvoldoende indien:

- de informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers; of
- informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen; of
- aansluiting op een infrastructuur het BBN3 vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen)

In elk van deze gevallen is BBN3 of hoger (zie VIR-BI) van toepassing.

Stap 2: Is BBN2 te zwaar?

Bij BBN2 informatiesystemen kan het ongewenst of onbedoeld openbaren van informatie leiden tot BBN2-schade:

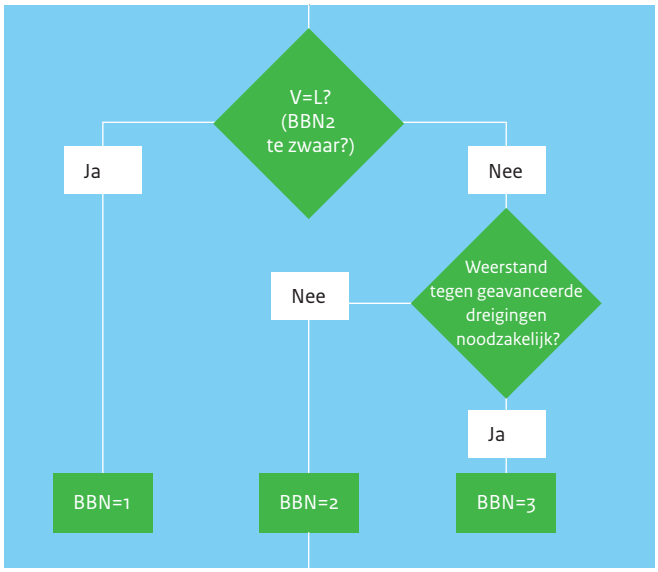
- politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of
- diplomatieke schade te herstellen door ambtelijke opschaling; of
- financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of
- verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of
- bindende aanwijzing van de AP in verband met schending van de privacy; of
- directe imagoschade, bijvoorbeeld door negatieve publiciteit.

Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing.

Stap 3: Bepaal extra vereisten voor beschikbaarheid en/of integriteit

In het geval van BBN1: leidt uitval van systemen en/of het verminkt raken van informatie tot schade vergelijkbaar met BBN2-schade (zie stap 2)? In dat geval kan worden overwogen (een deel) van de BIR controls en maatregelen, die toezien op beschikbaarheid dan wel integriteit op het niveau van BBN2 te nemen. De verantwoording en toezicht vindt plaats volgens BBN2.
In het geval van BBN2 of BBN3: leidt uitval van systemen en/of het verminkt raken van informatie tot grotere schade dan de BBN2-schade (zie hierboven)? In dat geval wordt op basis van expliciete risicoafweging bepaald voor welke controls welke aanvullende en/of zwaardere maatregelen nodig zijn. De verantwoording en toezicht vindt plaats volgens BBN3.

Grafisch:



Toelichting:
Geavanceerde dreigingen, zoals Advances Persistent Threats (APT's), gaan uit van een doelgerichte 'langdurige' cyberaanval op vooral kennisrijke landen en organisaties door statelijke actoren en criminele organisaties. De aanvaller is daarbij volhardend in zowel de pogingen om een organisatie binnen te dringen als ook om binnen de ICT-infrastuctuur heimelijk aanwezig te blijven.

Argumentatie voor het gekozen BBN

Beschrijf hier de keuze die is gemaakt voor het gekozen BBN en eventuele aanvullende controls en/of zwaardere maatregelen. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn.

Stap 6: Bepaal passenheid gekozen BBN

Per BBN gelden de volgende niveaus voor de betrouwbaarheids-aspecten “Beschikbaarheid” en “Integriteit”. BBN1: L/L, BBN2: MM en BBN3: MM[3].

In deze stap wordt per onderzocht proces en/of informatiesysteem de passenheid van het gekozen BBN bepaald door na te gaan welke extra schade kan ontstaan of welke schade waarschijnlijk niet aan de orde zal zijn voor de bij dit BBN behorende niveaus van “Beschikbaarheid” en “Integriteit”.

Samenvatting resultaten stap 1 t/m 4 in relatie tot gekozen BBN							
Stap 1	**Stap 2**		**Stap 3**	**Stap 4**			**Stap 5**
Rubricering	**Classificatie Proces**	**Classificatie Systeem**	**Dreigings profiel**	**B**	**I**	**V**	**BBN**
• Geen • Departementaal Vertrouwelijk, Stg. confidentieel, Stg. Geheim of Stg. Zeer Geheim (VIR-BI van toepassing)	O, B, S, KS	N, B, V	Beschrijving	L, M of hoger dan M	L, M of hoger dan M	L, M of H	1, 2 of 3

Argumentatie voor mate van passendheid gekozen BBN tov betrouwbaarheidseisen
Beschrijf hier welke mogelijke aanvullende of mindere schade is onderkend. Het is van belang dat de onderliggende keuzes goed worden gedocumenteerd.

[3] BIR2017, Bijlage 2.

Stap 7: Vaststellen resultaten workshop

Teken Formulier

Op ` heeft een workshop QuickScan Information Security plaatsgevonden voor

met ondersteunende systemen

[Eventueel beknopte samenvatting van belangrijkste resultaten stap 1 t/m 8 toevoegen]

Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
	Eigenaar proces / systeem	
	Key-user systeem	
	Functioneel beheerder	

Ik heb kennis genomen van de inhoud van het rapport en stem in met de resultaten van deze QuickScan. De resultaten van de Quickscan zijn geldig tot het moment dat de gegevens waarop deze zijn gebaseerd wijzigen.

Datum:

Naam:

Functie:

Handtekening:

Laten aftekenen door de proceseigenaar / systeemeigenaar.

