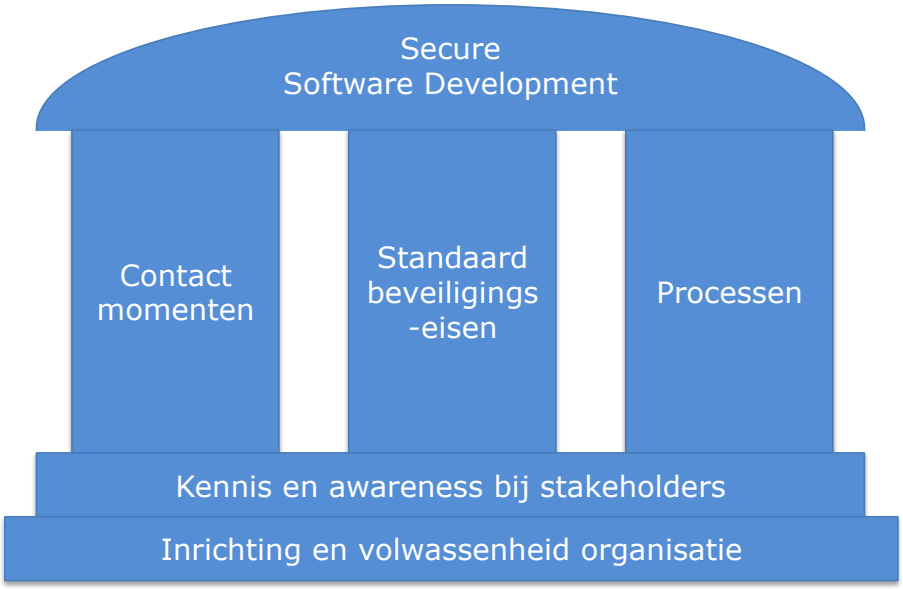
Grip op Secure Software Development (SSD)

'De opdrachtgever aan het stuur'

Versie 2.0



Status	CIP categorie 'Becommentarieerde Practice'	
Opdrachtgever	A. Reuijl	CIP
Auteurs	M. Koers	CIP
	R. Paans	Noordbeek
	R. van der Veer	SIG
	C. Kok	DKTP
	J. Breeman	BKWI
Datum	11 maart 2015	
Filenaam	Grip op SSD De methode v2 0	
URL	www.gripopssd.org	

Voorwoord en leeswijzer

Voor u ligt de handreiking Grip op Secure Software Development (SSD). Deze is opgezet vanuit het perspectief van een opdrachtgever die regisseert en stuurt op de ontwikkeling van gebruikersvriendelijke en veilige applicaties, zonder in te willen breken in het ontwikkelproces van interne/externe softwareleveranciers. Daarmee verrijkt Grip op SSD de internationaal erkende modellen die zijn gericht op softwareontwikkelingsprocessen. Dit document is tot stand gekomen door nauwe samenwerking tussen verschillende partijen (opdrachtgevers, opdrachtnemers en adviesorganisaties) en gebaseerd op uiteenlopende ervaringen en kennis uit de praktijk en literatuur.

Deze handreiking is om twee redenen geschreven. Ten eerste is het een uitdaging om als opdrachtgever van IT-projecten sturing te geven aan het ontwikkelen van veilige IT-diensten. Uitbesteding van ontwikkeling, onderhoud en beheer aan externe leveranciers maakt dit sturingsvraagstuk extra complex. Over en weer zijn er onuitgesproken verwachtingen rondom de informatiebeveiliging. De opdrachtgever verwacht een deskundige leverancier die spontaan de juiste maatregelen treft. Daarentegen verwacht de leverancier dat de opdrachtgever precies specificeert wat er moet gebeuren. Door het ontbreken van expliciete afspraken worden systemen opgeleverd met kwetsbaarheden die niet of te laat worden ontdekt.

Ten tweede bieden bestaande best practices, handboeken en methodieken voor softwareontwikkeling van systemen aan bestuurders en managers geen houvast. In de informatiebeveiliging ligt de nadruk op lange lijsten met passende technische en organisatorische beveiligingsmaatregelen en in de IT-beheerbibliotheken ligt de nadruk op het perfectioneren van processen. Deze documenten leveren geen praktisch toepasbare hulpmiddelen voor de bestuurder die zoekt om kwaliteit, veiligheid en resultaat voor zijn organisatie te waarborgen.

De SSD-methode omvat drie pijlers:

- **Contactmomenten.** De geëigende momenten om te sturen in het softwareontwikkelproces;
- **Standaard beveiligingseisen.** De standaard beveiligingseisen die de basis vormen voor de eisen die aan de leverancier worden gecommuniceerd. Naast deze handreiking is een standaardset beveiligingseisen gedefinieerd en beschikbaar gemaakt op http://gripopssd.org;
- **SSD-processen.** De processen, al dan niet als activiteit binnen de bestaande processen, voor onder meer het bijhouden van risico's en standaard beveiligingseisen en het volwassenheidsniveau van de organisatie.

Hoofdstuk 2 geeft een overzicht van de belangrijkste aspecten en elementen. De Hoofdstukken 3, 4 en 5 beschrijven elk één van de genoemde pijlers in verder detail. Hoofdstuk 6 beschrijft de verschillende actoren/rollen en hun taken. Hoofdstuk 7 beschrijft hoe een organisatie kan beginnen met de SSD-methode en stap voor stap volwassener kan worden.

De auteurs willen met name hun dank uitspreken voor de ondersteuning door de leden van de SSD practitioners community en de bij het samenstellen van dit document betrokken medewerkers van UWV, Noordbeek, SIG, Capgemini, Ordina, DKTP en BKWI.

Amsterdam, februari 2015

Termen en synoniemen

Daar waar 'leverancier' of 'hostingpartij' staat geschreven kan ook de 'interne ontwikkelafdeling' of de 'interne IT-afdeling' worden gelezen, want bij de interactie daarmee bestaan dezelfde uitdagingen.

Voor de actoren zijn generieke namen gebruikt, namelijk 'opdrachtgever', 'beveiligingsadviseur', 'Security Architect' en 'Security Officer', terwijl die in de doelorganisaties verschillende namen kennen. Dit document maakt gebruik van volgende termen en geeft mogelijke synoniemen.

Term	Uitleg	Synoniemen
Leverancier	Dit is een interne of externe partij die de software ontwerpt, bouwt, test en oplevert	Interne ontwikkelafdeling, externe softwareleverancier, bouwende partij, opdrachtnemer, supply-organisatie
Hostingpartij	De partij die de infrastructuur levert waarop de software draait	Interne IT-afdeling, externe hostingpartij, hosting provider
Ontwikkelaar	De persoon die daadwerkelijk de software ontwikkelt	
Opdrachtgever	De persoon die verantwoordelijk is voor het uitgeven van de opdracht tot ontwikkeling	
Organisatie van de opdrachtgever	De organisatie waartoe de opdrachtgever behoort	Demand-organisatie
Ontwikkelproces	Het proces van specificatie en ontwerp tot en met de bouw en ingebruikname van de applicatie	
Software	Zie paragraaf 1.3	
Applicatie	De toepassing van de ontwikkelde software	
IT-systeem	Het samenstel van één of meerdere applicaties en informatie die een gezamenlijke functie aanbieden	Systeem, informatiesysteem
Informatiebeveiliging	Zie paragraaf 1.4	
Risicoanalyse	Zie paragraaf 1.4	

Inhoudsopgave

1	**Inleiding, doelstelling en definities**	**7**
1.1	Aanleiding	7
1.2	Doelstelling	7
1.3	Het object voor Grip op SSD: 'software'	7
1.4	Termen voor Grip op SSD: 'informatiebeveiliging' en 'risicoanalyse'	8
1.5	De actoren voor SSD	8
2	**Pijlers binnen de SSD-methode**	**9**
2.1	Pijler 1: Contactmomenten	10
2.2	Pijler 2: Standaard beveiligingseisen	11
2.3	Pijler 3: SSD-processen	13
3	**De contactmomenten**	**15**
3.1	Het opstellen van specifieke beveiligingseisen	16
3.2	Code review	16
3.3	Security testen	18
3.4	Acceptatie van risico's	18
3.5	Pentesten	19
4	**De standaard beveiligingseisen**	**21**
4.1	Beveiligingsarchitectuur	21
4.2	Baseline security	22
4.3	Classificatie van systemen en gegevens	23
4.4	Maatregelen op basis van attack patterns en bekende dreigingen	25
5	**De processen voor SSD**	**27**
5.1	Business Impact Analyse	27
5.2	Onderhoud van standaard beveiligingseisen	28
5.3	Risicoanalyse	30
5.4	Risicobeheersing en risicoacceptatie	33
5.5	Verantwoording afleggen	33
6	**De organisatorische inrichting van SSD**	**36**
6.1	De opdrachtgever	36
6.2	Beveiligingsadviseurs	36
6.3	(Enterprise) Security Architecten	37
6.4	Security Officers	37
6.5	Technische Security Officers	38
6.6	De leverancier (opdrachtnemer)	39

7 Groeien via en sturen op maturity van SSD 40

7.1 Nulmeting 40
7.2 Definieer het minimum startpunt 40
7.3 Definieer de enterprise security architectuur blokken 41
7.4 Stel het gebruik van de BIA en risicoanalyse verplicht 41
7.5 Vergroot de voorspelbaarheid en optimaliseer 42

Bijlage A: Classificatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid 43
Bijlage B: Het vaststellen van Vertrouwelijkheid 49
Bijlage C: Business Impact Analyse (BIA) methodiek 51
Bijlage D: Risicoanalyse methodiek 56
Bijlage E: CAPEC Attack patterns 63
Bijlage F: Volwassenheidsniveaus 65
Bijlage G: Volwassenheidsniveaus voor SSD 71
Bijlage H: Het gebruik van het dashboard 79
Bijlage I: Referentiedocumentatie 81

1 Inleiding, doelstelling en definities

1.1 Aanleiding

Veel internationale standaarden voor informatiebeveiliging richten zich op de beveiliging van de bestaande systemen en infrastructuur (bijv. netwerken en werkplekken) en minder op softwareontwikkeling. Het ontwikkelen van veilige software wordt veelal gezien als een verantwoordelijkheid van de ontwikkelaar of de leverancier. Door de opdrachtgever worden vaak te weinig eisen gesteld ten aanzien van beveiliging. Leveranciers stellen daarop dat specifieke eisen voor de informatiebeveiliging ontbreken, waardoor door hen geen of onvoldoende aandacht kan worden geschonken aan deze aspecten. Dit leidt ertoe dat zwakheden in de software, systemen of hun inzet in de productieomgeving pas laat tijdens de ontwikkeling of pas in de gebruiksfase worden geconstateerd.

Om meer grip te krijgen op de veiligheid is er behoefte aan een methode die voorafgaand aan de ontwikkeling al eisen voor informatiebeveiliging meegeeft aan de leverancier. Deze eisen moeten passend zijn voor het toepassingsgebied waarbinnen de software wordt ingezet en omvatten tevens het gebruik van bestaande beveiligingsfunctionaliteit. Hierbij is het belangrijk dat er geen overbodige eisen worden gesteld, die onnodig kostenverhogend werken. Om deze reden is gekozen voor een methode met een aanpak, waarbij passende beveiligingseisen worden geformuleerd voor de op te leveren software en waarbij op diverse contactmomenten daarover wordt overlegd met de leverancier. Zo kan gedurende het ontwikkelproces al worden vastgesteld of het systeem zal voldoen aan de gestelde eisen.

1.2 Doelstelling

De doelstelling van een opdrachtgever van IT-projecten met betrekking tot informatiebeveiliging is als volgt:

> *De opdrachtgever wil veilige IT-systemen binnen een veilige infrastructuur, die door de gebruikers op een veilige wijze kunnen worden benut, conform de eisen vanuit de te ondersteunen bedrijfsprocessen.*

Dit document presenteert een Secure Software Development (SSD) methode, die de opdrachtgever in staat stelt sturing te kunnen geven op de resultaten, zonder dat daarbij directe invloed wordt uitgeoefend op het ontwikkelproces. De methode is toepasbaar bij verschillende ontwikkelmethodieken (waterval, agile) en is geschikt voor maatwerk èn standaard pakketten.

1.3 Het object voor Grip op SSD: ‘software’

In dit document wordt gesproken over het opleveren van software. Dit kunnen één of meerdere verschillende opdrachten aan de leverancier zijn, zoals het bouwen van een nieuw informatiesysteem, een nieuwe (web)applicatie, een nieuwe release of een majeure wijziging op een bestaand *informatiesysteem.*

1.4 Termen voor Grip op SSD: 'informatiebeveiliging' en 'risicoanalyse'

In dit document wordt gesproken over 'informatiebeveiliging'. Dit is een verzamelnaam die moet worden gelezen in een brede context en omvat onder andere ook de eisen voor privacybescherming. In dit kader moet ook de term 'risicoanalyse' breder worden gelezen. Indien sprake is van persoonsgerelateerde gegevens, die vallen onder de strekking van de Wet bescherming persoonsgegevens (Wbp) of de Algemene Verordening Gegevensbescherming (AVG), moet ook een Privacy Impact Analyse (PIA) worden uitgevoerd.

1.5 De actoren voor SSD

De SSD-methode is primair ingericht ter ondersteuning van de opdrachtgever. Hierbij moet de opdrachtnemer begrijpen hoe de opdrachtgever tot het formuleren van de eisen is gekomen en welk belang hij of zij daaraan hecht. Daarnaast zijn er de adviespartijen die met hun specifieke kennis de kwaliteit van de processen verder kunnen helpen verbeteren.

De betrokken partijen zijn vaak in drie partijen onder te verdelen:

- Opdrachtgever (de demand organisatie);
  - Bestuurders;
  - Inkoopafdeling;
  - Programma en Project management;
  - Enterprise, Business en IT architecten als vertegenwoordigers vanuit de bedrijfsprocessen;
  - Wijzigingsorganisatie en daarbinnen met name:
    - (Beveiligings-) testteams;
    - (Beveiligings-) beheerorganisatie.
- De organisatie van de leverancier (de supply-organisatie), waaronder:
  - Contractmanagement;
  - Ontwerpers en ontwikkelaars;
  - Testteams.
- De adviesorganisatie(s), waaronder:
  - Beveiligingsadviseur, voor het:
    - Inbedden van de SSD-methode in het demand-supply proces;
    - Inhoudelijke ondersteunen van de demand-organisatie;
    - Begeleiden van en toezien op Security testen.

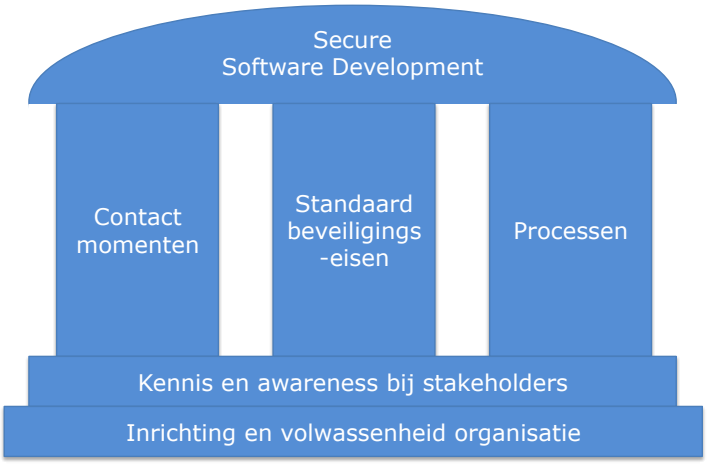
Een gedetailleerde organisatorische inrichting van de SSD-methode en gedetailleerde beschrijving van de actoren, rollen en taken is beschreven in Hoofdstuk 6.

2 Pijlers binnen de SSD-methode

Om te komen tot veilige software, zonder in te hoeven grijpen in het ontwikkelproces voor de software, kent de SSD-methode drie pijlers:

- De contactmomenten;
- De standaard beveiligingseisen;
- De SSD-processen.

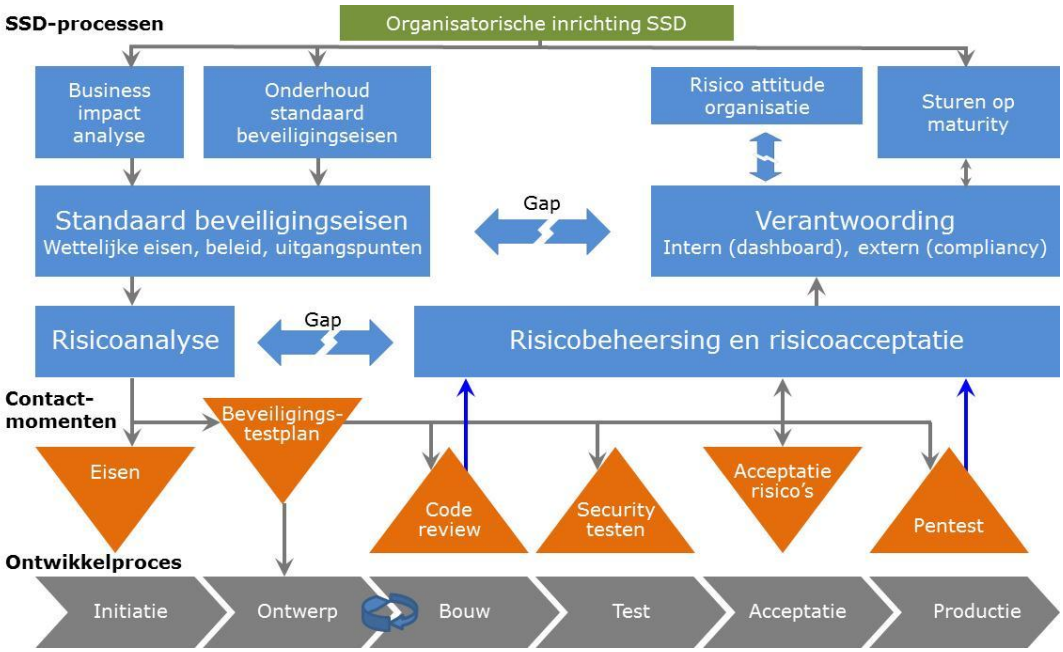
Het fundament onder de pijlers is kennis en awareness bij de beveiligingsadviseurs, procesdeskundigen, architecten, ontwerpers en testers. Via een groeiproces wordt awareness gecreëerd bij de stakeholders en de betrokkenen en wordt kennis en ervaring opgedaan over de te hanteren eisen en processen.



Figuur 1: pijlers van de SSD-methode

Hierbij dient de opdrachtgever te meten of de kennis en awareness daadwerkelijk groeit. Voor dit meetproces zijn volwassenheidsniveaus gedefinieerd die overeenkomen met die van het Capability Maturity Model (CMM). Voor de meeste organisaties is CMM niveau 3 voor SSD afdoende, namelijk 'vastgesteld proces (established)'.

De relatie van de pijlers met het ontwikkelproces is als volgt:

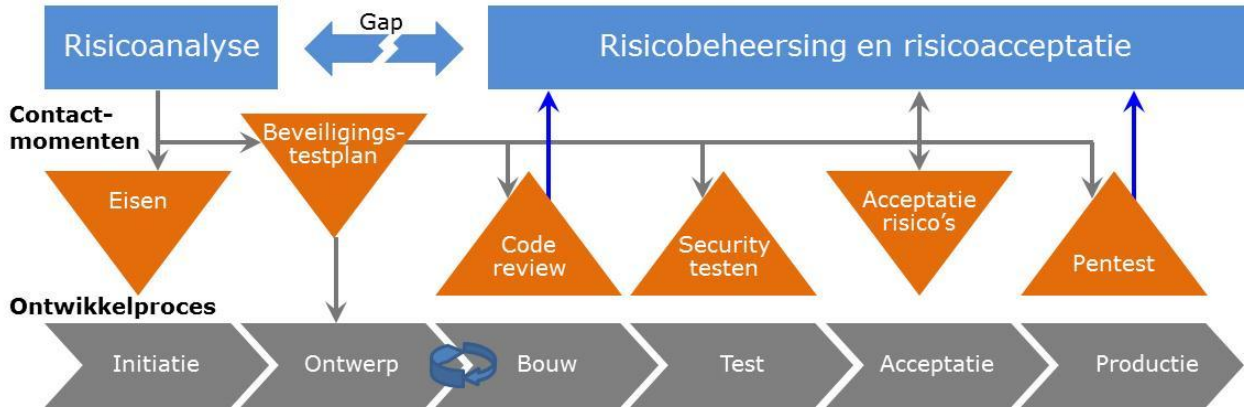


Figuur 2: relatie pijlers van de SSD-methode met het ontwikkelproces

2.1 Pijler 1: Contactmomenten

De SSD-methode gebruikt contactmomenten voor, tijdens en na de ontwikkeling van de software om ervoor te zorgen dat de software voldoet aan de gestelde eisen. Voorafgaand aan de bouw worden de beveiligingseisen gesteld en tijdens en na de bouw wordt gecontroleerd of de software voldoet aan deze eisen. Op de contactmomenten kan, wanneer nodig, tijdens de ontwikkeling worden bijgestuurd.
De vijf contactmomenten zijn:

- Het (op)stellen van de specifieke beveiligingseisen;
- Code reviews;
- Security testen;
- Acceptatie van risico's;
- Pentesten tijdens de implementatie en de gebruiksfase.



Figuur 3: pijler 1 - Contactmomenten

De SSD-methode veronderstelt dat er een formeel en gestructureerd ontwikkelproces bestaat bij de leverancier. De SSD-methode verandert het ontwikkelproces niet, maar brengt er een uitbreiding op aan.

In Hoofdstuk 3 worden de contactmomenten in detail behandeld. Hieronder volgt een beknopte beschrijving.

2.1.1 Het opstellen van specifieke beveiligingseisen

Uit de risicoanalyse volgt een classificatie van het systeem en de gegevens. De opdrachtgever zorgt op basis hiervan voor een verzameling specifieke beveiligingeisen. Zodra de eisen zijn geaccepteerd door de leverancier heeft de opdrachtgever de zekerheid dat de eisen zullen worden toegepast en heeft de leverancier de zekerheid dat er geen nieuwe eisen bij komen. Indien dit wel nodig is, treedt het proces voor change management in werking.

2.1.2 Code reviews

Een code review is een middel om tijdens of na de softwareontwikkeling inzicht te krijgen in het beveiligingsniveau door het bestuderen van broncode en de context daarvan, zoals het ontwerp of de

configuratie. Zo kan, indien nodig, tijdig worden bijgestuurd. De resultaten van de code review worden benut in het acceptatieproces bij de oplevering van de software.

2.1.3 Security testen

Tijdens de ontwerpfase worden de beveiligingseisen geconcretiseerd en verwerkt in het testplan. Het contactmoment 'Security testen' maakt onderdeel uit van het acceptatieproces en heeft tot doel te bepalen of de opgeleverde software voldoet aan de gestelde beveiligingseisen.

2.1.4 Acceptatie van risico's

Na de bouw vindt de formele acceptatie plaats van de software en de risico's. Dit valt onder de verantwoordelijkheid van de opdrachtgever, die daarbij overlegt met de beveiligingsadviseurs.

2.1.5 Pentesten

Een penetratietest (pentest) is een check van één of meer systemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk worden gebruikt om op deze systemen in te breken. Een pentest kan handmatig plaatsvinden, met gebruik van softwareprogramma's, of het kan geautomatiseerd plaatsvinden met softwarepakketten.

2.2 Pijler 2: Standaard beveiligingseisen

Het hebben van de standaard beveiligingseisen voorkomt dat alle maatregelen en daarmee alle beveiligingseisen per project opnieuw moeten worden bedacht. De standaard beveiligingseisen vormen de basis voor het samenstellen van de juiste beveiligingseisen per situatie.
De standaard beveiligingseisen dienen te bestaan uit:

- Beveiligingsarchitectuur;
- Baseline security;
- Classificatie van systemen en gegevens, gericht op de eisen voor Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV);
- Beveiligingsmaatregelen op basis van attack patterns en bekende dreigingen.

Figuur 4: pijler 2 - Standaard beveiligingseisen

Deze eisen kunnen op organisatieniveau worden opgesteld, maar beter nog is te komen tot gemeenschappelijke eisen binnen bedrijfssoorten en binnen de overheid. Het CIP kan een rol spelen bij de samenwerking die daarvoor nodig is.

Bij de risicoanalyse wordt het toepassingsgebied bepaald voor de beveiliging voor een nieuw systeem, een nieuwe release of een majeure wijziging. Hierbij wordt een selectie gemaakt uit de standaard beveiligingseisen, mede op basis van de te verwachten dreigingen. Het resultaat is een lijst van specifieke beveiligingseisen, die aan de leverancier worden overhandigd.

In Hoofdstuk 4 worden de standaard beveiligingseisen in detail behandeld. Hieronder volgt een beknopte beschrijving van de onderdelen.

2.2.1 Beveiligingsarchitectuur

De beveiligingsarchitectuur beschrijft de reeds bestaande beveiligingsmaatregelen in de productieomgeving. De risico's die reeds zijn afgedekt met deze beveiligingsmaatregelen hoeven niet nogmaals te worden afgedekt in de te bouwen applicatie. Deze maatregelen hoeven dus niet te worden meegenomen in de beveiligingseisen, maar dienen voor de leverancier wel inzichtelijk gemaakt te worden zodat wel van deze beveiligingsmaatregelen op een juiste manier gebruik gemaakt wordt.

2.2.2 Baseline security

De baseline security beschrijft de eisen, die vanuit de standaarden zijn geselecteerd die relevant worden geacht voor de organisatie. De baseline security wordt afgestemd met de leveranciers die verantwoordelijk zijn voor het opleveren van veilige systemen. Er is overeenstemming nodig tussen de opdrachtgever en de leverancier over het gebruik van een baseline. De SSD-methode beschrijft hoe dit kan worden ingevuld.

2.2.3 Classificatie van systemen en gegevens

De eindverantwoordelijke voor een bedrijfsproces laat een Business Impact Analyse (BIA) uitvoeren. Hierbij worden de gegevensstromen, informatiesystemen en gegevensverzamelingen in kaart gebracht en geclassificeerd voor de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). De BIV-classificatie wordt gebruikt voor de selectie van specifieke maatregelen

2.2.4 Maatregelen op basis van attack patterns en bekende dreigingen

Een 'attack pattern' is een ordening naar gelijksoortige aanvallen op kwetsbaarheden of zwakke plekken in een systeem of netwerk. De ordening van de risico's naar attack patterns brengt een structuur aan, waarmee de risico's overzichtelijk kunnen worden gehouden. Daarnaast is het van belang dat de bekende dreigingen steeds worden bijgehouden.

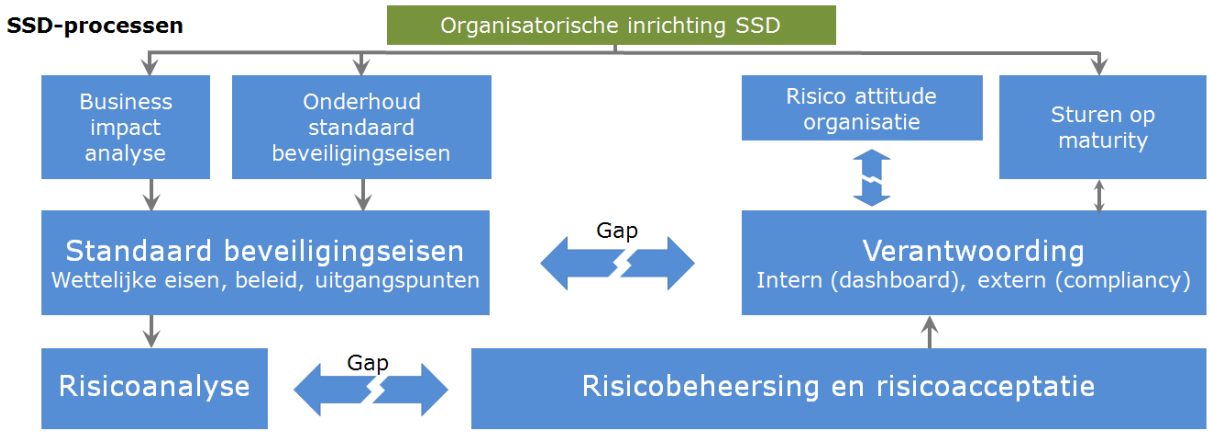
Het is efficiënt om de reeds genomen maatregelen voor risico's en attack patterns bij te houden, ter voorkoming van mogelijke duplicatie van maatregelen.

2.3 Pijler 3: SSD-processen

De opdrachtgever moet een visie hebben hoe sturing en richting te geven aan de veilige ontwikkeling van de software. De SSD-processen ondersteunen de opdrachtgever hierbij. Voor succes moet de opdrachtgever de processen gestructureerd hanteren, met name processen die er voor zorgen dat de beveiligingseisen passend en effectief worden opgesteld en meegenomen.

Binnen de eigen organisatie moeten daartoe processen worden ingericht of bestaande processen worden uitgebreid voor:

- De Business Impact Analyse (BIA);
- Het opbouwen en onderhouden van de verzameling aan standaard beveiligingseisen;
- De risicoanalyse en eventueel de Privacy Impact Analyse (PIA);
- Het afleggen van verantwoording;
- Het sturen op maturity van SSD.



Figuur 5: pijler 3 - SSD-processen

SSD kan alleen een succes worden als dit actief wordt ondersteund en wordt uitgedragen door de opdrachtgever. Deze moet een visie hebben op hoe dit moet worden bereikt voor informatiebeveiliging en moet daarvoor kennis, middelen en menskracht beschikbaar stellen. Degene die het SSD-proces aanstuurt moet een helder mandaat hebben en zich directief kunnen opstellen naar de lijn en de leveranciers.

Door de SSD-processen onderdeel uit te laten maken van de bestaande processen behoeven geen additionele processen ingericht te worden.

De 'Organisatorische inrichting van SSD' wordt in detail beschreven in Hoofdstuk 6. In Hoofdstuk 5 worden de processen voor SSD in detail behandeld. Hieronder volgt een beknopte beschrijving.

2.3.1 Business Impact Analyse

De eindverantwoordelijke voor een bedrijfsproces laat via een expliciete Business Impact Analyse (BIA) de kwaliteitseisen voor de binnen dat bedrijfsproces gebruikte informatiesystemen vaststellen. Het bedrijfsproces verschaft de context waarin de ondersteunende IT-middelen zich bevinden en is bepalend

voor de classificatie per IT-middel. Deze BIV-classificaties vormen het uitgangspunt voor het selecteren van de juiste maatregelen.

2.3.2 Onderhoud van de standaard beveiligingseisen

De standaard beveiligingseisen zijn een levende verzameling van eisen, die wordt aangepast als er nieuwe vormen van aanvallen worden gesignaleerd of als betere technieken voor beveiliging beschikbaar komen. Als de verzameling wordt aangepast, kan dit invloed hebben op de bestaande systemen. Daarom wordt door de beveiligingsadviseurs en security architecten per wijziging een inschatting gemaakt over de mogelijke gevolgen en de eventueel vereiste aanpassingen aan de bestaande systemen.

2.3.3 Risicoanalyse

Het proces voor risicoanalyse per relevant IT-middel is een effectgeoriënteerde aanpak. Díe kwetsbaarheden en risico's worden beschouwd, die inherent zijn aan de gebruikte IT-middelen, in samenhang met de context waarbinnen die IT-middelen worden gebruikt. De risicoanalyse heeft primair tot doel de opdrachtgever te ondersteunen bij het selecteren van de beveiligingseisen die nodig zijn om veilige software op te leveren. Wanneer de organisatie dit nodig acht kan een Privacy Impact Analyse (PIA) worden uitgevoerd.

2.3.4 Risicobeheersing en risicoacceptatie

Tijdens het ontwikkelproces zijn er verschillende contactmomenten waarop risico's inzichtelijk worden gemaakt. Deze risico's kunnen door (aanvullende) beveiligingsmaatregelen gemitigeerd of beheerst worden of geaccepteerd worden. In dit proces is wordt dit per project centraal bijgehouden. Hierdoor heeft de opdrachtgever inzicht in welke risico's zijn gemitigeerd en, nog belangrijker, welke risico's nog open staan.

2.3.5 Verantwoording afleggen

Het afleggen van verantwoording kan zowel intern (middels een dashboard) als extern (middels een compliancy statement). Het SSD-dashboard geeft aan hoe de risicoacceptatie van projecten zich verhoudt tot de risicoclassificatie. Een compliancy statement geeft aan hoe de beveiliging van de software zich verhoudt tot een of meerdere gekozen standaarden.

2.3.6 Sturen op maturity van SSD

De opdrachtgever heeft behoefte aan functionaliteit in de informatiesystemen en wil daarbij zo min mogelijk verstoringen en inbreuken. In dit kader moet de inrichting van SSD worden bewaakt en mogelijk worden verbeterd, totdat SSD daadwerkelijk de risico's voor de bedrijfsprocessen heeft teruggebracht passend bij de risicoattitude van de organisatie. Dit groeiproces vraagt om volwassenheidsniveaus, waarmee een organisatie de methode stapsgewijs kan invoeren en realistische verwachtingen en duidelijke groeidoelstellingen kan formuleren.

De volwassenheidsdoelstellingen, die zijn opgenomen in Bijlage F:, zijn het middel bij het 'sturen op maturity'. Deze zijn gebaseerd op het Capability Maturity Model (CMM) en op maat gesneden voor de SSD-processen.

3 De contactmomenten

Bij de klassieke aanpak van softwareontwikkeling geeft de opdrachtgever een opdracht aan de leverancier en ontvangt na enige tijd het complete product. Na een acceptatieproces wordt dit product daarna in productie genomen.

Voor informatiebeveiliging voldoet deze aanpak in de praktijk niet. De kern van 'veilig bouwen' is betrokkenheid van de opdrachtgever bij diverse fasen van het ontwikkeltraject. Alleen op basis van tussendoor waarnemen en, indien nodig, bijsturen kan men een effectief weerwoord bieden aan de huidige dreigingen voor IT.

SSD gebruikt de volgende vijf contactmomenten voor, tijdens en na de bouw van de software:

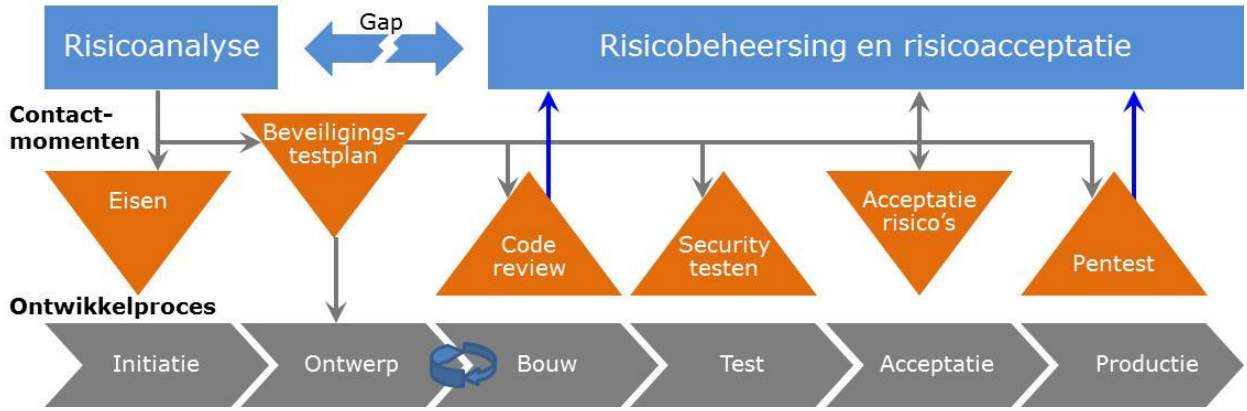
- **Het opstellen van de specifieke beveiligingseisen:**
  Hiermee wordt de leverancier geïnformeerd over welk niveau aan beveiliging wordt verwacht;

- **Code reviews:**
  Tussendoor of achteraf wordt geverifieerd of de juiste maatregelen zijn getroffen;

- **Security testen:**
  De leveranciers laat via het testen bevestigen dat de software voldoet aan de opgelegde specificaties, inclusief de beveiligingseisen en legt de testresultaten voor aan de opdrachtgever;

- **Acceptatie van risico's:**
  Als wordt besloten dat men niet kan of wil voldoen aan een bepaalde beveiligingseis, moet dit besluit door de opdrachtgever worden bevestigd via een expliciete risicoacceptatie;

- **Pentesten:**
  Hiermee wordt tijdens de implementatie en gebruiksfase geverifieerd dat de triviale risico's van openstaande verbindingen, standaard wachtwoorden of achterblijvende onderhoudsniveaus zijn afgedekt.



Figuur 6: de contactmomenten

In feite lijkt het bouwen van veilige software op het bouwen van een huis. Terwijl de medewerkers van de aannemer, de loodgieter, de installateur en diverse leveranciers bezig zijn, kijkt de nieuwe huiseigenaar (opdrachtgever) rond of er wordt gebouwd conform zijn of haar verwachting. De nieuwe huiseigenaar wil namelijk niet voor onplezierige verrassingen staan op het moment van de sleuteloverdracht.

3.1 Het opstellen van specifieke beveiligingseisen

Voor het ontwikkelen of modificeren van software is het eerste contactmoment binnen SSD het opstellen van de specifieke beveiligingseisen. Bij het definiëren van de eisen voor software wordt een risicoanalyse uitgevoerd om toepasselijke beveiligingseisen te bepalen. Op basis van de risicoanalyse en eventueel de PIA worden de relevante eisen geselecteerd en doorgenomen met de leverancier. Het proces van de risicoanalyse wordt in detail beschreven in paragraaf 5.2.

Het opstellen van beveiligingseisen gebeurt doorgaans eenmalig per project of release. Deze eisen worden meegenomen in de Project Start Architectuur (PSA) of in het Functioneel Ontwerp (FO). Bij een aanbesteding worden de eisen opgenomen in het Programma van Eisen (PvE).

De specifieke beveiligingseisen zijn een op de opdracht toegesneden deelverzameling van de standaard beveiligingseisen. Veelal hebben deze beveiligingseisen betrekking op eigenschappen die verweven zijn in de software. Een leverancier zal deze eisen niet stuk voor stuk behandelen en ‘afvinken’. Ontwerpers en bouwers zullen zelf vanuit een integraal concept uitwerken om te zorgen dat aan het gehele stelsel van eisen wordt voldaan, gebruikmakend van hun eigen bouwstenen en methoden.

Voor de specifieke beveiligingseisen geldt het principe ‘Comply or Explain’. Als de leverancier niet wil of kan voldoen aan een bepaalde eis, moet dit samen met de afweging aan de opdrachtgever worden vermeld en moet bij de opdrachtgever het proces voor risicoacceptatie worden doorlopen.

Het valt aan te raden met de leverancier(s) vóór de contractering te overleggen over de inhoud van de standaard beveiligingseisen waaruit de specifieke beveiligingseisen voortvloeien. Enerzijds voorkomt dit verrassingen bij het geven van de specifieke opdrachten, doordat de leveranciers weten welke beveiligingseisen zij kunnen verwachten. Bij hun prijsstelling kunnen zij al rekening houden met deze eisen. Anderzijds leert de ervaring dat leveranciers vaak waardevolle aanvullingen of feedback geven op beveiligingseisen, die de kwaliteit en effectiviteit van de eisen kunnen verbeteren.

3.2 Code review

Om beveiligingsrisico’s van software te bepalen kan de broncode worden onderworpen aan onderzoek via een zogenaamde code review. Gezien de kosten van dit type onderzoek wordt dit vaak alleen uitgevoerd als uit de Business Impact Analyse (BIA) blijkt dat er sprake is van een substantieel te beschermen belang.

3.2.1 Het doel van een code review

Bij een code review zoeken specialisten naar kwetsbaarheden door het systematisch bestuderen van code, ontwerp, configuratie en documentatie, vaak gebruikmakend van analysetools . Dit kan de vorm

hebben van 'pair programming', 'informal walkthroughs' of 'formal inspections' en wordt eventueel aangevuld met interviews.

Het doel van een code review is het vinden en oplossen van fouten in de software, die door de ontwikkelaars over het hoofd zijn gezien. Voorbeelden hiervan zijn 'format string exploits', 'race conditions', 'memory leaks' en 'buffer overflows'. Een nevendoel is het verbeteren van de competenties van de ontwikkelaars om te voorkomen dat zij die fouten nogmaals maken.

3.2.2 Te reviewen risicogebieden

Een code review kan beveiligingsrisico's signaleren, waarbij met name aandacht is voor de volgende gebieden:
Datatransport;

- Dataopslag;
- Data- en systeemautorisatie;
- Input- en output-validatie;
- Bewijssterkte en compleetheid van logging;
- Unieke identificatie van gebruikers;
- Zorgvuldig omgaan met wachtwoorden binnen de systemen en gegevensverzamelingen;
- Toegangsmanagement;
- Sessiemanagement;
- Gebruikersmanagement;
- Onderhoudbaarheid. Slecht onderhoudbare broncode kan dit leiden tot fouten bij aanpassingen. Die fouten kunnen weer leiden tot nieuwe kwetsbaarheden of datalekken;
- Testbaarheid;
- Beschikbaarheid. Door het beperken van Single Points of Failure en het isoleren van foutafhandeling kan worden voorkomen dat de software onbeschikbaar wordt bij een beveiligingsincident;
- Performance. Door het beperken van bottlenecks kan worden voorkomen dat de software ongewenst traag wordt bij een beveiligingsincident, zoals een DDoS aanval.

3.2.3 Code review en pentesten vullen elkaar aan

Een code review kan beveiligingsrisico's zichtbaar maken die een pentest niet vindt. Daarnaast kan een code review worden toegepast in elke fase van de ontwikkeling, terwijl een pentest alleen kan worden uitgevoerd op werkende software. Bij een code review worden in de regel meer kwetsbaarheden gevonden dan bij een pentest, omdat het inzichtelijk is waar kwetsbaarheden zich bevinden.

Desalniettemin blijft de pentest een belangrijke toets op de beveiliging, om te zorgen voor meer zekerheid en ook de software te toetsen in samenhang met de infrastructuur en andere software. De zekerheid wordt grotere omdat een code review een interpretatie is van broncode en die interpretatie kan fouten bevatten. De reviewer kan zaken over het hoofd zien of verkeerde aannames maken. De samenhang met infrastructuur en andere software is belangrijk omdat hierdoor nieuwe kwetsbaarheden geïntroduceerd kunnen worden.

Ook als men een code review uitvoert, blijft de pentest noodzakelijk. De beide aanpakken vullen elkaar aan.

3.3 Security testen

Bij de risicoanalyse worden aandachtspunten opgesteld voor het uiteindelijke testen van de op te leveren software, onder andere op basis van de 'misuse and abuse cases'. In de ontwerpfase wordt het testplan opgesteld, waarbij rekening wordt gehouden met deze mogelijkheden voor verkeerd gebruik en misbruik van functionaliteit en gegevens.

In de testfase van de software wordt aan de hand van het testplan gecontroleerd of de software voldoet aan de functionele eisen, de kwaliteitseisen en de beveiligingseisen. Testen en toetsen is een standaard onderdeel van ieder ontwikkelproces. In het kader van SSD moet dit proces worden uitgebreid met het expliciet testen op het voldoen aan de beveiligingseisen.

Voor testen en toetsen in een pragmatische insteek nodig. Hierbij geldt als kanttekening dat een 100 % test alleen mogelijk is tegen hoge kosten. Zo een volledige test geeft alleen de zekerheid dat wordt voldaan aan de gestelde beveiligingseisen, maar bevestigt niet dat het systeem daadwerkelijk volkomen veilig is.

Het verdient aanbeveling om bij testen en toetsen van de ontwikkelde software ook de relatie met eventuele gekoppelde interne en externe systemen te toetsen. Die systemen vallen weliswaar niet binnen de scope van de testfase, maar spelen wel een rol bij het mitigeren van de beveiligingsrisico's van een applicatie. Een ketting is zo sterk als zijn zwakste schakel.

Indien een test door zijn aard of complexiteit beter alleen door de leverancier of een derde partij kan worden uitgevoerd, dan verifieert (toetst) de opdrachtgever de testresultaten. Veelal worden deze testen uitgevoerd door de leverancier. De resultaten worden overlegd aan de opdrachtgever, die deze voor de beveiligingseisen laat verifiëren.

Eventuele afwijkingen worden vastgelegd in een afwijkingsrapportage en worden meegenomen in de risicoacceptatie.

3.4 Acceptatie van risico's

Indien bij de voorgaande contactmomenten is gebleken dat aan één of meer van de beveiligingseisen niet is voldaan, volgt het proces van risicoacceptatie door de opdrachtgever. Er wordt in dat proces een afweging gemaakt om de software niet te accepteren of om de afwijking(en) te accepteren. Dit laatste kan bijvoorbeeld als de ernst van de bevindingen laag is of de kosten van een eventueel herstel te hoog zijn. Als de afwijking betrekking heeft op meerdere bedrijfsonderdelen, dient de opdrachtgever bij de besluitvorming over risicoacceptatie zijn collega's te raadplegen.

De opdrachtgever maakt, in overleg met de beveiligingsadviseurs, de volgende afweging:

- **De applicatie voldoet en wordt geaccepteerd:**
  De software voldoet volledig aan de beveiligingseisen, wordt geaccepteerd en kan in productie worden genomen;

- **De software voldoet niet en moet worden aangepast:**
  De software voldoet niet aan de beveiligingseisen. De software moet worden aangepast en opnieuw worden getest, om vervolgens weer ter goedkeuring te worden aangeboden;

- **De software voldoet niet, maar wordt tijdelijk gedoogd:**
  De software voldoet niet aan de beveiligingseisen, maar het oplossen van de afwijkingen is minder belangrijk dan de noodzaak de software in productie te nemen. De onvolkomenheid wordt tijdelijk gedoogd en er wordt een plan opgesteld om de afwijking te herstellen en/of een mitigerende maatregel in te voeren;

- **De beveiligingseisen worden niet geaccepteerd:**
  De beveiligingseisen sluiten bij nader inzien niet aan op de eisen van de business. Dan worden de specifieke beveiligingseisen aangepast. De opdrachtgever bepaalt of de software desondanks toch in gebruik mag worden genomen en de gewijzigde eisen in een volgend release worden meegenomen, of dat de software eerst moet worden aangepast.