Bijlage 1: Handleiding workshop Quickscan

Inleiding

In deze bijlage is een handleiding beschreven die dient als ondersteuning voor de workshopleider bij de voorbereiding en uitvoering van de Quickscan information Security.

Workshopleider

Per Quickscan worden (bij voorkeur) een tweetal senior adviseurs ingezet. De ervaring leert dat dit leidt tot de beste resultaten. Één adviseur richt zich op de inhoud en de registratie daarvan, de ander begeleidt het proces. Deze adviseurs moeten de volgende kennis bezitten:

- 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 BIR
- Ervaring met het uitvoeren van quickscans

Voorbereiding

Inventariseren benodigde informatie voor scoping

De BIR2017 is van toepassing op een proces, informatiesysteem of een combinatie hiervan. Om de Quickscan Information Security toe te passen moet de scope gedefinieerd worden. 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 processen en systemen kan de volgende documentatie behulpzaam zijn:

- Procesbeschrijvingen
- Systeembeschrijvingen / systeemdocumentatie
- Bekende classificaties
- Bekende incidenten
- Reeds eerder uitgevoerde risicoafwegingen of audits
- Reeds eerder uitgevoerde quickscans of BIA's

Voorafgaand aan de workshop stemt de procesbegeleider de scope (welk proces, systeem(en)) met de opdrachtgever af zodat deze tijdens de workshop slechts gevalideerd hoeft te worden.

Selectie deelnemers workshop

De Quickscan Information Security wordt middels een workshop van twee uur uitgevoerd met diverse functionarissen. In de Quickscan Information Security worden de eisen die gesteld worden aan processen en systemen onderzocht. Een vertegenwoordiging vanuit de business is daarom vereist. Immers de proces / systeemeigenaar kan bepalen welke eisen er gesteld worden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van het proces / systeem. Hiernaast is het van belang bij het selecteren van de functionarissen voor de workshop dat men voldoende kennis heeft van het te onderzoeken proces met ondersteunende systemen.

De volgende functionarissen dienen minimaal om input te worden gevraagd:

- proces- / systeemeigenaar
- de eindgebruiker / key-user / representatieve gebruiker in het proces / van het ondersteunende systeem
- functioneel beheerder
- optioneel:
  - vertegenwoordiger van de service provider
  - projectleider
  - informatiebeveiligingsfunctionaris
  - functionaris gegevensbescherming
  - informatiemanager
  - architect
  - de Functionaris Gegevensbescherming (FG) indien opslag en verwerking van persoonsgegevens aan de orde is.

Niet altijd zal het mogelijk zijn om een workshop te plannen waar alle vereiste functionarissen aanwezig zijn. In plaats van een workshop kunnen dan individuele interviews gehouden worden. Hierbij is het van groot belang dat de argumentatie van de gemaakte keuzes goed wordt gedocumenteerd en gedeeld met de andere functionarissen. Bij individuele interviews ontbreken de groepsdiscussies. Deze dienen dus 'offline' middels reviewsessies plaats te vinden.

Uitnodigen deelnemers workshop

De deelnemers aan de Quickscan workshop kunnen volstaan met een minimale voorbereiding. Met de uitnodiging voor de bijeenkomst ontvangen de deelnemers informatie die hen een goed beeld geeft van het doel, de onderdelen van de bijeenkomst en wat het beoogde resultaat is. Een uitnodiging kan de volgende punten bevatten:

- Inleiding over waarom de Quickscan workshop wordt gehouden en het doel.
  - Het doel is: 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 Quickscan is een verantwoorde afweging om het basis beveiligingsniveau (BBN) te bepalen dat minimaal noodzakelijk is om een proces en de bijbehorende ondersteunende informatiesystemen te beschermen gegeven het belang dat de eigenaar daar aan toekent.
- Korte beschrijving van wat er in de 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 schade optreedt?
    - Welke impact heeft het wanneer de informatie in het proces/ systeem niet volledig of correct is?
    - Wordt er met (persoons) vertrouwelijke informatie gewerkt en hoe erg is het als deze op straat komt te liggen?
  - Bij vragen over de meegestuurde documenten dan kunt u ze vooraf stellen aan de contactpersoon

- 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 2 uur genomen worden en maximaal 4 uur.

- Wat er van de deelnemers verwacht wordt:
  - Vooraf doornemen van de meegestuurde scopebeschrijving
  - Input leveren tijdens de workshop
  - Review van het eindresultaat

- Bijlage: de Quickscan Information Security, beschrijving van de scope

De workshop Quickscan Information Security

Voor een snel en soepel verloop van de workshop is het verstandig dat de adviseur aan het begin van de Quickscan een algemene inleiding geeft op het gebied van informatiebeveiliging, waarbij ook de gehanteerde definities verduidelijkt. Hierbij gaat het in ieder geval om:

- Rubricering
- VIR, VIR-BI, BIR
- Baseline informatiebeveiliging (BIR2017)
- Basis beveiligingsniveau (BBN)
- BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid)
- Classificeren

Voor het samenstellen van deze inleiding kan geput worden uit deel 1 van de BIR2017. 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 goed wordt gevalideerd. Gebruik hiervoor de invulformulieren zoals beschreven in de stappen van de Quickscan Information Security.

Wanneer alle processtappen zijn doorlopen en de voorlopige conclusie is getrokken, is het aan de procesbegeleider om de ingevulde Quickscan Information Security na afloop ter review aan de workshopdeelnemers te sturen. Bij de review is het van belang dat er goed gekeken wordt naar de argumentatie die is gegeven waarom bepaalde keuzes zijn gemaakt.
Na verwerking van de reviewcommentaren wordt de resultaten van de Quickscan Information Security aangeboden aan de proces / systeemeigenaar.

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 DP Den Haag

April 2018 | 111847