3.4.1 Afspraken voor een gedoogperiode

Wanneer de software niet voldoet aan de beveiligingseisen en de onvolkomenheid tijdelijk wordt gedoogd, gelden de volgende afspraken:

- Er is een uitgewerkt plan met een business case beschikbaar, waarin wordt beschreven hoe en wanneer de gedoogoplossing zal worden gemigreerd naar een formeel goedgekeurde situatie;
- Het plan geeft aan welk budget benodigd is en toont aan dat dit budget beschikbaar is, inclusief eventuele meerkosten of minderkosten voor exploitatie;
- Het plan is goedgekeurd door de opdrachtgever.

De in het plan beschreven eindsituatie, inclusief de eventuele tussenstappen er naar toe, moet voldoen aan de specifieke beveiligingseisen.

3.5 Pentesten

Een penetratietest (pentest) is een check tijdens de implementatie en de gebruiksfase van één of meer systemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk worden gebruikt om op deze systemen in te breken. Een pentest kan met de kennis van een pentester, met gebruik van softwareprogramma's, handmatig plaatsvinden.

Een pentest kan ondersteund worden door geautomatiseerde testen, waarbij onder andere geverifieerd wordt of er geen triviale verbindingsmogelijkheden of functionaliteiten onbeveiligd open staan, die niet nodig zijn voor het functioneren van het systeem. Deze meer triviale testen worden aangeduid als "vulnerability scan". Tijdens deze vulnerability scans worden onder andere onderhoudsniveaus gecontroleerd van de middleware, de platformen en de netwerkcomponenten.

Voor het uitvoeren van pentesten is in aanvulling van een vulnerability scan kennis van een pentester noodzakelijk. Ook wordt in de pentest in aanvulling op de vulnerability scan geverifieerd dat de openstaande functionaliteit niet tot misuse of abuse van het systeem kan leiden.

De gebruikelijke vormen van een pentest zijn:

- **Black box testing:** hierbij probeert een specialist de software aan te vallen zonder kennis van de infrastructuur en werking van de software op voorhand, om een echte hacker te simuleren. Hierdoor is het niet altijd mogelijk om die problemen te vinden die zich diep in de software bevinden als het probleem geen waarneembaar afwijkende uitvoer heeft. Hoe omvangrijker de te testen software is, hoe minder effectief black box testen zijn;
- **Grey box testing:** hierbij probeert een specialist de software aan te vallen met rudimentaire kennis van de infrastructuur en de interne werking van de software op voorhand;
- **White box testing of crystal box testing:** hierbij probeert een specialist de software aan te vallen met inzicht in de broncode;
- **Monkey testing:** een speciale tactiek waarbij willekeurig interacties worden uitgevoerd met de software op zoek naar een kwetsbaarheid. De geautomatiseerde variant hiervan heet ‘fuzzing’.

Pentesten maken het mogelijk om voorafgaand aan de acceptatie en ingebruikname te sturen op risico’s die zich voordoen in de productieomgeving. Pentesten kunnen aanleiding zijn de beveiligingseisen uit te breiden.

4 De standaard beveiligingseisen

De standaard beveiligingseisen vormen de kennisbron voor het toepassen van de SSD-methode. Deze bestaan uit:

- Beveiligingsarchitectuur, veelal bestaat deze uit verschillende blokken met beveiligingsmaatregelen;
- Baseline security, gebaseerd op de gangbare standaarden;
- Classificatie van systemen en gegevens, gericht op de eisen voor Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV);
- Beveiligingsmaatregelen op basis van attack patterns en bekende dreigingen.

Figuur 7: de standaard beveiligingseisen

Bij de risicoanalyse wordt het toepassingsgebied bepaald voor de beveiliging voor de op te leveren software. Hierbij wordt een selectie gemaakt uit de standaard beveiligingseisen, mede op basis van de te verwachten dreigingen. Het resultaat is een lijst van specifieke beveiligingseisen, die aan de leverancier worden overhandigd.

4.1 Beveiligingsarchitectuur

De enterprise security-architectuur legt de beveiligingsmaatregelen vast die al zijn genomen binnen de eigen organisatie. De architectuur heeft tot doel bij te dragen aan synergie en beschrijft daartoe de samenhang tussen de verschillende beveiligingsmaatregelen.

Veelal is de enterprise security architectuur verdeeld in blokken, gericht op specifieke groepen componenten in de infrastructuur. Voorbeelden hiervan zijn de Active Directory, de netwerkcomponenten en diverse vormen van middleware en platformen. Dat voorkomt dat bedrijfsbrede beveiligingsmaatregelen versnipperd worden ingericht en beheerd. Dit geldt ook voor de informatie die daarbinnen is opgeslagen. Deze blokken zijn overigens vaak geen losse entiteiten, maar onderdeel van de overkoepelende enterprise architectuur. Het hebben van een kwalitatief goede (volwassen) beveiligingsarchitectuur vraagt om het hebben van een kwalitatief goede enterprise architectuur.

In ketenverband kunnen sommige van de beveiligingsmaatregelen ook buiten de eigen organisatie liggen, zoals de DigiD voorzieningen. Indien gebruik wordt gemaakt van DigiD zijn risico's voor de authenticatie van burgers al bekend, evenals de daarvoor benodigde maatregelen.

De architectuur kan ook belemmeringen en beperkingen aangeven. Zo worden authenticatie- en autorisatiegegevens soms gebruikt voor doelbinding en voor het bewaken van functiescheiding. Op het moment dat wordt overgeschakeld naar een federatief ketenbreed stelsel voor Identity & Acces Management (IAM), werkt dit niet meer. Voor doelbinding en functiescheiding moet dan een alternatief worden gevonden.

Door het delen van de kennis over de architectuur blokken is het mogelijk beveiligingsfuncties te hergebruiken. Hergebruik leidt tot minder additionele kwetsbaarheden en vereenvoudigt de testwerkzaamheden. Hierbij past een actieve samenwerking met de leverancier en de hostingpartij.

4.2 Baseline security

Een baseline heeft het karakter van een best practice. Hierdoor zijn verdergaande afspraken per situatie noodzakelijk. Dit kan enerzijds gebeuren door de leverancier de best practice te laten concretiseren in een beveiligingsplan- of aanpak en deze per situatie formeel te laten vastleggen.
Voor de beveiliging van software zijn met name de volgende internationale standaarden van belang:

- **ISO 27002:2005:**
  Deze standaard behandelt de mogelijke beveiligingsmaatregelen als best practices en vormt een goede basis voor de selectie van maatregelen voor een specifieke situatie. Hoofdstuk 12 'Information systems acquisition, development and maintenance - building security into applications' beschrijft de richtlijnen en adviezen voor het verwerven, ontwikkelen en beheer van software;
- **ISO/IEC 27002:2013:**
  Deze update omvat een aantal nieuwe hoofdstukken en maatregelen ten opzichte van de standaard ISO 27002:2005 en zijn maatregelen verdiept en herschikt. Daarnaast zijn deze geüpdate naar de huidige stand der techniek en is in de nieuwe versie meer aandacht voor leveranciersrelaties. In de 2013-versie is hoofdstuk 12 vervangen door hoofdstuk 14 met dezelfde naam.
  Door de verschillen kunnen de versies niet door elkaar gebruikt worden;
- **BIR:**
  De Baseline Informatiebeveiliging Rijksoverheid (BIR) is afgeleid van de ISO 27002:2005 en bevat 50 aanvullende vuistregels als een best practice. Door de (semi) overheidsinstanties wordt gebruik gemaakt van de BIR, echter op de verschillende overheidslagen bestaan variaties op de BIR:
  - Voor gemeenten de BIG
  - Voor waterschappen de BIWA
  - Voor provincies de Interprovinciale Baseline Informatiebeveiliging (IBI);
- **ISO 27034:**
  Deze standaard bevat in Hoofdstuk 4 'Application Security Validation' (in ontwikkeling) een normenkader dat is toegespitst op de beveiligingsmaatregelen bij de bouw van software. Het normenkader is code-centrisch en is bedoeld als meetbaar hulpmiddel voor de ontwikkelaars;
- **OWASP Application Security Verification Standard:**
  De OWASP ASVS biedt een basis om de beveiligingsmaatregelen van webapplicaties te testen;
- **ISO 25010:**
  Deze standaard biedt een denkraam voor beveiliging als kwaliteitseigenschap van software en beschrijft uitputtend de verschillende aspecten waarover afspraken gemaakt dienen te worden.

De baseline kan worden uitgebreid met extra normen die door de opdrachtgever als noodzakelijk worden bestempeld voor de specifieke situatie van de eigen organisatie en met de technologiestacks in de productieomgeving.

Bij het maken van deze handreiking is ook een overzicht gemaakt van beveiligingseisen op basis van onder andere de bovengenoemde standaarden en de input van security experts. Op de website http://gripopssd.org is de standaard set beveiligingseisen beschikbaar, alsook standaard contracten en trainingsmateriaal.

De organisatie dient een selectie te maken uit de normen en maatregelen van de gangbare standaarden. Hiervoor is een Business Impact Analyse (BIA) nodig, waarbij de specifieke beveiligingsbehoeften van de bedrijfsprocessen in kaart wordt gebracht. Op basis van de specifieke situatie van de organisatie wordt de baseline samengesteld.
Een meer pragmatische aanpak is integrale adoptie van het BIR. Deze is opgezet op basis van de gemiddelde behoefte van (semi) overheidsinstanties en mag worden geïmplementeerd op basis van 'Comply or Explain'. Hierdoor is de opdrachtgever gerechtigd aan te geven welke normen en maatregelen uit het BIR wel of niet worden geïmplementeerd binnen de eigen organisatie en wordt zo een passende baseline neergezet.

4.3 Classificatie van systemen en gegevens

De opdrachtgever stelt het belang van de bedrijfsprocessen en de software vast door de software en gegevens in te delen naar beveiligingsklassen. De klassen zijn ingedeeld conform de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV), zoals verder is toegelicht in Bijlage A. Voor iedere klasse geldt een minimale basis van de te stellen beveiligingseisen en de te nemen beveiligingsmaatregelen, zoals het wel of niet het opleggen van onweerlegbaarheid bij het invoeren van een transactie, het wel of niet versleutelen van gegevens etc.

De basis voor de inrichting van de informatiebeveiliging in een organisatie is ISO27001 en ISO27002, die integraal zijn opgenomen in de 'Baseline Informatiebeveiliging Rijksdienst (BIR)'. De onderstaande tabel bevat een overzicht van de classificatieniveaus, waarin de BIR als baseline is gearceerd.

Kwaliteitsaspect	**Het belang**			
Beschikbaarheid	Hoog	Midden	Laag	
Integriteit	Hoog	Midden	Laag	
Vertrouwelijkheid	Strikt Vertrouwelijk, Risicoklasse 3	Vertrouwelijk, Risicoklasse 2	Intern, Risicoklasse 1	Openbaar, Risicoklasse 0

De baseline voor informatiebeveiliging is gericht op:

- Het standaardniveau voor Beschikbaarheid is Midden;
- Het standaardniveau voor Integriteit is Midden;
- Het standaardniveau voor Vertrouwelijkheid is gebaseerd op de vereisten voor Vertrouwelijk of Risicoklasse 2.

Alleen door middel van een risicoanalyse kunnen de niveaus
naar boven of naar beneden worden bijgesteld.

De BIV-classificatie wordt gebruikt voor de selectie van specifieke maatregelen, zoals het wel of niet het opleggen van onweerlegbaarheid bij het invoeren van een transactie, het wel of niet versleutelen van gegevens etc.

4.4 Maatregelen op basis van attack patterns en bekende dreigingen

In de praktijk worden bij de risicoanalyses veelal risico's per project geïnventariseerd, zonder dat men weet wat andere projectleiders binnen de organisatie doen. Dit leidt tot incomplete en ad hoc lijsten van risico's, waardoor er geen sprake is van een samenhangende risicobeheersing.

Binnen de SSD-methode worden de risico's centraal bijgehouden. Hierdoor wordt bij iedere risicoanalyse uitgegaan van hetzelfde overzicht aan risico's, waarbij tijdens de risicoanalyse wordt bepaald welke daarvan wel of niet relevant zijn voor de betreffende software.

De opdrachtgever laat de lijst van bekende risico's opbouwen aan de hand van:

- De classificatie van systemen en gegevens;
- Het analyseren van de kwetsbaarheden binnen de productieomgeving;
- Het gebruikmaken van attack patterns die beschikbaar zijn gesteld op publieke bronnen of via leveranciers van beveiligingsoplossingen;
- Het opstellen van profielen van mogelijke aanvallers.
- Publieke bronnen voor attack patterns en dreigingen zijn onder andere:
- NCSC 'Whitepaper ICT-beveiligingsrichtlijnen voor webapplicaties' met voorbeelden van risico's en maatregelen;
- SANS Institute 'Top 20 list of security vulnerabilities' met voorbeelden van zwakheden door bekende programmeerfouten;
- MITRE 'Common Vulnerabilities and Exposures (CVE)';
- US-CERT 'Technical Cyber Security Alerts';
- Microsoft 'Security Advisory';
- OWASP 'Top 10' met de meest voorkomende kwetsbaarheden in webapplicaties;
- CAPEC.

4.4.1 TSP en CAPEC

Het framework Team Software Process (TSP) van het Software Engineering Institute (SEI) biedt een gestructureerde aanpak voor het opstellen van eisen voor software. Hierbij is TSP-Secure specifiek gericht op het formuleren van beveiligingseisen. Inschatting van dreigingen kan gebeuren via CAPEC. CAPEC is een openbare, door de community ontwikkelde lijst van 1.000 attacks, geordend naar patterns. Iedere attack is voorzien een uitleg. Deze lijst is een goede basis om met de leverancier van software afspraken te maken over hoe wordt omgegaan met bekende attacks en welke maatregelen daar standaard voor worden getroffen. In Bijlage E: is een relevant deel van de CAPEC-1.000 lijst opgenomen.

CAPEC heeft als nadeel dat deze is opgesteld voor beveiligingsadviseurs, ontwikkelaars en testers. De lijst is heel gedetailleerd en daardoor niet goed bruikbaar voor een risicoanalyse vanuit het oogpunt van de bedrijfsprocessen.

4.4.2 Centrale lijst met attack patterns en dreigingen

De centrale lijst met attack patterns en dreigingen is bedoeld voor het gestructureerd uitvoeren van een risicoanalyse. Deze lijst kan tevens worden gebruikt voor:

- **Testen:**
  Attack patterns lenen zich door hun concrete karakter goed voor het opzetten van testen. Hierbij geldt dat voor bekende dreigingen vaak al geautomatiseerde hulpmiddelen bestaan voor het testen;

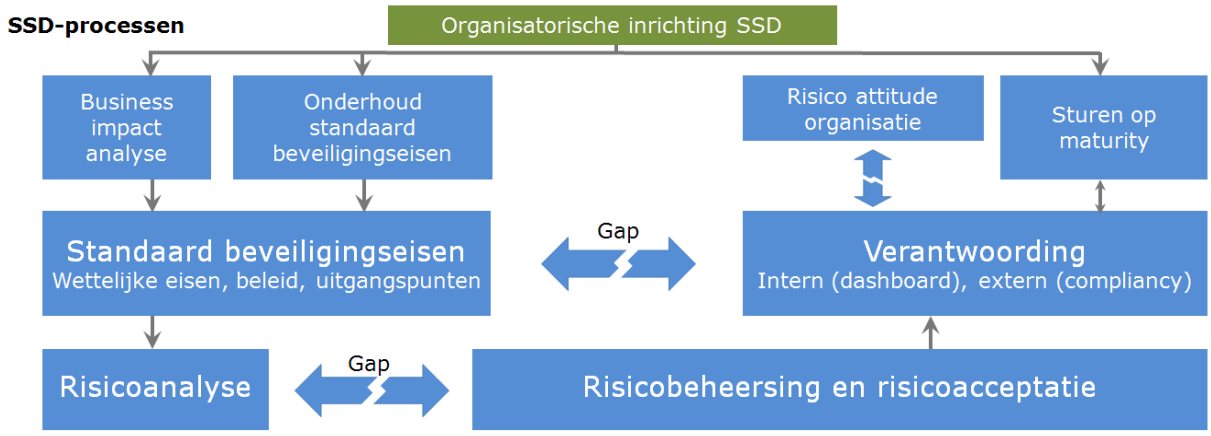
- **Awareness:**
  Het voordeel van het delen van de inhoud van de lijst met betrokkenen, partners en leveranciers is dat dit bijdraagt aan de awareness binnen en buiten de eigen organisatie;

- **Kennisdeling:**
  Door te delen kan de kennis van andere partijen worden benut om te komen tot een betere lijst en kan informatie over eventuele maatregelen worden gedeeld.

Belangrijk is dat steeds de relatie wordt beschouwd tussen enerzijds de attack patterns en dreigingen en anderzijds de beveiligingsmaatregelen. Hierbij kan worden aangegeven welk risico bestaat door het niet hebben van een bepaalde maatregel. Dit is van direct belang voor het proces van risicoacceptatie.

5 De processen voor SSD

De processen/activiteiten voor SSD worden primair ingericht bij de opdrachtgever, maar daarbij moeten de leveranciers zorgen voor gesprekspartners en inhaken op de wensen van de opdrachtgever. SSD kan alleen succesvol zijn als de processen/activiteiten aan beide zijden van de demand-supply relatie worden opgepakt en ingevuld.



Figuur 8: de SSD processen

5.1 Business Impact Analyse

Verschillende industriestandaarden (zoals ISO 27001/2) schrijven voor dat de opdrachtgever verantwoordelijk is voor een effectieve werking van de maatregelen voor informatiebeveiliging. In dit kader dient de opdrachtgever:

- Op basis van een expliciete Business Impact Analyse (BIA) de kwaliteitseisen voor de binnen een bedrijfsproces gebruikte informatiesystemen vast te stellen. De bedrijfsprocessen verschaffen de context waarin de ondersteunende IT-middelen zich bevinden en zijn bepalend voor de BIV-classificatie per IT-middel;
- Zich op basis van de BIA inzicht te vormen over:
  - De primaire en secundaire bedrijfsprocessen, die noodzakelijk zijn voor de uitvoering van de kerntaken;
  - De doelstellingen van ieder bedrijfsproces;
  - De uitwerking van ieder bedrijfsproces in deelprocessen en informatiestromen;
  - De IT-middelen die noodzakelijk zijn voor de uitvoering van die deelprocessen en voor het in stand houden van de informatiestromen;
  - De relevante dreigingen voor deze IT-middelen;
  - De vereisten voor de borging van de kwaliteitsaspecten “Beschikbaarheid, Integriteit en Vertrouwelijkheid” (BIV) zijn van de dienstverlening per IT-middel.
- Per IT-middel een risicoanalyse uit te laten voeren, waarna de minimaal vereiste maatregelen worden geselecteerd;
- De juiste maatregelen te laten implementeren en uit te dragen;

- Vast te stellen dat de getroffen maatregelen aantoonbaar overeenstemmen met de beveiligingseisen en dat deze maatregelen daadwerkelijk worden nageleefd;
- Periodiek het geheel van de beveiligingseisen en het stelsel van beveiligingsmaatregelen te laten evalueren.

De uiteindelijke uitkomst van de BIA door de organisatie is een lijst van relevante IT-middelen met bijbehorende BIV-classificaties. Deze uitkomst dient als basis voor de standaard beveiligingseisen. De risicoanalyse (zie paragraaf 5.3) leidt tot specifieke beveiligingseisen en beveiligingsmaatregelen per IT-middel.

In Bijlage C: worden achtereenvolgens de overwegingen en stappen besproken om vanuit het bedrijfsproces tot een lijst van BIV-classificaties te komen voor de relevante IT-middelen.

5.2 Onderhoud van standaard beveiligingseisen

Beveiligingseisen zijn afgeleid van de strategische doelstellingen en de risicoattitude van de organisatie en met name die van senior management. De risicoattitude is afgeleid van de bedrijfswaarden en het beschikbare budget. Voor een deel worden de uitgangspunten bepaald door externe factoren, zoals wet- en regelgeving, begrotingseisen en andere eisen waaraan de organisatie moet voldoen.

Het is niet de intentie van de organisatie alle risico's koste wat het kost te voorkomen, maar te komen tot een bewuste afweging van de kosten van maatregelen versus de mogelijke te voorkomen schade. Als maatregelen weloverwogen niet worden genomen, moet bekend zijn waarom zo is besloten. Hiertoe is het proces voor een formele risicoacceptatie ingericht. Bij de afwegingen spelen begrippen zoals 'risk appetite' en 'risicocriteria' een rol.

Het onderhoud van standaard beveiligingseisen bestaat uit twee activiteiten: het opstellen van de eisen en het onderhouden van eisen. De beveiligingsadviseurs en security architecten bewaken de actualiteit van de verzameling standaard beveiligingseisen. Daarvoor zijn diverse bronnen beschikbaar, zoals NCSC, OWASP en NIST.

5.2.1 Het opstellen van standaard beveiligingseisen

De standaard beveiligingseisen vormen de kennisbron voor het toepassen van de SSD-methode. Hun kwaliteit is een essentiële voorwaarde voor het succesvol implementeren van SSD. De opdrachtgever dient een proces in te richten om deze kennisbron initieel op te bouwen. Deze opbouwactiviteit omvat onder andere:

- **Eigenaarschap:**
  Voor alle onderdelen van de standaard beveiligingseisen moeten eigenaren worden aangewezen en gemandateerd, die verantwoordelijk zijn voor de inhoud en het onderhoud van hun gedeelte. Deze eigenaren moeten met gezag kunnen optreden, zodat zij in staat zijn de synergie en de effectiviteit van de standaard beveiligingseisen te borgen en uit te dragen;

- **Beveiligingsarchitectuur:**
  Architecten beschrijven de verschillende blokken, zoals voor het centrale netwerk en de decentrale netwerken, de werkstations, de verschillende typen platformen etc. Voor ieder van

deze blokken moet een Security Architect de beveiligingsaspecten uitwerken en de beveiligingsmechanieken functioneel beschrijven, zoals voor identificatie, authenticatie, autorisatie, versleuteling, logging, monitoring, rapportage etc. Het doel van deze beschrijving is projectleiders, ontwikkelaars etc. handvatten te bieden om gebruik te maken van de reeds bestaande beveiligingsmechanieken en te zorgen voor synergie;

- **Baseline security:**
  Beveiligingsadviseurs moeten een selectie maken uit de normen en maatregelen zoals die zijn beschreven in de gangbare standaarden, zoals genoemd in paragraaf 4.2 en 4.4. De beveiligingsadviseurs maken deze selectie op basis van hun ervaring met het bestaande applicatielandschap, de bestaande infrastructuur en hun kennis van de dreigingen voor de bedrijfsprocessen;

- **Classificatie van systemen en gegevens:**
  De classificatie van systemen en gegevens kan gekoppeld worden aan de verplichte toepassing van een minimale set van de standaard beveiligingseisen. De opdrachtgever laat aan de hand van Bijlage C: organisatiespecifieke criteria opstellen voor de classificatie voor Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) en laat deze classificatie hanteren binnen de bedrijfsprocessen. Achtereenvolgens worden Business Impact Analyses (BIA's) uitgevoerd voor de verschillende systemen en gegevensverzameling. Daarbij worden de BIV-classificaties toegekend aan deze systemen en gegevensverzamelingen, die als basis dienen voor de risicoanalyses;

- **Beveiligingsmaatregelen op basis van attack patterns en bekende dreigingen:**
  Beveiligingsadviseurs en Security Architecten verzamelen uit publieke en andere bronnen informatie over attack patterns en dreigingen. Zij stellen een structuur op voor de centrale lijst en vullen die lijst, dusdanig dat dit een goede basis vormt voor de risicoanalyses. Tevens wordt hierbij meer gedetailleerd materiaal, zoals de CAPEC lijst, gereedgezet voor de leveranciers die software moeten gaan ontwikkelen en bouwen.

Het resultaat van deze initiële opbouwactiviteit dient te worden afgestemd met de betrokkenen en de leveranciers, aangezien die er later mee moeten gaan werken. Hierbij dient consensus te worden bereikt over de structuur en diepgang van het materiaal en over de technische en financiële realiseerbaarheid van de eisen.

5.2.2 Het onderhouden van standaard beveiligingseisen

Pas bij het echte gebruik van de standaard beveiligingseisen blijkt of deze daadwerkelijk bijdragen aan de gewenste veiligheid van de software. De betrokkenen bij de ontwerpen, de risicoanalyses, het bouwen en testen etc. doen ervaring op en merken welke eisen zinvol zijn en welke eisen de plank misslaan of als bureaucratisch worden ervaren. Hierover moet worden teruggekoppeld aan de eigenaren van de onderdelen van de standaard beveiligingseisen.

De eigenaren moeten onderhoud uitvoeren aan hun gedeelte. Dit kan op ad hoc basis, indien blijkt dat bepaalde eisen niet effectief zijn, of wanneer nieuwe dreigingen bekend worden. Er is ook periodiek onderhoud nodig, waarbij bijvoorbeeld jaarlijks alle bronnen worden nagelopen om de daarin

opgenomen wijzigingen te verzamelen en te beoordelen of die in de standaard beveiligingseisen moeten worden verwerkt.

Het verdient aanbeveling informatie over de standaard beveiligingseisen uit te wisselen met andere (semi) overheidsinstanties, bijvoorbeeld via CIP. Door gebruik te maken van dit kennisnetwerk bespaart de organisatie op de eigen onderhoudskosten van dit stelsel en verkrijgt men meer effectiviteit doordat meer kennis wordt gebundeld.

5.3 Risicoanalyse

De risicoanalyse heeft tot doel per project zwakheden in de beveiliging of de opzet van de software te vinden en te onderkennen. Zo een risicoanalyse kan daarnaast ook betrekking hebben op delen van het applicatielandschap of delen van de infrastructuur.

De risicoanalyse vindt plaats tijdens of voorafgaand aan de requirement-fase en de architectuurfase. Hierbij worden de bronnen van dreigingen op de specifieke software geïdentificeerd, onder andere met behulp van de resultaten van de BIA en de attack patterns:

- De dreigingen zijn veelal gerelateerd aan de kwetsbaarheden van de gekozen IT-middelen;
- De dreigingen die voortvloeien uit het uitvoeren van activiteiten worden ook meegenomen bij de analyse;
- De risico's zijn gericht op uitbuiting van de afhankelijkheden en kwetsbaarheden van de IT-middelen.

Hierbij is het van belang dat de bij de risicoanalyse betrokken beveiligingsadviseur of security architect kennis heeft van:

- Hoe de software en gegevens worden gebruikt en eventueel hoe die eventueel kunnen worden misbruikt of worden aangevallen. Dit zijn de 'misuse en abuse cases';
- Welke functionaliteit wordt geleverd door de software en welke gegevens daarbij worden gebruikt. De BIV-classificatie voor die functionaliteit en die gegevens wordt gebruikt om de benodigde eisen te selecteren. Dit zijn de eisen die het juiste beschermingsniveau realiseren, rekening houdend met de risico's, het beleid van de organisatie en de vigerende wet- en regelgeving;
- De reeds getroffen maatregelen binnen andere gerelateerde software en binnen de infrastructuur.

Soms wordt deze analyse gecombineerd met een Privacy Impact Analyse (PIA) in het kader van de Wet bescherming persoonsgegevens (Wbp) of de Algemene Verordening Gegevensbescherming (AVG). Bij deze analyse worden de specifieke beveiligingseisen geselecteerd, namelijk toegesneden op de software die moet worden ontwikkeld.

Indien een risico niet kan worden afgedekt door een mitigerende maatregel, dan moet dit risico aan de business worden voorgelegd. De business kan óf het risico accepteren, óf besluiten de gevraagde functionaliteit te laten vervallen.

In Bijlage D: wordt de methodiek voor het uitvoeren van risicoanalyses besproken, waarbij de BIV-classificatie het uitgangspunt is voor het selecteren van de juiste maatregelen.

Indien de impact van aanvullende maatregelen groot is, moeten de demand- en de supply organisatie afspraken maken over hoe met de wijziging wordt omgegaan. Dit kan leiden tot het aanpassen van de contractuele verplichtingen ten aanzien van de te hanteren beveiligingseisen of tot het opnemen van de benodigde maatregelen in een toekomstig release.

5.3.1 Inschatting van dreigingen via STRIDE

De analysemethode STRIDE is ontwikkeld door Microsoft. Dit is een 'threat assessment'. Er wordt een decompositie uitgevoerd, waarna per relevante component de gevoeligheid voor dreigingen wordt geanalyseerd.

De naam STRIDE is een afkorting van de namen van zes categorieën aan dreigingen, namelijk:

- **S**poofing (misbruik van de gebruikersidentiteit, namelijk zich als een ander voordoen);
- **T**ampering (schending van de Integriteit);
- **R**epudiation (weerlegbaarheid);
- **I**nformation disclosure (schending van de privacy of het lekken van data);
- **D**enial of Service (DoS) (onbeschikbaarheid);
- **E**levation of privilege (misbruik van bevoegdheden).

5.3.2 Kwalificering van de risico's

Een risico is de kans dat iets gebeurt wat een bepaalde impact heeft. Om risico's op waarde te schatten en te vergelijken zijn er kwalitatieve en kwantitatieve methoden. Het gebruik van numerieke waarden bij het inschatten van de schade ten gevolge van incidenten en verstoring leidt tot schijnzekerheid. Vandaar dat in dit document is gekozen voor een pragmatische wijze van kwalificering met een driedeling, namelijk 'Hoog', 'Midden' en 'Laag'.

Voor het bepalen van de kans van optreden van een dreiging geldt:

Kans van optreden	Definitie
Hoog	Het voorval is zeer waarschijnlijk. Er zijn geen of onvoldoende mitigerende maatregelen genomen om te voorkomen dat het voorval ook daadwerkelijk ernstige gevolgen heeft. Er is niet veel moeite/expertise nodig om het voorval op te laten treden.
Midden	Het voorval is waarschijnlijk. Er zijn echter voldoende mitigerende maatregelen genomen zodat de schade bij optreden van beperkt blijft. Er is beperkte moeite/expertise nodig om het voorval op te laten treden.
Laag	Het voorval is niet waarschijnlijk of er zijn ruim voldoende mitigerende maatregelen genomen zodat er geen significante schade zal optreden. Er is aanzienlijke moeite/expertise nodig om het voorval op te laten treden.

Voor het bepalen van de omvang van de mogelijke schade door een dreiging geldt:

Omvang van de schade	Definitie
Hoog	De te verwachten schade leidt tot ernstige (politieke) imagoschade of ernstige vertrouwensschade bij de ketenpartners of langdurige interruptie van het primaire proces.
Midden	De te verwachten schade leidt tot beperkte imagoschade of beperkte vertrouwensschade bij een van de ketenpartners of beperkte interruptie van het primaire proces.
Laag	De te verwachten schade leidt nauwelijks tot imagoschade of vertrouwensschade bij ketenpartners of interruptie van het primaire proces.

Voor het inschatten van de omvang van de schade wordt de kans van optreden gecombineerd met de omvang van de mogelijke gevolgen volgens de onderstaande indeling:

Risico (per dreiging)			
	Omvang van de schade door een dreiging		
Kans van optreden	**Laag**	**Midden**	**Hoog**
Laag	Laag	Laag	Midden
Midden	Laag	Midden	Hoog
Hoog	Midden	Hoog	Hoog

Het eindresultaat van deze risicoanalyse is een lijst met dreigingen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht in de ernst van deze dreigingen. Deze lijst is het uitgangspunt voor het bepalen welke standaard beveiligingseisen en beveiligingsmaatregelen toepasselijk zijn en of aanvullende maatregelen nodig zijn en om vast te stellen of er mogelijk nog een restrisico bestaat. Dat is een risico dat niet wordt gemitigeerd door het bestaande en voorziene stelsel van maatregelen voor informatiebeveiliging. Indien er sprake is van een restrisico dient dit te worden gemeld aan de opdrachtgever, die schriftelijk het restrisico moet accepteren namens het betreffende bedrijfsonderdeel.

5.3.3 Eisen aan de methode voor risicoanalyse voor SSD

De risicoanalyse begint op bedrijfsprocesniveau en eindigt op infrastructuurniveau. Het doel van de risicoanalyse is het in een zo vroeg mogelijk stadium identificeren en begrijpen van risico's en het benoemen van mitigerende beveiligingseisen.

De risicoanalyse moet rekening houden met:

- Het toepassingsgebied. Dit betreft de scope, namelijk de processen en diensten die moeten worden geleverd;
- De bekende dreigingen, die volgen uit de centrale lijst met attack patterns en bekende dreigingen, maar ook de (nog) onbekende dreigingen voor:
- Beschikbaarheid;

- Integriteit;
- Vertrouwelijkheid, inclusief privacy;
- Controleerbaarheid.
- Het wel of niet hergebruiken van bestaande reeds genomen maatregelen (hergebruik van bestaande architectuur);
- De technologie die wordt ingezet en de architectuurkeuzen die worden gemaakt;
- De technische implementatie;
- De ontwikkelprocessen, onderhoudsprocessen en werkprocessen.

Het resultaat van de risicoanalyse moet aangeven:

- Welke beveiligingseisen zijn relevant voor de software, uit te splitsen naar het inrichten van preventieve, detectieve, correctieve en repressieve beveiligingsmaatregelen;
- Welke defecten en fouten leiden tot welke beveiligingsrisico's;
- Waar in de levenscyclus moeten beveiligingseisen worden getest en of getoetst op defecten en fouten;
- Welke artefacten moeten worden getest en getoetst;
- Welke testhulpmiddelen en testtechnieken moeten worden gebruikt;
- Welke restrisico's blijven openstaan.

Als kanttekening geldt dat de kwaliteit van de risicoanalyse volledig afhankelijk is van de competenties en ervaring van de hierbij betrokken medewerkers. De opdrachtgever zal aandacht moeten besteden aan het opleiden en trainen van deze medewerkers.

5.4 Risicobeheersing en risicoacceptatie

Tijdens het ontwikkelproces worden de verschillende contactmomenten benut om de beveiligingsrisico's inzichtelijk te maken. Deze risico's worden bij voorkeur zo vroeg mogelijk in het ontwikkelproces door (aanvullende) beveiligingsmaatregelen gemitigeerd of beheerst gemaakt of worden geaccepteerd. In dit proces worden de geaccepteerde risico's per project centraal bijgehouden. Hierbij wordt ook de reden aangegeven per openstaand risico. Veelal zal de openstaande status het gevolg zijn van een welbewuste keuze, op basis van een afweging van de kosten van een vereiste maatregel versus de ernst van de dreiging en de daaruit mogelijk voortvloeiende schade. Hierdoor heeft de opdrachtgever inzicht in welke risico's zijn gemitigeerd en, nog belangrijker, welke risico's nog open staan.

Het is van belang dat deze keuzes voor het wel of niet mitigeren inzichtelijk zijn voor de opdrachtgever danwel diegene die verantwoordelijk is voor het ondersteunde bedrijfsproces. Het mag niet zo zijn dat dergelijke keuzes lager in de lijn worden gemaakt zonder dat de opdrachtgever hiervan op de hoogte is en hierover verantwoording kan worden afgegeven.

5.5 Verantwoording afleggen

Het afleggen van verantwoording kan zowel intern (middels een dashboard) als extern (middels een compliancy statement). Het SSD-dashboard geeft aan hoe de risicoacceptatie van projecten zich verhoudt tot de risicoclassificatie. Een compliancy statement geeft aan hoe de beveiliging van de software zich verhoudt tot een of meerdere gekozen standaarden.

5.5.1 Intern bijhouden en rapporteren met het SSD-dashboard

SSD beschikt over een dashboard, waarmee senior management inzicht heeft in de effectiviteit van de via SSD gerealiseerde risicobeheersing. In het dashboard wordt de risicoclassificatie van de software afgezet tegen de risico's die worden gelopen doordat bepaalde maatregelen niet zijn geïmplementeerd. De risicoclassificatie is gebaseerd op de BIV-classificatie van de informatiesystemen en de gegevensverzamelingen, terwijl de gerapporteerde risico's het gevolg zijn van expliciete en welbewuste risicoacceptaties.

Voor de aanduiding van de ernst van een risico wordt een kwalitatieve risicoschatting gebruikt met een driedeling 'Hoog', 'Midden' en 'Laag'. Deze indeling sluit aan bij hoe de betrokkenen bij SSD omgaan met risico's. Naar het gevoel van de direct betrokkenen leidt een meer gedetailleerde kwantitatieve benadering eerder tot schijnzekerheid dan tot meer nauwkeurigheid. In de praktijk blijkt de kwalitatieve driedeling goed aan te sluiten bij hoe veel organisaties acteren.

Het dashboard maakt inzichtelijk of de overeengekomen beveiligingsmaatregelen daadwerkelijk zijn afgedekt, of dat er sprake is van een gap. Bij iedere niet geïmplementeerde maatregel wordt een toelichting opgenomen, zodat inzichtelijk is wat de afwegingen zijn geweest. Dit kunnen ontbrekende technische middelen zijn, een besluit op basis van kosten versus nut, budgettaire beperkingen, prioriteitsstelling etc. In Bijlage H: staat beschreven hoe het dashboard op een uitbreidbare wijze kan worden gevuld.

5.5.2 Extern bijhouden van en rapporteren over compliancy

Er zijn verschillende industriespecifieke standaarden en raamwerken waaraan organisaties geacht worden compliant te zijn. Voor de overheid kennen we de BIR, voor de bancaire sector SOX en PCI-DSS en wat algemener de ISO 2700x serie. Deze standaarden hebben vaak een breder toepassingsgebied dan software.

Er zijn veel verschillende standaarden, met verschillende indelingen die niet altijd aansluiten bij de bedrijfsvoering. Ook worden de standaarden bij updates soms op een andere manier gestructureerd. Om na invoering het onderhoud van documenten te beperken raden wij aan om bij te houden op welke manier het eigen informatiebeveiligingsbeleid en gedetailleerde documenten zoals codeerstandaarden samenhangen met die standaarden. Dat kan met een compliancy statement waarin beschreven staat op welke manier compliancy bewerkstelligd wordt en waar specifieke informatie te auditen is.

5.5.3 Gap analyse

Door de gap af te zetten tegen de risicoclassificatie van de systemen, kan inzichtelijk worden gemaakt welke applicatie voor de bedrijfsvoering de hoogste risico's impliceren. Deze informatie kan worden gebruikt bij het stellen van prioriteiten voor verbeterprojecten en nieuwe releases.

Door de onderliggende afwegingen van de niet geïmplementeerde maatregelen te analyseren, kunnen de oorzaken van de gap worden geanalyseerd. Hiermee kan men zien welke opdrachtgevers mogelijk lichtvaardig maatregelen achterwege laten, of dat er te weinig budgettaire ruimte is voor het werkelijk veilig maken van de software. Op basis van de analyse van de onderliggende afwegingen kan senior management acties initiëren, waarmee de effectiviteit van SSD wordt verbeterd.

Het via het dashboard geconstateerde verschil in vereiste en geïmplementeerde maatregelen kan worden gebruikt om te bepalen hoe groot het overblijvend risico is, namelijk het restrisico. Senior management moet bepalen of dit restrisico acceptabel is voor de organisatie. De risicoattitude van senior management speelt hierbij een beslissende rol welke restrisico's men wil mitigeren door het treffen van aanvullende beveiligingsmaatregelen.

Het herhaaldelijk uitvoeren van de gap analyses maakt het mogelijk om de voortgang of achteruitgang vast te stellen met betrekking tot het informatiebeveiligingsbeleid. Ook kan worden vastgesteld of de standaard beveiligingseisen op een te hoge of een te lage perceptie van de risicoacceptatie door de organisatie zijn gebaseerd.

6 De organisatorische inrichting van SSD

Voor de invoering van SSD is vereist dat de organisatie over een duidelijke structuur beschikt voor het aansturen van de informatiebeveiliging en het controleren op handhaving en naleving. SSD heeft onder andere invloed op:

- De beveiligingsprocessen;
- De Security Architectuur;
- De Baseline Security;
- Het risicobeheersingsproces met de BIA, risicoanalyses en PIA's;
- De inkoopprocedures en contracten;
- De interactie tussen enerzijds de ontwerpers en ontwikkelaars en anderzijds de beveiligingsadviseurs en de pentesters.

Daarom moeten een aantal functies of rollen zijn belegd, zoals die van de beveiligingsadviseurs, de Security Architecten en de Security Officers. Binnen verschillende doelorganisaties kunnen hiervoor verschillende namen in gebruik zijn, maar er moeten medewerkers zijn die de taken behorende bij deze functies of rollen uitvoeren.

6.1 De opdrachtgever

De ultieme opdrachtgever is altijd de Directie of de Raad van Bestuur van de organisatie. Deze zullen de rol van opdrachtgever delegeren aan de actuele opdrachtgever, zoals bijvoorbeeld verantwoordelijken voor bedrijfsprocessen, applicatie-eigenaren, projectleiders etc.

De actuele opdrachtgever is de verantwoordelijke voor een bedrijfsproces of een eigenaar van een applicatie, die de opdracht verstrekt voor nieuwbouw of modificatie van software. De opdrachtgever is degene die is gemandateerd om besluiten te nemen over beveiligingseisen en het accepteren van afwijkingen. Hij of zij vertegenwoordigt hierbij de gebruikersorganisatie of de stakeholders.

Voor iedere opdracht voor het ontwikkelen van software moet duidelijk zijn wie de actuele opdrachtgever is, aangezien die bij de SSD-methode verantwoordelijk is voor de aansturing, besluitvorming en risicoacceptatie. Vanuit de ultieme opdrachtgever moet er een heldere mandatering zijn naar de actuele opdrachtgever, omdat SSD met gezag moet worden aangestuurd.

6.2 Beveiligingsadviseurs

Een beveiligingsadviseur participeert in de ontwikkeling van strategie en beleid gericht op informatiebeveiliging, bevordert en coördineert de ontwikkeling van processen en procedures in dit kader en ziet toe op de realisatie van het beleid. De beveiligingsadviseur ondersteunt het lijnmanagement in alle fasen van de PDCA-cyclus op het gebied van informatiebeveiliging.

Beveiligingsadviseurs zijn de experts op het gebied van standaarden voor informatiebeveiliging en geven daarover gevraagd en ongevraagd advies aan de opdrachtgever en aan andere betrokkenen.

Een beveiligingsadviseur is degene die de opdrachtgever adviseert over de beveiligingseisen, de te nemen maatregelen, de inschatting van de ernst van afwijkingen en het wel of niet accepteren van afwijkingen. Dit kan ook een Security Officer zijn, een Security Architect of een andere expert op het gebied van informatiebeveiliging.

Binnen de SSD-methode zijn de beveiligingsadviseurs betrokken bij het opstellen van de standaard beveiligingseisen, het adviseren van de opdrachtgevers, het uitvoeren van de risicoanalyses, het opstellen van 'misuse and abuse cases', het invullen van de contactmomenten en het interpreteren van rapportages over testactiviteiten, incidenten en verstoringen.

6.3 (Enterprise) Security Architecten

De enterprise security architectuur is het middel om de samenhang te bewaken tussen de enterprise architectuur, de ontwikkelingen binnen en buiten de eigen organisatie en de te nemen en reeds genomen beveiligingsmaatregelen. Om deze reden dienen de Enterprise Security Architecten op een centrale plaats te worden gepositioneerd binnen de organisatie, bijvoorbeeld bij de Chief Information Officer (CIO).

De rol van een Enterprise Security Architect is meer dan alleen het leveren van een enterprise security architectuur. Die architectuur is slechts een middel om het echte doel te bereiken, namelijk veilige software in een veilige omgeving. De echte rol bestaat daarom tevens uit het inhoudelijk aansturen van de Security Architecten en de Security Officers.

De Enterprise Security Architecten kunnen daarnaast adviseren om onderzoeken te laten uitvoeren, ontwerpen te laten reviewen en daarbij ondersteunend zijn. De keuze om een onderzoek te laten uitvoeren of een ontwerp te laten reviewen is overigens aan de opdrachtgever. Zo kan meer zekerheid worden verkregen dat de software voldoet aan de specifieke beveiligingseisen en wordt geëxecuteerd in een veilige omgeving.

De Security Architecten binnen de bedrijfsonderdelen geven ondersteuning aan de lijnverantwoordelijken, de IT-architecten, de projectleiders en de ontwerpers, onder andere bij nieuwe projecten. Zij zorgen dat op de juiste wijze gebruik wordt gemaakt van de voorgeschreven mechanismen voor identificatie, authenticatie, autorisatie, versleuteling, logging, monitoring, rapportage etc. en bewaken het voldoen aan de specifieke beveiligingseisen.

6.4 Security Officers

De Security Officers zijn de contactpersonen voor de eigenaren van de bedrijfsprocessen, de informatiesystemen en de gegevensverzamelingen. Zij weten wat er op de werkvloer gebeurt, welke veranderingen daar plaatsvinden en wie de echte stakeholders zijn. Veelal zijn zij gepositioneerd bij een afdeling voor Informatie Management (IM), die rapporteert aan de Directie van een bedrijfsonderdeel. De Security Officers hebben twee hoofdtaken:

- **Het stellen van beveiligingseisen:**
  De Security Officers bepalen samen met de betrokkenen binnen de bedrijfsprocessen de risico's, de specifieke beveiligingseisen vanuit het oogpunt van de bedrijfsprocessen op de werkvloer en de te nemen beveiligingsmaatregelen. Een instrument hiervoor is de risicoanalyse;

- **Het adviseren over het accepteren van risico's:**
  De Security Officers stemmen afwijkingen op de beveiligingseisen af met de applicatie-eigenaren. Hierbij hebben zij een adviserende rol, dankzij het feit dat zij zowel de afwijkingen begrijpen als de werkprocessen binnen het bedrijfsproces door en door kennen.

Grotere organisaties hebben vaak meerdere Security Officers, één voor elk bedrijfsonderdeel en een coördinerende Chief Security Officer (CSO) of Chief Information Security Officer (CISO).
De Enterprise Security Architect ondersteunt de Security Officers door het inbrengen van kennis en ervaring over de enterprise security architectuur en de risicoanalyses, inclusief de 'misuse and abuse cases'. Doordat informatie en ervaring in twee richtingen worden uitgewisseld, draagt deze interactie bij aan hergebruik van kennis en ervaring organisatiebreed.

6.5 Technische Security Officers

De Technische Security Officers zijn binnen de eigen IT-organisatie gepositioneerd of zijn de contactpersonen voor informatiebeveiliging in de richting van de externe leveranciers en hostingpartij. Zij hebben kennis van de specifieke aspecten van de techniek en de beheerprocessen binnen de IT-organisatie en van die bij de leveranciers en hostingpartij.

De Technische Security Officers hebben twee hoofdtaken:

- **Het borgen van beveiligingseisen:**
  De Technische Security Officers zijn samen met de Inkoopafdeling verantwoordelijk voor de contractuele borging van de beveiligingseisen. De borging betreft niet alleen de beveiligingseisen per applicatie, maar ook de beveiligingseisen die gesteld worden vanuit de enterprise security architectuur en die gelden voor de IT-organisatie, de leveranciers en de hostingpartij;

- **Het inventariseren van risico's in de productieomgeving:**
  Dagelijks doen zich incidenten en verstoringen voor die de werking van de informatievoorziening nadelig beïnvloeden. Als een incident of verstoring is gerelateerd aan informatiebeveiliging, wordt er een Technische Security Officer bij betrokken. Afhankelijk van de ernst volgt een 'root cause analysis', waarbij naast de analyse van de oorzaak de 'lessons learned' worden vastgelegd. Soms leidt dit tot een verandering in de standaard beveiligingseisen.

Enerzijds levert de Enterprise Security Architect ondersteuning en coaching aan de Technische Security Officers en anderzijds ontvangt hij of zij waardevolle informatie over wat werkelijk gebeurt op de IT-werkvloer. Doordat informatie en ervaring in twee richtingen worden uitgewisseld, draagt deze interactie bij aan hergebruik van kennis en ervaring organisatie breed en wordt de centrale verzameling aan standaard beveiligingseisen doorlopend verrijkt.

6.6 De leverancier (opdrachtnemer)

Een aantal afdelingen of functies van de leveranciers voor software zijn betrokken bij SSD. Dit zijn onder andere:

- Contractmanagement;
- Ontwerpers en ontwikkelaars;
- Testteams.

De leveranciers moeten in een vroeg stadium worden betrokken bij de uitrol van SSD. Daarbij is het van belang contractuele afspraken te maken. Zo moet het hanteren van een minimum lijst van beveiligingseisen in het contract worden vastgelegd, evenals de contactmomenten, het testplan voor informatiebeveiliging, de code review, testen en toetsen en wie pentesten doet. Alle zaken met betrekking tot SSD moeten door de leverancier transparant worden vastgelegd voor de opdrachtgever. De opdrachtgever hoeft dan niet alle testen opnieuw te doen, maar kan de resultaten toetsen en steekproeven laten uitvoeren.

Voor de leveranciers is tevens inzicht nodig in de tijdslijn voor de uitrol van SSD. Zij moeten weten wanneer de processen aan hun kant moeten zijn ingericht.

Het valt aan te bevelen de leveranciers te betrekken bij het opstellen van de baseline security met de eisen die vanuit de standaarden zijn geselecteerd als zijnde relevant voor de organisatie. Vanuit hun eigen ervaring kunnen de leveranciers de baseline reviewen, evenals de overige onderdelen van de standaard beveiligingseisen. De leveranciers hebben er zelf belang bij dat dit een dekkend stelsel wordt, dat op een pragmatische en kosteneffectieve wijze kan worden gerealiseerd. Uiteindelijk worden zij aangesproken op het resultaat, namelijk het opleveren van veilige systemen.

Voor de leveranciers heeft het werken volgens SSD ook voordelen. Zodra de specifieke beveiligingseisen zijn vastgelegd kan de leverancier dit verwerken in zijn prijsstelling en heeft de zekerheid dat er geen nieuwe eisen meer bij komen. Indien dit wel nodig is, treedt het proces voor ‘change management’ in werking.

7 Groeien via en sturen op maturity van SSD

SSD is niet bedoeld voor een aanpak via een 'big bang'. De groei van de organisatie kan stapsgewijs en door middel van geleidelijke verbeterprogramma's worden gerealiseerd. De voor SSD opgestelde volwassenheidsniveaus vormen een leidraad bij het definiëren van de programma's. Tevens fungeren de volwassenheidsniveaus als meetpunten om te bepalen in hoeverre de organisatie grip heeft op het verkrijgen en inzetten van veilige software. De volwassenheidsniveaus zijn beschreven in Bijlage F: en zijn een variant op die voor het Capability Maturity Model (CMM).

Een pragmatische dakpansgewijze aanpak om door middel van fasen en verbeterprogramma's te groeien is hieronder opgenomen.

7.1 Nulmeting

De doelorganisatie moet eerst de eigen status weten van de aan SSD ten grondslag liggende processen. In hoeverre worden zaken nu al effectief aangestuurd en waar zitten de manco's?

Bij voorkeur moeten onderzoekers worden ingezet die ervaring hebben met SSD bij andere organisaties. Deze onderzoekers voeren de nulmeting uit, namelijk een onderzoek naar de IST, de SOLL en de GAP. De IST is de actuele situatie van de relevante processen en de SOLL is de in dit document opgenomen beschrijving van SSD. Hieruit volgt de GAP, namelijk de lijst van manco's.

Voor het invullen van ieder manco moet een plan worden opgesteld. Dit leidt tot een overkoepelend actieplan en een tijdschema voor een geleidelijke invoer. Bij het opstellen van het tijdschema is voorzichtigheid geboden, aangezien SSD deels is gebaseerd op een cultuuromslag. Die kan men alleen geleidelijk realiseren.

7.2 Definieer het minimum startpunt

De kern van SSD is de kennisbron, namelijk de verzameling van standaard beveiligingseisen. Bij het opbouwen van deze kennisbron moeten prioriteiten worden gezet. Er kan worden gestart met de relatief eenvoudig te realiseren onderdelen, zoals:

- **Taken voor SSD:**
  De actoren voor SSD zijn beschreven in dit document, inclusief de door hen uit te voeren taken. Binnen de doelorganisatie moeten de juiste personen worden gekoppeld aan de taken voor SSD en zij moeten worden gemandateerd. Allereerst gaat het hierbij om de eigenaren van de standaard beveiligingseisen, de beveiligingsadviseurs, de Enterprise Security Architecten en de (Technische) Security Officers;

- **Classificaties:**
  Het classificatieschema moet worden opgesteld voor de informatiesystemen en gegevensverzamelingen. Voor veel doelorganisaties is hiervoor reeds veel materiaal aanwezig en kan men het opstellen van het classificatieschema als een 'quick win' oppakken. De echte

uitdaging ligt echter bij de uitrol. Niettemin is classificatie een absolute vereiste om met SSD te kunnen aanvangen;

- **De baseline security:**
  De meeste doelorganisaties hebben al een informele baseline voor security. Deze moet worden geformaliseerd, dat wil zeggen worden gedocumenteerd als een verzameling aan beveiligingseisen voor de infrastructuur. Een alternatief is gebruik te maken van een baseline van een andere (semi) overheidsinstantie, die een vergelijkbare infrastructuur heeft en die baseline aan te passen aan de eigen specifieke situatie;

- **Het SSD-dashboard:**
  Vanaf het begin van de uitrol van SSD speelt het dashboard een belangrijke rol om een overzicht te hebben over de voortgang van de diverse acties en de processen te kunnen bewaken. Dit dashboard wordt geleidelijk gevuld naarmate meer informatiesystemen en gegevensverzamelingen onder SSD gaan vallen.

Parallel aan deze initiële acties moet overleg plaatsvinden met de leveranciers, om hen voor te bereiden op de wijziging in de interactie met hen. Zij moeten worden overtuigd dat van hen actieve participatie wordt verwacht, plus meedenken over het inrichten van de contactmomenten.

7.3 Definieer de enterprise security architectuur blokken

De Enterprise Security Architecten en de Technische Security Officers moeten vervolgens de enterprise security architectuur blokken gaan documenteren en de synergie borgen tussen deze blokken. Tevens moet worden getoetst of de architectuur marktconform is, namelijk of deze architectuur past bij die van andere (semi) overheidsinstanties, met name de ketenpartners.
Binnen de overheid wordt gestreefd naar schaalvergroting, namelijk naar kostenverlaging door IT-infrastructuren samen te nemen en het aantal rekencentra en technische beheerorganisaties te verminderen. Bij het opstellen van de architectuur dient men hier rekening mee te houden.
Vervolgens komt de uitrol van de enterprise security architectuur. Dit impliceert het voorlichten en begeleiden van de Security Architecten, de IT Architecten en de projectleiders, zodat zij weten op welke wijze zij gebruik kunnen maken van deze architectuur.

7.4 Stel het gebruik van de BIA en risicoanalyse verplicht

Voor het uitrollen van de Business Impact Analyses (BIA's) is besluitvorming nodig van het hoogste gezag binnen de organisatie, namelijk de Raad van Bestuur of de Directie. Zonder een instructie van bovenaf is een BIA gedoemd te mislukken. Dit is namelijk een majeure operatie, die veel aspecten van een bedrijfsonderdeel raakt. De BIA slaagt alleen als deze een draagvlak heeft binnen de gebruikersorganisatie, namelijk als men het nut ervan inziet, of als het van bovenaf wordt opgelegd. Het resultaat van de BIA zijn de BIV-classificaties van de informatiesystemen en gegevensverzamelingen. Deze zijn randvoorwaardelijk voor de uitrol van de risicoanalyses.

Een hulpmiddel om de risicoanalyses uit te rollen is het SSD-dashboard. Hierin moeten alle projecten worden opgenomen, met een indicatie of wel of niet een risicoanalyse wordt uitgevoerd. Als dit wordt gekoppeld aan bedrijfsonderdelen, kan worden gerapporteerd bij welke onderdelen voldoende en bij

welke nog onvoldoende aandacht wordt gegeven aan dit essentiële onderdeel van SSD. Via dergelijke rapportage kan het management worden overtuigd zich aan SSD te conformeren.

Een aandachtspunt bij risicoanalyses betreft de competenties en ervaring van de betrokkenen. Zeker in het begin is training en coaching nodig om tot zinvolle resultaten te komen die een toegevoegde waarde hebben voor de uitrol van SSD. In de planning moet voldoende ruimte worden ingebouwd voor de opbouw van deze competenties en ervaring.

7.5 Vergroot de voorspelbaarheid en optimaliseer

Een zorgvuldig tijdschema en een pragmatische insteek zijn van belang voor de uitrol en het vervolgens groeien van SSD. Bij het opzetten van de planning moet men realistisch zijn en niet te snel resultaten verwachten. Een beheerst groeipad is van belang, met kleine stappen die ieder op zich kortcyclisch worden ingericht, zodat ook bij belemmeringen of vertragingen snel kan worden bijgestuurd of kan worden geëscaleerd.

Zowel de volwassenheidniveaus als het SSD-dashboard zijn hulpmiddelen om de uitrol in goede banen te leiden. Deze passen bij een dakpansgewijze aanpak met fasen en verbeterprogramma's, waarbij stap voor stap SSD wordt geoptimaliseerd. Zo groeit men naar het gewenste doel, namelijk veilige IT-systemen binnen een veilige infrastructuur, die door de gebruikers op een veilige wijze kunnen worden benut, conform de eisen vanuit de te ondersteunen bedrijfsprocessen.

Bijlage A: Classificatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid

De opdrachtgever stelt het belang van de bedrijfsprocessen en de software vast door de software en gegevens in te delen naar beveiligingsklassen. De klassen zijn ingedeeld conform de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Voor iedere klasse geldt een minimale basis van de te stellen beveiligingseisen en de te nemen beveiligingsmaatregelen.

1. Definities: Beschikbaarheid, Integriteit en Vertrouwelijkheid

De definities van de drie voor de bedrijfsprocessen gangbare kwaliteitsaspecten zijn:

Beschikbaarheid:
Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot gegevens en aanverwante bedrijfsmiddelen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening;

- **Integriteit:**
  Integriteit betreft het waarborgen van de juistheid, tijdigheid, actualiteit en volledigheid van informatie en de verwerking daarvan.
  Een onderdeel van Integriteit betreft de onweerlegbaarheid (non-repudiation). Dit is de mate waarin kan worden aangetoond dat acties of gebeurtenissen hebben plaatsgevonden, zodat deze acties of gebeurtenissen later niet kunnen worden ontkend;

- **Vertrouwelijkheid:**
  Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd en dat ongeautoriseerde onthulling wordt voorkomen.

Specifiek voor de ontwikkeling van software geldt een vierde kwaliteitsaspect, namelijk:

- **Controleerbaarheid:**
  Controleerbaarheid betreft de mogelijkheid om met een voldoende mate van zekerheid te kunnen vaststellen of wordt voldaan aan de eisen ten aanzien van Beschikbaarheid, Integriteit en Vertrouwelijkheid. Niet alleen accountants, maar ook het management en bijvoorbeeld systeembouwers dienen erop toe te zien dat voldoende en toereikende signaleringen en vastleggingen worden ingebouwd in systemen om deze controleerbaar te maken. Hierbij gaat het zowel om de presentatie van de beoogde goede werking als om de weergave van fouten en of gebreken.

Deze definities zijn conform de gangbare internationale standaarden voor informatiebeveiliging en privacybescherming.

2. BIR als baseline voor classificatie

De basis voor de inrichting van de informatiebeveiliging is ISO27001 en ISO27002, die integraal zijn opgenomen in de 'Baseline Informatiebeveiliging Rijksdienst (BIR)'.

De onderstaande tabel is een overzicht van de classificatieniveaus, waarin het BIR als baseline met arcering is gemarkeerd.

Kwaliteitsaspect	**Het belang**			
Beschikbaarheid	Hoog	Midden	Laag	
Integriteit	Hoog	Midden	Laag	
Vertrouwelijkheid	Strikt Vertrouwelijk, Risicoklasse 3	Vertrouwelijk, Risicoklasse 2	Intern, Risicoklasse 1	Openbaar, Risicoklasse 0

De baseline voor informatiebeveiliging is gericht op:

- Het standaardniveau voor Beschikbaarheid is Midden;
- Het standaardniveau voor Integriteit is Midden;
- Het standaardniveau voor Vertrouwelijkheid is gebaseerd op de vereisten voor Vertrouwelijk of Risicoklasse 2.

Alleen door middel van een risicoanalyse kunnen de niveaus naar boven of naar beneden worden bijgesteld.

Voorbeelden:

- Voor een informatiesysteem dat een wettelijke taak of financiële transacties ondersteunt waarvoor onweerlegbaarheid nodig is, geldt een hoge eis voor Integriteit;
- Voor netwerkvoorzieningen en informatiesystemen die een proces ondersteunen dat maar zeer beperkt mag worden onderbroken geldt een hoge eis voor Beschikbaarheid;
- De Vertrouwelijkheid van een informatiesysteem is afhankelijk van de classificatie van de gegevens die worden opgeslagen, verwerkt of getransporteerd. Het niveau van Vertrouwelijkheid van bijvoorbeeld medische of strafrechtelijke gegevens is Risicoklasse 3, of Strikt Vertrouwelijk.

3. Beschikbaarheid: 3 niveaus

De beschikbaarheid heeft betrekking op de vraag of de software beschikbaar is op het moment en in de toestand waarin dat gewenst en bedoeld is. De beschikbaarheidseisen zijn afhankelijk van de consequenties voor de organisatie bij een eventuele afwezigheid van de software, de invloed op andere processen en bedrijfsmiddelen en de tijdsperiode waarbinnen de software moet worden hersteld.
Het classificatiemodel voor beschikbaarheid kent drie niveaus, namelijk 'hoog', 'midden' en 'laag'. Het classificatiemodel is gericht op het risico dat de software en daarmee het ondersteunde bedrijfsproces niet beschikbaar is.

Niveau van Beschikbaarheid	Beschrijving
Hoog	Het optreden van een verstoring zal voor de organisatie belangrijke nadelige consequenties hebben. • Indien de software of onderdelen daarvan niet beschikbaar zijn, loopt de organisatie zeer grote schade op; • Aangrenzende processen vinden geen doorgang; • De eis voor het herstel is < 1 dag.
Midden	Het optreden van een verstoring kan voor de organisatie nadelige consequenties hebben, maar middels compensatie en herstel zijn de gevolgen van een optredend risico beheersbaar. • Indien de software of onderdelen daarvan niet beschikbaar zijn, loopt de organisatie grote schade op; • Aangrenzende processen raken verstoord, maar vinden (deels) doorgang; • De eis voor het herstel is < 3 dagen.
Laag	Het optreden van een verstoring heeft voor de organisatie (vrijwel) geen consequenties. • Indien de software of onderdelen daarvan niet beschikbaar zijn, wordt slechts geringe schade gelopen; • Aangrenzende processen worden niet verstoord; • De eis voor het herstel is < 2 weken.

4. **Integriteit: 3 niveaus**

Het classificatiemodel voor Integriteit is gericht op het risico dat de gegevens vanuit de software niet juist, niet tijdig, niet actueel of onvolledig worden opgeslagen, verwerkt, of getransporteerd. De integriteitniveaus zijn met name relevant voor de geautomatiseerde gegevensverwerking zonder menselijke interventie.

Niveau van Integriteit	**Beschrijving**
Hoog	Bij manipulatie van het bedrijfsproces, het informatiesysteem of de gegevens loopt de organisatie grote schade op, zoals: • Door onjuiste financiële transacties kan het vertrouwen in de organisatie worden aangetast. De Integriteit van de gegevens wordt onder andere geborgd door het: • Vereisen van onweerlegbaarheid voor financiële transacties; • Stelsel van maatregelen voor interne beheersing en functiescheiding.
Midden	Bij manipulatie van het bedrijfsproces, het informatiesysteem of de gegevens loopt de organisatie beperkte schade op, zoals: • Door onvolledige of te laat opgeleverde gegevens, bijvoorbeeld voor financiële transacties, kan het vertrouwen in de organisatie worden aangetast; • (Complexe) wetgeving kan niet goed worden uitgevoerd doordat de gegevensverwerking niet juist, tijdig, actueel en volledig is. De Integriteit van de gegevens wordt onder andere geborgd door het: • Beschermen tegen ongeautoriseerde mutaties; • Handhaven van de interne en externe consistentie; • Vaststellen van de Integriteit van data van input tot output.
Laag	Bij manipulatie van het bedrijfsproces, het informatiesysteem of de gegevens loopt de organisatie geringe schade op, zoals bij: • Onjuiste, onvolledige of te laat opgeleverde gegevens, zoals in interne verslagen, hebben in de regel weinig tot geen negatieve effecten; • Onjuiste, onvolledige of te laat opgeleverde gegevens hebben weinig tot geen invloed op het vertrouwen in de organisatie; • De Integriteit van data kan niet met zekerheid worden vastgesteld.

De Integriteit van gegevens berust op drie doelen. Dat zijn:

- Tegengaan van ongeautoriseerde datamutaties door ongeautoriseerde gebruikers:
  Gebruikers zijn alleen toegestaan om objecten aan te passen binnen hun functie.
- Tegengaan van vervuiling van integere gegevens met gegevens waarvan de Integriteit nog niet of niet kan worden vastgesteld:
  - Tijdens de verwerking wordt alleen gebruik gemaakt van gegevens waarvan de juistheid, tijdigheid en volledigheid is geborgd;

- Tijdens de verwerking wordt alleen gebruik te maken van gegevens die alleen door daartoe geautoriseerden, zijn gemuteerd.
- Handhaven van interne consistentie: Gedurende het proces van verwerking wordt de Integriteit van de data bewaakt van en zijn geprogrammeerde controles gedefinieerd voor vaststelling van de Integriteit van de gegevens tijdens de verschillende processtappen.

Als vuistregel geldt: wanneer niet kan worden voldaan aan de borging van de Integriteit van de gegevens, dan zijn deze gegevens (mogelijk) niet integer.

5. Vertrouwelijkheid: 4 niveaus

Het classificatiemodel voor vertrouwelijkheid is gericht op het risico van ongeautoriseerde onthulling van gevoelige gegevens. De classificatie van gegevens wordt ook wel rubricering genoemd. Binnen dit document wordt het begrip classificering gehanteerd, waarbij geen onderscheid wordt gemaakt tussen classificering en rubricering.

Classificatie Vertrouwelijkheid	Voorbeelden
Openbaar (Risicoklasse 0) • Niet vertrouwelijke publiekelijk beschikbare bedrijfsgegevens.	• Brochures, webpagina's op internet, jaarverslag.
Interne informatie (Risicoklasse 1) • Niet privacygevoelige, niet-publieke persoonsgegevens. Ongeautoriseerde onthulling leidt tot geringe schade.	• E-mailverkeer, interne procedures en werkinstructies.
Vertrouwelijk (Risicoklasse 2) • Privacygevoelige persoonsgegevens, vertrouwelijke gegevens. Ongeautoriseerde onthulling leidt tot materiële of immateriële schade. De schade kan direct of indirect zijn.	• Persoonsgegevens van klanten (voor zover deze niet in een andere klasse vallen), BSN, financiële of economische situatie van de betrokkene (schulden van individuen); • Personeelsdossiers, salarisstroken, personeelsbeoordelingen; • IP-adressen; • Aanbestedingsdocumentatie; • Strategische beleidsdocumenten.
Strikt vertrouwelijk, Geheim (Risicoklasse 3) • Privacy bijzondere persoonsgegevens. Informatie die, indien dit openbaar wordt, de organisatie direct of indirect ernstige (politieke) schade kan berokkenen. Ongeautoriseerde onthulling leidt tot grote	• Persoonsgegevens over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijk gedrag; • Gegevens die misbruikbaar zijn voor identiteitsfraude, zoals biometrie,

materiële of immateriële schade.	inloggegevens (wachtwoorden), encryptiesleutels; • Strategische plannen en plannen die politiek zeer gevoelig liggen binnen de organisatie of de keten.

Bijlage B: Het vaststellen van Vertrouwelijkheid

Het proces van toekennen van een niveau betreffende de Vertrouwelijkheid van gegevens kent de volgende stappen:

- Voorzet: De opsteller van de informatie doet een voorstel tot classificatie van de Vertrouwelijkheid en 'brengt deze aan' op de informatie;
- Vaststelling: De vertrouwelijkheidclassificatie wordt vastgesteld door degene die verantwoordelijk is voor de inhoud;
- Handhaving: De verantwoordelijke ziet toe op de juiste vertrouwelijkheidclassificatie van de gegevens.

Voor classificatie van gegevens is het relevant onderscheid te maken tussen bedrijfsgegevens en persoonsgegevens. Als voorbeeld:

- Persoonsgegevens zijn gegevens die gerelateerd kunnen worden aan natuurlijke personen. Een polis (ofwel een klantdossier) wordt in deze context beschouwd als een verzameling van persoonsgegevens;
- Bedrijfsgegevens zijn gegevens omtrent het (verloop) van het bedrijfsproces. Informatie over de voortgang binnen het proces van polisadministratie wordt beschouwd als een verzameling van bedrijfsgegevens.

Bedrijfsgegevens en persoonsgegevens worden tijdens de uitvoering van de bedrijfsprocessen vaak met elkaar vermengt. Voor de classificering van een gegevensverzameling vormt dit geen probleem. De hoogste vertrouwelijkheidclassificatie van gegevens in een gegevensverzameling is bepalend voor de beveiliging van de gehele verzameling.

1. Risicoklasse 0, Openbare informatie

Gegevens in Risicoklasse 0 zijn openbare persoonsgegevens. Deze omvatten persoonsgegevens waarvan algemeen is aanvaard dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene, zoals publiekelijk beschikbare telefoonboeken, brochures, (openbare) internetsites etc.

2. Risicoklasse 1, Interne informatie

Gegevens in Risicoklasse 1 zijn alleen toegankelijk voor medewerkers van de organisatie en voor derde partijen (gegevens ontvangers, bewerkers en cliënten) waar zij voor bedoeld zijn. Hierbij geldt doelbinding.
De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn beperkt, waardoor de standaard beveiligingsmaatregelen veelal toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens. Tevens vallen hieronder de gegevens gericht op interne werkprocedures.

3. **Risicoklasse 2, Basis vertrouwelijkheidniveau**

Gegevens in Risicoklasse 2 mogen uitsluitend worden gebruikt en geraadpleegd door medewerkers die er uit hoofde van hun functie of taak gebruik van moeten kunnen maken en derde partijen (gegevensontvangers, bewerkers en cliënten) waar zij voor bedoeld zijn.
Artikel 13 Wbp vereist bij de beveiliging van persoonsgegevens een risicogerichte benadering. Het artikel vraagt om 'passende technische en organisatorische maatregelen' die 'rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen'.
De baseline gaat uit van een basis vertrouwelijkheidniveau. Dit omvat het borgen van de Vertrouwelijkheid van:
Gegevens die ten hoogste 'Departementaal Vertrouwelijk (DepV)' zijn gerubriceerd. Zie hiervoor het Besluit Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI);
Privacygevoelige gegevens die ten hoogste als Risicoklasse 2 zij geclassificeerd;
Gegevens over de financiële of economische situatie van de betrokkene. Dit zijn bijvoorbeeld gegevens over schulden van individuen;
Gegevensverzamelingen die worden verwerkt die betrekking hebben op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkenen).
Gegevens in Risicoklasse 2 komen veelvuldig voor bij (semi) overheidsinstanties. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie zoals het Burger Service Nummer BSN, personeelsdossiers, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van strategische beleidsvorming ('beleidsintimiteit') of gestructureerde gegevensverzamelingen over grote delen van de bevolking.

4. **Risicoklasse 3, Geheim of strikt vertrouwelijk**

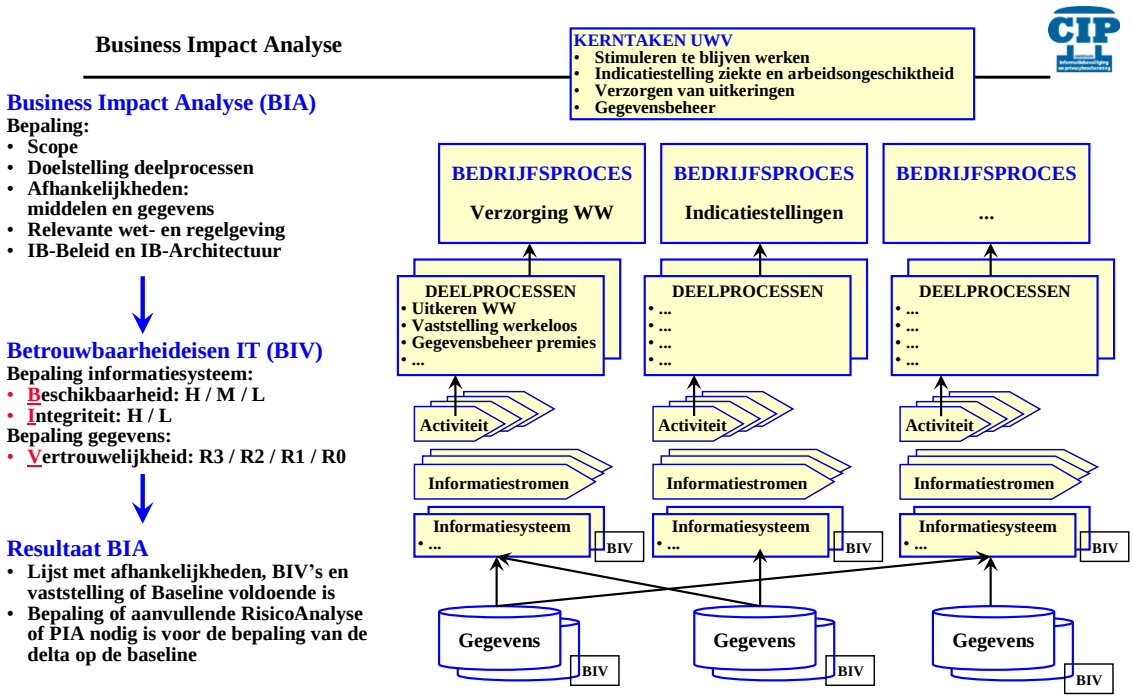
Gegevens in Risicoklasse 3 mogen alleen toegankelijk zijn voor een limitatief omschreven groep medewerkers van de organisatie. Risicoklasse 3 omvat:
Persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gedrag en onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
Gegevens die kunnen worden misbruikt voor identiteitsfraude, zoals biometrische gegevens, inloggegevens als gebruikersnamen en wachtwoorden.

Bijlage C: Business Impact Analyse (BIA) methodiek

De opdrachtgever van een project of de eindverantwoordelijke voor een bedrijfsproces is verantwoordelijk voor het maken van een afweging tussen de zakelijke waarden binnen het bedrijfsproces versus de mogelijke schade als gevolg van een inbreuk op een van de kwaliteitsaspecten. Via een Business Impact Analyse (BIA) wordt de BIV-classificatie opgesteld voor de betreffende software:

- **Beschikbaarheid en Integriteit**: De classificatie voor Beschikbaarheid en Integriteit van een IT-middel is afhankelijk van het bedrijfsproces waarbinnen de software wordt gebruikt;
- **Vertrouwelijkheid**: De classificatie voor Vertrouwelijkheid van de gegevens is met name afhankelijk van de mate van privacygevoeligheid van de gegevens. Deze is onafhankelijk van het proces waarvoor die worden gebruikt.

Het BIA-proces verloopt schematisch weergegeven als volgt:



Figuur 9: het BIA-proces

De stappen en verantwoordelijkheden voor de BIA zijn:

Stappen BIA	Verantwoordelijke
1. Doelstelling van het bedrijfsproces: ○ **Het vaststellen van de doelstellingen van het bedrijfsproces in het kader van het uitvoeren van de kerntaken van de organisatie.**	**Opdrachtgever**
2. Bepalen van de scope: ○ **Het identificeren van de primaire en ondersteunende deelprocessen;** ○ **Het identificeren van de informatiestromen.**	**Opdrachtgever**
3. Selectie van kaderstellende documenten: ○ **Het inventariseren van de relevante beleidsdocumenten en architectuurdocumenten binnen de scope;** ○ **Het selecteren van de relevante wet- en regelgeving;** ○ **Het samenvatten van de eisen die volgen uit het beleid, de architectuur en de wet- en regelgeving.**	**Beveiligingsadviseur**
4. Vaststellen van de dreigingen: ○ **Het identificeren van de mogelijke dreigingen voor de IT-middelen binnen de deelprocessen en informatiestromen.**	**Beveiligingsadviseur, Security Architect**
5. Afhankelijkheden van IT-middelen: ○ **Het inventariseren van de activiteiten die nodig zijn voor de uitvoering van de deelprocessen;** ○ **Het identificeren van de afhankelijkheid van de IT-middelen die de activiteiten binnen de deelprocessen ondersteunen;** ○ **Het in hoofdlijnen analyseren hoe IT-middelen kunnen worden aangevallen of kunnen worden misbruikt;** ○ **Het bepalen van de gevolgen voor het deelproces als het IT-middel uitvalt of wordt verstoord;** ○ **De BIV-classificatie per IT-middel vaststellen.**	**Beveiligingsadviseur, Security Architect, Ontwerpers**
6. Controle Resultaat BIA: ○ **Het controleren op naleving van het BIA-proces.**	**Opdrachtgever**

Het resultaat van de BIA is een lijst van IT-middelen die relevant zijn voor het deelproces, met een BIV-classificatie per IT-middel.

Stap 1. Doelstelling van het bedrijfsproces

De doelstellingen van een bedrijfsproces zijn leidend bij de inventarisatie van de eisen voor Beschikbaarheid en Integriteit. Het bedrijfsproces is opgebouwd uit een of meer primaire en ondersteunende deelprocessen, waarbij wordt vastgesteld in welke mate die voor hun correcte en tijdige uitvoering afhankelijk zijn van de IT-middelen en wat de gevolgen zijn van eventuele onbeschikbaarheid van die IT-middelen. De opdrachtgever maakt de volgende afwegingen:

Overwegingen voor Bedrijfsproces
Wat zijn de doelstellingen van het bedrijfsproces? ○ **Hoe lang kan het bedrijfsproces onderbroken of verstoord zijn voordat dit leidt tot ernstige consequenties voor de organisatie?** ○ **Uit welke primaire en ondersteunende deelprocessen bestaat het bedrijfsproces?** ○ **Wat is de invloed van een onderbreking of verstoring van deze deelprocessen op het behalen van de doelstellingen van het bedrijfsproces?** ○ **Welke compenserende maatregelen zijn beschikbaar om bij een onderbreking of verstoring de doelstellingen van het bedrijfsproces alsnog of deels te realiseren?**

`

Het resultaat van deze stap is een lijst van deelprocessen en hun invloed op het bedrijfsproces, plus een overzicht van compenserende maatregelen om de ernst van de gevolgen van een falend deelproces te verminderen.

Stap 2. Bepalen van de scope

De opdrachtgever maakt een selectie van de voor het uitvoeren van het bedrijfsproces relevante deelprocessen, die van essentieel belang zijn om de gewenste doelstellingen te kunnen realiseren. Per relevant deelproces gelden de volgende overwegingen voor de opdrachtgever:

Overwegingen voor Deelproces en Informatiestromen
Welke informatiestromen zijn identificeerbaar binnen het deelproces? ○ **Welke IT-middelen ondersteunen het deelproces en de informatiestromen?** ○ **Op welke wijze kan een IT-middel het deelproces of de informatiestromen onderbreken of verstoren?** ○ **Wanneer het IT-middel uitvalt of niet goed functioneert, blijven de consequenties daarvan alleen beperkt tot het ondersteunde deelproces, of worden daarmee ook andere deelprocessen onderbroken of verstoord?** ○ **Welke compenserende maatregelen zijn beschikbaar om een onderbreking of verstoring van een IT-middel tijdelijk of permanent op te vangen?**

Het resultaat van deze stap is een lijst van IT-middelen en hun invloed op het deelproces en de informatiestromen, plus een overzicht van compenserende maatregelen voor falende IT-middelen.

Stap 3. Selectie van kaderstellende documenten

De beveiligingsadviseur stelt de zakelijke en juridische eisen voor het deelproces en de informatiestromen vast aan de hand van relevante beleidsdocumenten en architectuurdocumenten en de relevante wet- en regelgeving.
Het resultaat van deze stap is een overzicht van de zakelijke en juridische eisen, die gelden als een verplicht kader voor de onderliggende IT-middelen.

Stap 4. Vaststellen van de dreigingen

De beveiligingsadviseur en de Security Architect identificeren de mogelijke dreigingen voor de IT-middelen binnen de deelprocessen en informatiestromen. Hiertoe wordt de centrale lijst met attack patterns en dreigingen gehanteerd, zodat vanuit een eenduidige benadering de risicobeheersing wordt uitgevoerd.
Mogelijke dreigingen zijn inbraken door hackers, DDoS-aanvallen, virusaanvallen, Trojaanse paarden, interne en externe fraude met gegevens en transacties, misbruik van onbeschermde achterdeuren in de systemen en netwerken, technische storingen, uitval van een rekencentrum, uitval van netwerken etc. Hierbij kan tevens gebruik worden gemaakt van externe informatiebronnen over dreigingen, zoals de OWASP Top-10, NCSC Advisories etc.
Het resultaat van deze stap is een overzicht van de relevante dreigingen voor de IT-middelen binnen de beschouwde scope.

Stap 5. Afhankelijkheden van IT-middelen

In deze stap analyseren de beveiligingsadviseur, de Security Architect en de ontwerpers de afhankelijkheid van de IT-middelen die de activiteiten binnen de deelprocessen en de informatiestromen ondersteunen. Er moet worden vastgesteld hoe de IT-middelen kunnen worden aangevallen of kunnen worden misbruikt en wat de gevolgen voor het deelproces en de informatiestromen als het IT-middel uitvalt of wordt verstoord.

Overwegingen voor de Afhankelijkheden van IT-middelen
De opdrachtgever combineert per IT-middel de bovengenoemde tussenresultaten: ○ **De afhankelijkheid van het bedrijfsproces voor een falend deelproces en de daarvoor eventueel beschikbare compenserende maatregelen;** ○ **De afhankelijkheid van een deelproces en de informatiestromen voor een falend IT-middel en de daarvoor eventueel beschikbare compenserende maatregelen;** ○ **De zakelijke en juridische eisen;** ○ **De mogelijk relevante dreigingen voor de IT-middelen binnen de scope.**

Het resultaat van deze stap is een lijst van IT-middelen die relevant zijn voor het deelproces, met een BIV-classificatie per IT-middel en een motivatie waarom voor deze BIV-classificatie is gekozen.

Stap 6. Controle Resultaat BIA

De opdrachtgever is verantwoordelijk voor het uitvoeren van de BIA en daarmee ook voor de correctheid van het resultaat. In dit kader wordt hij of zij geassisteerd door de beveiligingsadviseurs en Security Architecten bij het interpreteren van de lijst van IT-middelen en het stellen van prioriteiten voor de uit te voeren risicoanalyses.

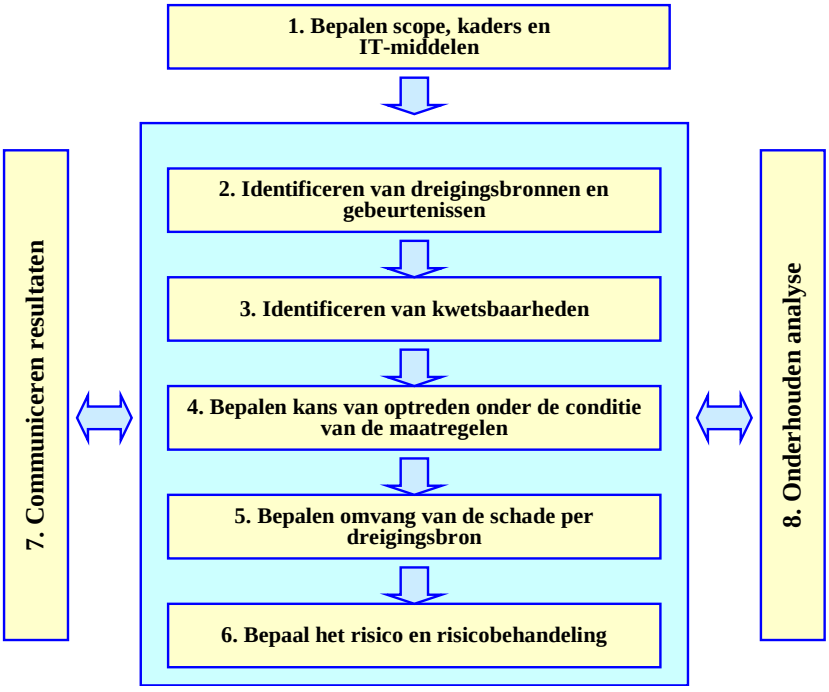
De opdrachtgever verifieert of het uiteindelijke doel is gerealiseerd, namelijk inzicht in de BIV-classificaties van alle software, dat wil zeggen van alle informatiesystemen, (web)applicaties, gegevensverzamelingen etc. binnen de scope.

Bijlage D: Risicoanalyse methodiek

Het proces voor risicoanalyse per relevant IT-middel is gebaseerd op de standaard NIST Special Publications 800-30 'Guide for Conducting Risk Assessments'. Dit is een IT-middel effectgeoriënteerde aanpak, waarmee aandacht wordt besteed aan de kwetsbaarheden en risico's die inherent zijn aan de gebruikte IT-middelen en de context waarbinnen die IT-middelen worden gebruikt. Hierbij worden de bronnen van dreigingen op IT-middelen geïdentificeerd, onder andere met behulp van de resultaten van de Business Impact Analyse (BIA):

- De dreigingen zijn veelal gerelateerd aan de kwetsbaarheden van de gekozen IT-middelen;
- De dreigingen die voortvloeien uit het uitvoeren van activiteiten worden ook meegenomen bij de analyse;
- De risico's zijn gericht op uitbuiting van de afhankelijkheden en kwetsbaarheden van de IT-middelen.

De processtappen zijn:



Figuur 10: processtappen in een risicoanalyse

In het risicoanalyseproces worden de volgende stappen doorlopen:

- Het vaststellen van de scope voor de risicoanalyse, namelijk het identificeren van de IT-middelen (informatiesystemen, applicaties, gegevensverzamelingen en andere bedrijfsmiddelen) waarvoor de risico's en de vereiste aanvullende maatregelen moeten worden bepaald. Tevens worden hierbij de zakelijke en juridische kaders en andere relevante gegevens uit de BIA gekopieerd;
- Het identificeren van dreigingsbronnen en dreigingsgebeurtenissen die relevant zijn binnen de gekozen scope;
- Het identificeren van de bekende kwetsbaarheden;
- Het bepalen van de kans van optreden van de dreigingen, onder de conditie van het bestaande of voorziene stelsel van maatregelen en de bekende kwetsbaarheden;
- Het bepalen van de omvang van de schade bij een inbreuk op de kwaliteitsaspecten Beschikbaarheid, Integriteit of Vertrouwelijkheid;
- Het bepalen van het risico. Dit is het combineren van de kans van optreden en de omvang van de te verwachten schade, gezien over alle dreigingen.

Bij deze analyse wordt gebruik gemaakt van het netto risico, namelijk het risico dat overblijft als men veronderstelt dat het bestaande en reeds voorziene stelsel van maatregelen voor informatiebeveiliging goed functioneert.

Hieronder worden de processtappen verder toegelicht.

Stap 1. Bepalen scope, kaders en IT-middelen

De opdrachtgever stelt de context en de scope vast.

Stap 1. Bepalen scope, kaders en IT-middelen
○ **De opdrachtgever bepaalt het doel van de risicoanalyse. Deze kan betrekking hebben op het in kaart brengen van risico's voor een deelproces of informatiestroom, of op een vernieuwing van een of meer IT-middelen, of op een majeur project voor nieuwe IT-middelen.**
○ **Bij de BIA is de relatie geschetst tussen de bedrijfsprocessen, de deelprocessen, de informatiestromen en de daarbinnen gebruikte IT-middelen. Tevens zijn de zakelijke en juridische randvoorwaarden geïnventariseerd voor de activiteiten.**
○ **De opdrachtgever selecteert uit dit BIA-overzicht de IT-middelen die relevant zijn binnen de scope van deze risicoanalyse. Aan de hand van de BIV-classificatie van deze IT-middelen stelt hij of zij de prioriteiten vast voor de risicoanalyse, waarbij hij met name de IT-middelen opneemt die afwijken van de baseline.**

Een IT-middel kan volstaan met de baseline aan maatregelen voor informatiebeveiliging als de BIV-classificatie is 'B = Midden, I = Midden en V = Risicoklasse 2'.

Zodra er sprake is van een hogere of lagere classificatie dient het IT-middel te worden opgenomen in de lijst voor het uitvoeren van een risicoanalyse. Indien men meer of minder maatregelen wil treffen dan de baseline voorschrijft geldt het principe 'Comply or Explain'.

Het resultaat van deze stap is een lijst met IT-middelen waarvoor het risico moet worden bepaald, plus een overzicht van de zakelijke en juridische kaders waarbinnen met deze IT-middelen moet worden gewerkt.

Stap 2. Identificeren van de dreigingsbronnen

De gebeurtenissen, of dreigingsbronnen worden geïdentificeerd, die kunnen leiden tot een inbreuk op een of meerdere kwaliteitsaspecten van de gekozen IT-middelen. Bij deze dreigingsbronnen wordt rekening gehouden met de mogelijkheden van de dreigingsbron en de intentie van de dreigingsbron.

Stap 2. Identificeren Dreigingsbronnen en gebeurtenissen
○ **De organisatie houdt een centraal overzicht bij van de dreigingen die relevant zijn voor de bedrijfsprocessen en de onderliggende IT-middelen. Dit overzicht maakt onderscheid naar applicaties met webtoegang en zonder, de verschillende gebruikte platformen (besturingssystemen en middleware) en wel of niet onderdeel van een financiële stroom;** ○ **De opdrachtgever selecteert uit dit overzicht de dreigingen die relevant zijn binnen de scope.**
○ **De opdrachtgever organiseert een risicoworkshop;** ○ **De risicoworkshop wordt bijgewoond door experts op het gebied van de betreffende (web)applicaties, platformen, middleware en netwerken, plus vertegenwoordigers vanuit de te ondersteunen deelprocessen;** ○ **Het resultaat van de workshop is een lijst van de dreigingen die betrekking hebben op de IT-middelen binnen de scope.**
○ **De opdrachtgever analyseert de bronnen van de verschillende risico's. Met dit inzicht wordt vervolgens de mogelijkheden, bijvoorbeeld van hackers of fraudeurs en de intentie van de bronnen in kaart gebracht om tot een beter beeld te komen van het risico.**

Het resultaat van deze stap is een lijst met dreigingsbronnen en dreigingen die relevant worden geacht voor de IT-middelen binnen de scope.

Stap 3. Identificeren van de kwetsbaarheden

Ieder platform, zoals besturingssystemen en middleware, kent zwakheden. Via diverse bronnen, zoals de CIS Benchmarks, worden adviezen gegeven voor de hardening van platformen. Via tooling zoals een Compliance scan en Vulnerability scans kan de hardening en het gebruik van de juiste patchlevels worden bewaakt. Tevens worden audits uitgevoerd, waarbij door de auditors gedetecteerde zwakheden als bevindingen worden gerapporteerd.

De organisatie dient de zwakheden binnen de eigen infrastructuur te kennen en deze gestructureerd vast te leggen. Als bron kan men de rapportages gebruiken vanuit de tooling, de bevindingen van de auditors en de kennis en ervaring van de beheerders van de IT-middelen.

In deze processtap worden de kwetsbaarheden van de gekozen IT-middelen geïdentificeerd en onder welke omstandigheden dergelijke kwetsbaarheden kunnen worden uitgebuit.

Stap 3. Identificeren van kwetsbaarheden
○ **De organisatie houdt een overzicht bij van de kwetsbaarheden die relevant zijn voor de IT-middelen. Dit overzicht maakt onderscheid naar applicaties met webtoegang en zonder, de verschillende gebruikte platformen (besturingssystemen en middleware) en wel of niet onderdeel van een financiële stroom;** ○ **De opdrachtgever selecteert uit dit overzicht de kwetsbaarheden die relevant zijn binnen de scope.**
○ **De opdrachtgever organiseert een tweede risicoworkshop;** ○ **De risicoworkshop wordt bijgewoond door experts op het gebied van de betreffende (web)applicaties, platformen, middleware en netwerken, plus vertegenwoordigers vanuit de te ondersteunen deelprocessen;** ○ **De omstandigheden waarin de eerder opgesomde kwetsbaarheden kunnen worden uitgebuit, worden geëvalueerd en besproken;** ○ **Hierbij worden de kwetsbaarheden van de IT-middelen zelf bekeken en niet bijvoorbeeld de zwakheden in de onderliggende infrastructuur, tenzij door een combinatie van de infrastructuur met het IT-middel een specifieke zwakheid ontstaat;** ○ **Het resultaat van de workshop is een lijst van de relevante kwetsbaarheden die betrekking hebben op de IT-middelen binnen de scope.**
○ **De opdrachtgever analyseert de bronnen van de verschillende kwetsbaarheden. Met dit inzicht wordt vervolgens de mogelijkheden, bijvoorbeeld van hackers of fraudeurs en de intentie van de bronnen in kaart gebracht om tot een beter beeld te komen van het risico.**

Het resultaat van deze stap is een lijst met kwetsbaarheden die relevant worden geacht voor de IT-middelen binnen de scope en inzicht hoe deze kwetsbaarheden zouden kunnen worden misbruikt.

Stap 4. Bepalen van de kans van optreden

Nu de dreigingsbronnen en de bronnen van kwetsbaarheden inzichtelijk zijn, wordt geanalyseerd wat de kans is dat de geïdentificeerde dreigingen op zullen treden en de kans dat de bedreiging een kwetsbaarheid succesvol uitbuit.

Stap 4. Bepalen Kans van optreden
○ **De opdrachtgever stelt de kans dat een bedreiging optreedt vast op basis van ervaring en inzicht van de betrokkenen;** ○ **Deze kans wordt ingedeeld naar 'laag', 'midden' of 'hoog', zoals hieronder beschreven.**
○ **De opdrachtgever maakt een inschatting of de dreiging in staat zal zijn een kwetsbaarheid op een succesvolle wijze uit te buiten.**

Voor de bepaling van de kans van optreden geldt de volgende indeling:

Kans van optreden	**Definitie**
Hoog	Het voorval is zeer waarschijnlijk. Er zijn geen of onvoldoende mitigerende maatregelen genomen om te voorkomen dat het voorval ook daadwerkelijk ernstige gevolgen heeft.
Midden	Het voorval is waarschijnlijk. Er zijn echter voldoende mitigerende maatregelen genomen zodat de schade bij optreden van beperkt blijft.
Laag	Het voorval is niet waarschijnlijk of er zijn ruim voldoende mitigerende maatregelen genomen zodat er geen significante schade zal optreden.

Het resultaat van deze stap is een lijst met dreigingsbronnen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht hoe groot de kans is dat deze manifest worden.

Stap 5. Bepalen omvang van de schade

Per dreiging of dreigingsbron wordt een inschatting gedaan over de magnitude van de schade aan het IT-middel, waarna de mogelijke gevolgen worden vastgesteld voor de deelprocessen en het bovenliggende bedrijfsproces.

Stap 5. Bepalen Omvang van de schade
○ **De opdrachtgever bepaalt per dreiging of dreigingsbron de gevolgen voor het IT-middel op het moment dat het risico manifest wordt. Hierbij wordt verondersteld dat de reeds geïmplementeerde en voorziene maatregelen voor informatiebeveiliging effectief zijn;** ○ **De opdrachtgever stelt de omvang van de mogelijke schade vast voor de deelprocessen en het bovenliggen bedrijfsproces.**

Voor de bepaling van de omvang van de mogelijke schade geldt de volgende indeling:

Omvang van de schade	**Definitie**
Hoog	De te verwachten schade leidt tot ernstige (politieke) imagoschade of ernstige vertrouwensschade bij de ketenpartners.
Midden	De te verwachten schade leidt tot beperkte imagoschade of beperkte vertrouwensschade bij een van de ketenpartners.
Laag	De te verwachten schade leidt nauwelijks tot imagoschade of vertrouwensschade bij ketenpartners.

Het resultaat van deze stap is een lijst met dreigingsbronnen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht in de omvang van de mogelijke schade als deze manifest worden.

Stap 6. Bepalen van de risico's

Het vaststellen van de ernst van een risico is het combineren van de kans van optreden van een bedreiging die daadwerkelijk tot uitbuiting van een kwetsbaarheid leidt en de omvang van de mogelijke schade van een dergelijke uitbuiting.

Stap 6. Bepalen van de risico's
○ **De opdrachtgever stelt de ernst van een risico vast;** ○ **Aangezien een kwalitatieve analysemethode wordt gebruikt, betreft dit vooral het gebruiken van ervaring in combinatie met het gezonde verstand bij het maken van de afweging;** ○ **Het is aan te raden de afwegingen en conclusies te toetsen bij de direct betrokkenen, ter verificatie of zij eenzelfde risicoappreciatie hebben als de opdrachtgever.**

Voor de bepaling van de ernst van de risico's wordt de kans van optreden gecombineerd met de omvang van de mogelijke gevolgen volgens de onderstaande indeling:

Risico			
	Omvang van de gevolgen		
Kans van optreden	**Laag**	**Midden**	**Hoog**
Laag	Laag	Laag	Midden
Midden	Laag	Midden	Hoog
Hoog	Midden	Hoog	Hoog

Het eindresultaat van deze risicoanalyse is een lijst met dreigingsbronnen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht in de ernst van de dreigingen.
Deze lijst is het uitgangspunt voor het bepalen of aanvullende maatregelen nodig zijn en om vast te stellen of er mogelijk nog een restrisico bestaat. Dat is een risico dat niet wordt gemitigeerd door het bestaande en voorziene stelsel van maatregelen voor informatiebeveiliging. Indien er sprake is van een restrisico dient dit te worden gemeld aan de eindverantwoordelijke, die schriftelijk het restrisico moet accepteren namens de organisatie.

Bijlage E: CAPEC Attack patterns

CAPEC is een openbare, door de community ontwikkelde lijst van 1.000 attacks, geordend naar patterns. Iedere attack is voorzien een uitleg. Deze lijst is een goede basis om met de leverancier van software afspraken te maken over hoe wordt omgegaan met bekende attacks en welke maatregelen de leverancier daar standaard voor treft.

De onderstaande nummering refereert naar het attack pattern in de CAPEC-1000 lijst versie 2.0.

- **Toegang tot de systemen wordt misbruikt:**
  Ga na of de interactie met de systemen kunnen worden misbruikt voor:
  - **Data Leakage Attacks - (118):**
    Een hacker misbruikt de communicatiemogelijkheden in een applicatie om vertrouwelijke informatie op te vragen. Dit kunnen persoonlijke gegevens zijn of informatie over de applicatie zelf, waarmee vervolgens zwakheden kunnen worden gevonden, waarop andere attacks worden uitgevoerd;
  - **Resource Depletion - (119):**
    Een hacker overbelast een applicatie, waardoor de applicatie tegen een grens aanloopt en zich onjuist gedraagt, of waardoor Data Leakage ontstaat;
  - **Abuse of Functionality - (210):**
    Een hacker gebruikt de functionaliteit van een applicatie voor doeleinden waarvoor die niet was bedoeld en kan hierdoor onveilige activiteiten uitvoeren;
  - **Probabilistic Techniques - (223):**
    Een hacker vindt gaten in de beveiliging door simpelweg (of slim) veel pogingen te ondernemen. Ook als de kans klein is, lukt het de hacker vaak om binnen te komen.

- **De identiteit van een gebruiker wordt misbruikt:**
  Voorkom dat de identiteit van de gebruiker kan worden misbruikt voor of via:
  - **Social Engineering Attacks - (403):**
    Een hacker manipuleert gebruikers en stimuleert hen tot het uitvoeren van acties, het onthullen van vertrouwelijke informatie, of het verschaffen van fysieke toegang tot computersystemen of faciliteiten. Een aantal vormen van social engineering zijn beschreven in http://www.social-engineer.org;
  - **Spoofing - (156)**
    Een hacker verbergt zijn of haar eigen identiteit door die van een ander te gebruiken. Zo worden gegevens op naam van de ander verkregen of worden aan een ander onjuiste gegevens verstrekt;
  - **Exploitation of Authentication - (225):**
    Een hacker verkrijgt de gegevens over de authenticatie van een gebruiker doordat de authenticatievoorziening de gegevens niet afdoende heeft afgeschermd;
  - **Exploitation of Privilege/Trust - (232):**
    Een hacker of gebruiker heeft rechten of eigent zich die toe en voert daarmee ongeautoriseerde handelingen uit. Hierbij wordt de reguliere controle of functiescheiding ontweken.

- **De invoer van gegevens wordt misbruikt:**
  Ga na dat de ingevoerde gegevens geen instructies bevatten:
  - **Injection - (152):**
    Een hacker voert in een invoerveld niet een gegeven in, maar een instructie zoals een SQL-statement. Als de software de invoerinformatie doorlaat wordt deze niet verwerkt als een gegeven, maar wordt de instructie uitgevoerd.

- **Zwakheden in de software worden benut:**
  Voorkom dat het ontwerp niet aansluit op de gewenste afhandeling van taken, waardoor de software mogelijk ongewenst gedrag vertoont of toegang geeft tot vertrouwelijke gegevens:
  - **Time and State Attacks - (172):**
    Een hacker zorgt ervoor dat meerdere activiteiten elkaar zodanig nadelig beïnvloeden dat de applicatie in een ongewenste situatie komt, waardoor deze ongewenst gedrag vertoont;
  - **Data Structure Attacks - (255):**
    Een hacker heeft of verkrijgt toegang tot vertrouwelijke gegevens, doordat deze niet in een afdoende mate worden afgeschermd door de gegevensstructuur, het ontwerp of de opslagmethode;
  - **Resource Manipulation - (262):**
    Een hacker manipuleert de instellingen van de software of heeft directe toegang tot vertrouwelijke gegevens.

- **Zwakheden in de fysieke beveiliging worden benut:**
  Voorkom fysieke toegang, waarmee de logische toegang wordt omzeild:
  - **Physical Security Attacks - (436):**
    Een hacker probeert fysieke toegang te verkrijgen tot vertrouwelijke gegevens, software, hardware of netwerk.

Bijlage F: Volwassenheidsniveaus

In deze bijlage wordt een voor SSD gebruikte variant op het Capability Maturity Model (CMM) toegelicht. Dit model hanteert 5 volwassenheidsniveaus, die beschrijven in welke mate een organisatie zich heeft ontwikkeld of kan ontwikkelen.
De vijf niveaus zijn:

1. Informeel of ad hoc uitgevoerd (performed);
2. Beheerst proces (managed);
3. Vastgesteld proces (established);
4. Voorspelbaar proces (predictable);
5. Geoptimaliseerd proces (optimized).

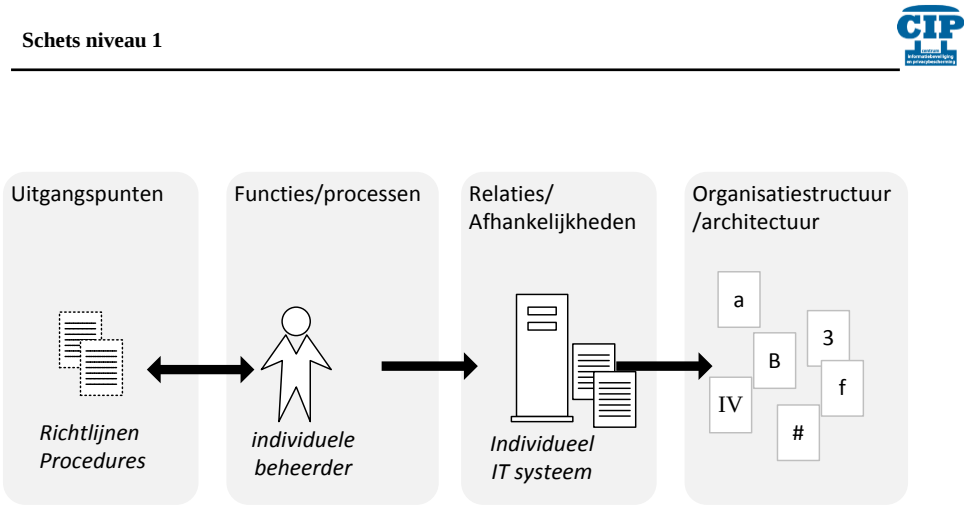
Iedere organisatie is vrij in het voor SSD na te streven niveau. Voor de meeste organisaties is niveau 3 afdoende. Hogere niveaus vragen om grote investeringen en een hoog bewustzijn binnen de gehele organisatie.

Het niveau dat wordt nagestreefd vormt de stip op de horizon. Een invulling van de processen voor SSD evolueert als de beveiligingsorganisatie zich vormt. De tussenliggende niveaus vormen de stappen daar naartoe.

Niveau 1 – Informeel uitgevoerd (performed)

Op niveau 1 wordt door de (externe) leverancier software ontwikkeld, terwijl de eigen organisatie in onvoldoende mate beschikt over beleid, richtlijnen, beveiligingseisen of (werk)instructies om de leverancier aan te sturen. Hierbij ontbreekt het aan formele specificatieprocessen en processen om eisen te stellen en ingerichte testprocessen met bijvoorbeeld penetratietests.

Ondanks het ontbreken van deze faciliteiten worden de basale practices voor informatiebeveiliging uitgevoerd en zo eisen aan de software gesteld. Dit gebeurt op basis van de persoonlijke expertise en inzet van de betrokkenen.

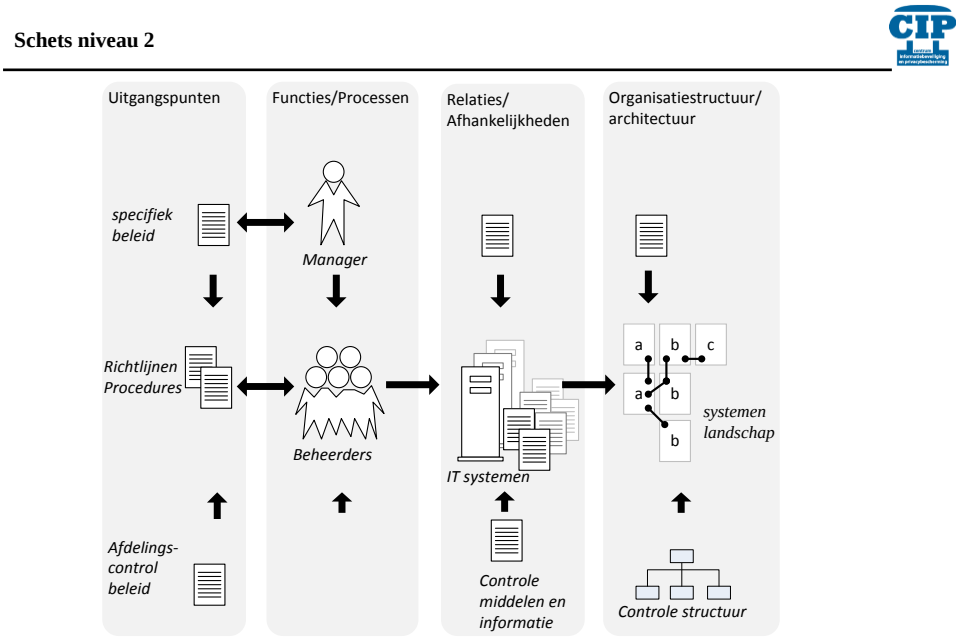


Figuur 11: schets niveau 1 volwassenheid

De schets voor niveau 1 geeft aan dat er geen of slechts beperkt sprake is van enige vorm van instructies, procedures op proces en object niveau (de software). Het meegeven van eisen en het bewaken van de kwaliteit van de software vindt plaats op aangeven van de individuele functionaris voor informatiebeveiliging. De taken en verantwoordelijkheden van dit type functionarissen zijn wel beschreven.

Niveau 2 – Beheerst proces (managed)

Op niveau 2 wordt de eigen organisatie ondersteund door operationeel beleid en richtlijnen op afdelingsniveau. Er ligt een zekere mate van architectuur aan ten grondslag. De eisen worden niet meer per applicatie bedacht en meegegeven aan de leverancier, maar de eisen worden hergebruikt en er vindt periodiek evaluatie plaats van beleid van de eigen afdeling.
De organisatie leert slechts op lokaal (afdelings-) niveau, omdat alleen een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen. Daardoor is de werkwijze op lokaal niveau wel traceerbaar, herhaalbaar en gestandaardiseerd, maar nog niet organisatiebreed.
Er is structurele rapportage over de veiligheid van software op projectniveau, maar nog geen structurele rapportage van afdelingsniveau naar het hogere management.



Figuur 12: schets niveau 2 volwassenheid

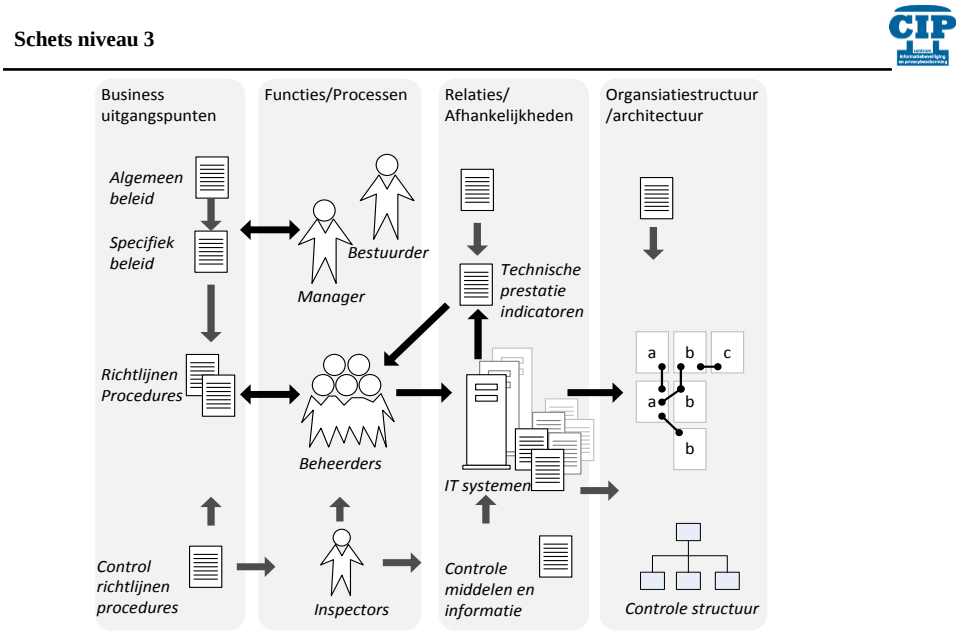
De schets voor niveau 2 geeft aan dat het beleid, richtlijnen en werkinstructies op afdelingsniveau vastliggen en sturing op de naleving bestaat. Dit leidt tot een lerend proces. De organisatie brede architectuur met het applicatielandschap en daarmee de te hanteren enterprise security-architectuur blokken zijn beperkt beschreven.

Op dit niveau staat het beleid, richtlijnen en werkinstructies niet noodzakelijkerwijs in verband met het beleid en de richtlijnen op organisatieniveau. De specificatieprocessen zijn niet structureel ingericht, waarbij er geen relatie vastligt tussen de specificatieprocessen en de overige processen voor informatievoorziening en beveiliging. De meegegeven eisen sluit ook niet noodzakelijkerwijs aan op de architectuur van het bedrijfsbrede IT-landschap.

Niveau 3 – Vastgesteld proces (established)

Op niveau 3 wordt de eigen organisatie ondersteund door beleid en richtlijnen op afdelingsniveau en bedrijfsniveau. Beleid, richtlijnen en werkinstructies op afdelingsniveau sluiten aan op het beleid en de richtlijnen op organisatieniveau.
Overeenkomstig niveau 2 worden de eisen niet meer per applicatie bedacht en meegegeven aan de leverancier, maar de eisen worden hergebruikt en vindt er periodiek evaluatie plaats van het beleid. In aanvulling op niveau 2 ligt er een duidelijke relatie tussen het gehanteerde beleid en de bedrijfsbrede architectuur. De vereisten vanuit de organisatie zijn vertaald naar niet alleen de applicaties, maar ook de inrichting van de context, de systemen, het IT-landschap en de beheerprocessen. Deze vertaling is geborgd en wordt bewaakt.

De processen voor specificaties, testen en management zijn organisatiebreed structureel ingericht en zijn traceerbaar, herhaalbaar en gestandaardiseerd. De organisatie leert bedrijfsbreed, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op zowel afdelingsniveau als bedrijfsniveau. Er is een structurele rapportage over de veiligheid van de software naar het hogere management. De leercyclus op algemeen en specifiek beleidsmatig niveau neemt meerdere maanden in beslag.



Figuur 13: schets niveau 3 volwassenheid

De schets voor niveau 3 geeft aan dat het beleid, richtlijnen en (werk)instructies zowel op afdelingsniveau als op bedrijfsniveau vastliggen en er sturing op de naleving bestaat. In tegenstelling tot niveau 2 wordt de sturing afgestemd met de bestuurder. De bestuurder is betrokken bij de handhaving van het beleid en de uitvoering, waarbij wordt gerapporteerd via zogenaamde inspectors die worden ondersteund door controlemiddelen en informatie.

In de SSD-methode wordt het controlemiddel en informatie gevormd door het dashboard. Desgewenst vindt er aanscherping of juist afzwakking van het beleid en de gehanteerde richtlijnen plaats. Dit leidt tot een lerend proces op zowel afdelingsniveau als op bedrijfsniveau. De architectuur organisatiebreed

van het systeemlandschap en daarmee de te hanteren enterprise security-architectuur blokken zijn beschreven en worden gehanteerd. Op dit niveau sluit het beleid, richtlijnen en werkinstructies op afdelingsniveau aan op het beleid en de richtlijnen op organisatieniveau. De specificatieprocessen zijn structureel ingericht en worden bedrijfsbreed gehanteerd. De specificatieprocessen sluiten aan op de processen voor informatievoorziening en informatiebeveiliging en omgekeerd. De meegegeven eisen sluiten op de architectuur van het bedrijfsbrede IT-landschap.

Verhogen van de efficiëntie op niveau 4 en 5

Een verdere groei in volwassenheid in niveaus 4 en 5 richt zich op de verbetering van efficiency in de cycli tussen beleid en controle. Dit past bij zowel ISO/IEC-15504 en CobiT, als bij CMMi. In beide standaarden worden de bovenliggende niveaus enkel benaderd vanuit wijziging in bestuurlijke volwassenheid en niet door de procesgerelateerde volwassenheid.

Niveau 4 – Voorspelbaar proces (predictable)

Op niveau 3 is er een actieve relatie tussen de verschillende betrokkenen en de verschillende processen. In aanvulling op niveau 3 wordt er op niveau 4 gestuurd op de snelheid van de interacties. De organisatie leert daarbij per te accepteren applicatie(-wijziging), zonder dat de samenhangen tussen de keuzen op afdelingsspecifiek niveau en bedrijfsalgemeen niveau uit het oog wordt verloren.
De operationele werkelijkheid wordt voortdurend bewaakt en aangepast om de organisatiebrede beleidsdoelen te behalen.

Beleid, richtlijnen en werkinstructies sluiten aan op het beleid en de richtlijnen op organisatieniveau. De processen zijn structureel. De vereisten vanuit de organisatie zijn vertaald naar de eisen voor de software, de bedrijfsbrede architectuur, inclusief het IT-landschap en de (beveiligings-)organisatie. Deze vertaling is geborgd en wordt bewaakt. Onderdeel van de bewaking is een structurele (frequente) rapportage vanuit de SSD-processen naar de verschillende managementniveaus. Het management heeft op ieder gewenst moment inzicht in de stand van zaken.

Het lerend vermogen in de uitvoerende en specifieke beleidsmatige laag is op niveau 4 tot een maximum geoptimaliseerd. Dit is mogelijk door de verregaand geautomatiseerde feedbacklus op de specifiek beleidsmatige laag.

Het lerend vermogen op algemeen beleidsmatig niveau is echter niet intrinsiek aan de uitvoerende processen, maar volgt uit feedback van de algemene controle. Deze leercyclus op algemeen beleidsmatig en specifiek beleidsmatig niveau neemt normaal gesproken nog steeds meerdere maanden in beslag.

Niveau 5 – geoptimaliseerd (optimized)

Op niveau 5 is in aanvulling op niveau 4 een sterk en expliciet (traceerbaar) verband tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering. Dit resulteert in de mogelijkheid om de organisatie dynamisch aan te passen op basis van praktische ervaringen en prognoses van buiten de eigen organisatie.

De organisatie leert op uitvoerend en beleidsmatig niveau, in een samenhangende vorm onder een algemeen beleid. De operationele werkelijkheid en effectiviteit van beleid worden voortdurend bewaakt. Het beleid kan op zeer korte termijn worden aangepast om invulling te geven aan plotselinge wijzigingen in de omgeving. Externe ontwikkelingen, zoals veranderende wet- en regelgeving, worden daarbij opvallend snel vertaald naar nieuw specifiek beleid en uitvoering. Bovendien is de organisatie in staat om daarbij prognoses af te geven over kosten en reactiesnelheid.

De bewaking en rapportage naar het hogere management is mede gebaseerd op de relatie tussen externe factoren en intern het algemeen beleid, specifiek beleid en de uitvoering. De prestatie-indicatoren zijn eenvoudig traceerbaar en vergelijkbaar met andere organisaties.
Het lerend vermogen is op alle lagen tot een maximum geoptimaliseerd, door de verregaande geautomatiseerde feedbacklussen op alle lagen.

Bijlage G: Volwassenheidsniveaus voor SSD

1. De SSD CCM niveaus voor het opstellen van beveiligingseisen

De volgende tabel toont de CMM niveaus voor het opstellen van beveiligingseisen.

B.01 Beveiligingseisen stellen		
SSD criterium (wie en wat)	De organisatie geeft beveiligingseisen mee aan de softwareleveranciers voor haar IT-diensten.	
	Niveau	Criterium (wie en wat)
SSD-CMM model	1. Informeel uitgevoerd (performed process)	De aan de leverancier meegegeven eisen bestaan uit een kopie uit standaard beveiligingseisen. De functionaris bepaalt bij het specificeren niet of slechts beperkt de samenhang met het bedrijfsbrede eisen. De eisen zijn niet tot stand gekomen na een risicoanalyse en een correlatie met de bedrijfsarchitectuur.
	2. Beheerst proces (managed process)	De aan de leverancier meegegeven eisen bestaan uit een selectie van standaard beveiligingseisen. Eisen worden bij meerdere software ontwikkeltrajecten ingezet. De eisen zijn met de leverancier afgestemd. Afspraken over het gebruik zijn met de leveranciers contractueel geborgd. Bij de selectie van de eisen is beperkt een correlatie gemaakt met de bedrijfsarchitectuur en enterprise security-architectuur blokken, waardoor nog slechts beperkt onnodige eisen worden voorkomen. De eisen zijn niet tot stand gekomen na een risicoanalyse. (specifiek beleid) Controle vindt plaats op de juistheid van de eisen vindt plaats in een cyclisch proces, waardoor deze periodiek worden geactualiseerd. (specifieke control)
	3. Vastgesteld proces (established)	In aanvulling op niveau 2 zijn de eisen in lijn gebracht met de bedrijfsarchitectuur en enterprise security-architectuur blokken, waardoor er geen onnodige eisen worden meegegeven. De eisen zijn tot stand gekomen na een risicoanalyse, waardoor de eisen aansluiten op de bedrijfsbehoefte. (algemeen beleid) Controle op de juistheid van de eisen vindt plaats op twee niveaus. In aanvulling op het niveau 2 worden ze periodiek gecorreleerd met de bedrijfsarchitectuur en de enterprise security-architectuur blokken. (algemene control)

B.01 Beveiligingseisen stellen			
	4. Voorspelbaar proces (predictable process)	In aanvulling op niveau 3 bestaan er prestatie-indicatoren van normen en metrieken die medewerkers op uitvoerend niveau in staat stellen om corrigerend op te treden c.q. tijdig maatregelen te nemen tegen beveiligingsrisico's in software. De uitvoering wordt daarmee van dag tot dag aantoonbaar in lijn gehouden met het specifieke beleid.	
	5. Geoptimali-seerd proces (optimized process)	In aanvulling op niveau 4 bestaan er prestatie-indicatoren van normen en metrieken die het hoger management in staat stellen om de leveranciers snel bij te sturen en consequenties voor (en van) beveiligingseisen vast te stellen. Dit is mogelijk door het hanteren van internationaal geaccepteerde prestatie-indicatoren. De specifieke en algemene eisen worden daarmee van dag tot dag aantoonbaar in lijn gehouden met doelstellingen van de organisatie.	
Indicatoren SSD-norm	<u>Cyclisch proces</u>		
	Het proces voldoet aan een standaard patroon, met daarin de elementen Voorbereiding, Ontwikkeling, Goedkeuring, Uitvoering/Implementatie en Evaluatie		Plan-Do-Check-Act (PDCA) Observe Orient, Do Act (OODA)

2. De SSD CCM niveaus voor code reviews

De volgende tabel toont de CMM niveaus voor code reviews.

SSD criterium (wie en wat)	De organisatie toetst of de software zo is geschreven dat voldaan kan worden aan voorwaarden die gesteld zijn.		
	Niveau	Criterium (wie en wat)	
SSD-CMM model	1. Informeel uitgevoerd (performed process)	Code reviews maken geen onderdeel uit van testplannen om de kwaliteit van software te bepalen, behalve als aangetoond moet worden dat de software structureel niet voldoet, wordt op ad hoc basis de leverancier gevraagd een rapportage van code reviews te leveren.	
	2. Beheerst proces (managed process)	Voor zeer bedrijfskritische applicaties wordt steekproefsgewijs een code review uitgevoerd. Afspraken hierover maken structureel onderdeel uit van het testplan. (specifiek beleid) Incidenteel wordt hier terugkoppeling op gegeven door de organisatie. (specifieke control)	
	3. Vastgesteld proces (established process)	Voor zeer bedrijfskritische applicaties wordt standaard een code review uitgevoerd. Afspraken hierover maken structureel onderdeel uit van het testplan. (algemeen beleid) Resultaten van de code reviews worden in het dashboard bijgehouden en meegenomen in het risicoacceptatieproces. (algemene control)	
	4. Voorspelbaar proces (predictable process)	Standaard wordt een code review uitgevoerd. Door gebruik van een methodische aanpak is onderlinge vergelijking van de kwaliteit van de software mogelijk.	
	5. Geoptimali-seerd proces (optimized process)	De leveranciers hanteren dezelfde tooling en prestatie-indicatoren, waardoor prestaties van de leveranciers onderling vergelijkbaar zijn.	
Indicatoren SSD-norm	<u>Cyclisch proces</u>		
	Het proces voldoet aan een standaard patroon, met daarin de elementen Voorbereiding, Ontwikkeling, Goedkeuring, Uitvoering/Implementatie en Evaluatie	Plan-Do-Check-Act (PDCA) Observe Orient, Do Act (OODA)	

3. De SSD CCM niveaus voor Security testen

De volgende tabel toont de CMM niveaus voor het Security testen.

B.03 Security testen		
SSD criterium (wie en wat)	De demand organisatie voert uit, of laat uitvoeren, een kwaliteitscontrole op de software.	
	Niveau	Criterium (wie en wat)
SSD-CMM model	1. Informeel uitgevoerd (performed process)	De keuze om te testen en/of te toetsen en de wijze waarop worden door de applicatie-eigenaar op ad-hoc basis genomen. Er wordt geen gebruik gemaakt van bedrijfsbrede testprocessen en testvoorzieningen. De testsets worden per release bepaald, waarbij er geen verband vaststaat met vooraf overeen gekomen beveiligingseisen.
	2. Beheerst proces (managed process)	Security testen gebeurt tegen bedrijfsbreed vastgestelde beveiligingseisen. Er wordt bij voorkeur gebruik gemaakt van bedrijfsbrede testprocessen en testvoorzieningen. De resultaten van de tests zijn onderling vergelijkbaar. De testsets zijn nog niet afgestemd op de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld. (specifiek beleid) De resultaten van de tests worden doorgegeven om centraal bijgehouden te worden in het dashboard. Er wordt nog niet bijgehouden of voldaan wordt aan de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld. (specifieke control)
	3. Vastgesteld proces (established process)	Security testen gebeurt tegen bedrijfsbreed vastgestelde beveiligingseisen. Er wordt gebruik gemaakt van bedrijfsbrede testprocessen en bij voorkeur ook van bedrijfsbrede testvoorzieningen. De resultaten van de tests zijn onderling vergelijkbaar. De testsets zijn afgestemd op de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld. (algemeen beleid) De resultaten van de tests worden doorgegeven om centraal bijgehouden te worden in het dashboard. Ook wordt bijgehouden of voldaan wordt aan de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld. (algemene control)
	4. Voorspelbaar proces (predictable process)	Bij het Security testen wordt gebruik kortcyclische processen, waardoor een eerder voorspelbaar is of software niet aan de eisen voldoet.

B.03 Security testen			
	5. Geoptimali-seerd proces (optimized process)	De leveranciers hanteren dezelfde tooling en prestatie-indicatoren, waardoor prestaties van de leveranciers onderling vergelijkbaar zijn.	
Indicatoren SSD-norm	<u>Cyclisch proces</u>		
	Het proces voldoet aan een standaard patroon, met daarin de elementen Voorbereiding, Ontwikkeling, Goedkeuring, Uitvoering/Implementatie en Evaluatie.	Plan-Do-Check-Act (PDCA) Observe Orient, Do Act (OODA)	

4. De SSD CCM niveaus voor pentesten

De volgende tabel toont de CMM niveaus voor pentesten.

B.04 Pentesten		
SSD criterium (wie en wat)	De organisatie toetst of de software ook tijdens het systeemgebruik geen beveiligingsrisico's bevat.	
	Niveau	Criterium (wie en wat)
SSD-CMM model	1. Informeel uitgevoerd (performed process)	Pentesten maken geen onderdeel uit van de beveiligingsaanpak volgens de SSD methode. Slechts na één of meerdere beveiligingsincidenten worden pentesten uitgevoerd.
	2. Beheerst proces (managed process)	Voor zeer bedrijfskritische applicaties worden pentesten uitgevoerd. Dit is echter nog geen periodiek proces. (specifiek beleid) Voor zeer bedrijfskritische applicaties worden de bevindingen bijgehouden in het dashboard en zo teruggekoppeld naar de applicatie eigenaren. (specifieke control)
	3. Vastgesteld proces (established process)	Voor de bedrijfskritische applicaties worden periodiek pentesten uitgevoerd. (algemeen beleid) Voor de bedrijfskritische applicaties worden de bevindingen bijgehouden in het dashboard en zo teruggekoppeld naar de applicatie eigenaren. (algemene control)
	4. Voorspelbaar proces (predictable process)	Direct na oplevering van een applicatie(-release) worden een pentesten uitgevoerd, zodat de bevindingen meegenomen kunnen worden in het acceptatieproces. Deze pentesten maken onderdeel uit van het testplan.
	5. Geoptimali-seerd proces (optimized process)	De direct na oplevering van een applicatie(-release) uitgevoerde pentesten worden gebruikt. Na een melding van een toename in beveiligingsdreigingen van de NCSC wordt gericht een pentest uitgevoerd. De resultaten worden gebruikt als criterium om de release terug te draaien of te besluiten een (applicatie)service tijdelijk uit te schakelen.
Indicatoren SSD-norm	<u>Cyclisch proces</u>	
	Het proces voldoet aan een standaard patroon, met daarin de elementen Voorbereiding, Ontwikkeling, Goedkeuring, Uitvoering/Implementatie en Evaluatie	Plan-Do-Check-Act (PDCA) Observe Orient, Do Act (OODA)

5. De SSD CCM niveaus voor risicoacceptatie

De volgende tabel toont de CMM niveaus voor risicoacceptaties.

B.05 Risicoacceptatie		
SSD criterium (wie en wat)	De applicatie-eigenaar binnen de demand organisatie heeft inzicht in de beveiligingsrisico's en accepteert tijdelijk eventuele restrisico's en neemt hierop actie.	
	Niveau	Criterium (wie en wat)
SSD-CMM model	1. Informeel uitgevoerd (performed process)	De risicoacceptatie is beperkt tot het informeren van de applicatie-eigenaar van de gevonden afwijkingen op de gestelde eisen. De applicatie-eigenaar accepteert de restrisico's zonder dat daar vervolgafspraken over worden gemaakt.
	2. Beheerst proces (managed process)	De applicatie-eigenaar wordt geïnformeerd over de gevonden afwijkingen op de gestelde eisen. De applicatie-eigenaar accepteert de risico's en deze worden bijgehouden in het dashboard. Afwijkingen op de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld zijn nog niet meegenomen en worden ook niet in het dashboard bijgehouden. (specifiek beleid) De applicatie-eigenaar accepteert de eventuele restrisico's op de bevindingen op de standaard baseline beveiligingseisen. Doordat deze in het dashboard worden bijgehouden en afgestemd met de applicatie-eigenaren worden daar vervolgafspraken over gemaakt. (specifieke control)
	3. Vastgesteld proces (established process)	De applicatie-eigenaar wordt geïnformeerd over de gevonden afwijkingen op de gestelde eisen. De applicatie-eigenaar accepteert de risico's en deze worden bijgehouden in het dashboard. Afwijkingen op de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld zijn daarin (vanaf niveau 3) wel meegenomen. (algemeen beleid) De applicatie-eigenaar accepteert de eventuele restrisico's op de bevindingen op de beveiligingseisen die zijn gebaseerd op de standaard baseline en de eisen die vanuit de bedrijfsbrede beveiligingsarchitectuur worden gesteld. Doordat beiden in het dashboard worden bijgehouden en afgestemd met de applicatie-eigenaren worden daar vervolgafspraken over gemaakt. (algemene control)

B.05 Risicoacceptatie			
	4. Voorspelbaar proces (predictable process)	Afstemming met de applicatie-eigenaar over de restrisico's en wegwerken van de restrisico's vindt niet alleen op basis van de bevindingen via het dashboard plaats. De applicatie-eigenaar voorkomt dat negatieve bevindingen in het dashboard terecht komen, door deze kortcyclisch weg te werken, dus door het versneld uitbrengen van een release, waarin de bevinding is weggewerkt.	
	5. Geoptimali-seerd proces (optimized process)	Het dashboard maakt gebruik van internationaal geldende prestatie-indicatoren. De afstemming en het wegwerken van de restrisico's met de applicatie-eigenaar leidt nog beperkt tot bevindingen. Bevindingen worden kortcyclisch weggewerkt. Het dashboard wordt gebruikt om aan te tonen dat de organisatie op het gebied van informatiebeveiliging optimaal functioneert.	
Indicatoren SSD-norm	<u>Cyclisch proces</u>		
	Het proces voldoet aan een standaard patroon, met daarin de elementen Voorbereiding, Ontwikkeling, Goedkeuring, Uitvoering/Implementatie en Evaluatie.	Plan-Do-Check-Act (PDCA) Observe Orient, Do Act (OODA)	

Bijlage H: Het gebruik van het dashboard

In het SSD dashboard wordt bijgehouden in hoeverre applicaties aan de beveiligingseisen voldoen. De inhoud van het dashboard is over de 2 assen dynamisch:

- De set van applicaties (geheel of gedeeltelijk) tegen beveiligingseisen worden aangehouden verandert in de tijd?
- De beveiligingseisen die tegen de beveiligingseisen worden aangehouden veranderen in de tijd.

Het is voor een correcte interpretatie van de inhoud van het dashboard van belang dat het dashboard met deze dynamica kan omgaan. Door het juiste gebruik van kleuren in het dashboard wordt de dynamica ondersteund en kan een zuivere rapportage over de compliancy met de SSD normen worden gegeven.

Het gebruik van kleuren in het SSD dashboard

De rapportages is steeds gericht op applicaties[1]. Uitspraken of een applicatie aan een eisen voldoet geldt altijd voor de gehele applicatie. Als een deel van de applicatie (bijvoorbeeld een module) niet aan de eis voldoet, voldoet daarmee de gehele applicatie niet aan deze eis. Deze lijn doortrekkend betekent dit:

- **Groen:**
  De gehele applicatie voldoet aan deze eis.

- **Rood:**
  In de applicatie is op één of meerdere plekken een afwijking geconstateerd. Welke afwijking dat is, wordt in een commentaarveld opgeslagen.

- **Lichtgroen:**
  De eis is voor deze applicatie niet van toepassing (nvt). Hierover is uitleg (comply) en overeenstemming verkregen.

- **Oranje:**
  Met de kleur oranje kan worden aangeduid dat met de applicatie-eigenaar afspraken zijn gemaakt over de eindigheid van de afwijking. (Dit conform het gedoogaanpak in 3.4.1 in het document van de SSD-methode.)

- **Wit:**
  Er is nog geen constatering, simpelweg omdat er nog geen formele constatering is. Dit geldt bij een nieuwe recent toegevoegde eis of bij een applicatie die nog niet of slechts gedeeltelijk tegen de SSD-normen is aangehouden.

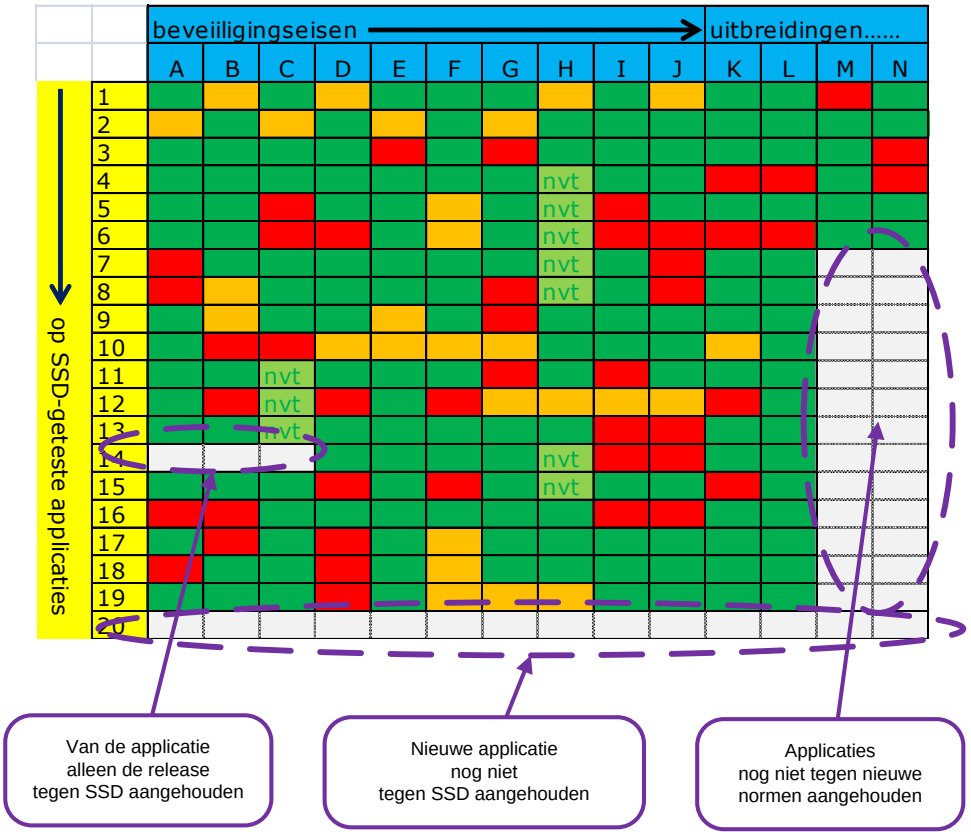
[1] In compliancy-termen: "Het object of control is de applicatie." Door in het dashboard ook de applicatie-eigenaar en de softwareleverancier bij te houden, kan ook bepaald worden in hoeverre de applicatie-eigenaar en de softwareleverancier in control zijn.

Dit betekent: Als in een release er alleen naar een module in een applicatie wordt gekeken, dan kunnen alleen uitspraken gedaan worden over afwijkingen, waarmee een constatering alleen van wit naar rood kan (of alleen "nog meer rood wordt") . Volgens deze redenatie kan, omdat niet naar de gehele applicatie is gekeken, bij deze wijziging nooit een constatering van wit naar groen.

In de praktijk kijkt de tester altijd naar de gehele applicatie. Dat een deel van de eisen voor een applicatie op wit staat na een release zal veelal alleen na oplevering door de leveranciers plaatsvinden. Hierbij doet de leverancier alleen een uitspraak over de opgeleverd module.

Hoe ziet het SSD dashboard qua kleuring in de praktijk eruit?

Doordat er nieuwe applicaties bijkomen of applicaties nog (steeds) niet tegen de SSD eisen zijn aangehouden en doordat het aantal eisen in de praktijk gaat toenemen, zal steeds op een deel van de eisen bij verschillende applicaties nog niet test (of toets) hebben plaatsgevonden.
Hierdoor kan het dashboard bijvoorbeeld de volgende vulling hebben.



Bijlage I: Referentiedocumentatie

- Grip op Secure Software Development website: http://gripopssd.org

- Software Security: Building Security In, Gary McGraw, ISBN: 0-321-35670-5, Januari 2006
- Procedure Risicoanalyse, Standaard methodiek Groep ICT, RABO-groep, 4 januari 2011
- Team Software ProcessSM (TSPSM) Body of Knowledge (BOK), Juli 2010, Technical Report CMU/SEI-2010-TR-020, ESC-TR-2010-020
- https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/326-BSI.html
- http://nl.wikipedia.org/wiki/ISO_25010
- Presentatie iComply: Secure Software foundation, 13 februari 2013, Woerden
- BSIMM4, september 2012, Gary McGraw, Sammy Migues en Jacob West
- Department of Homeland Security (DHS) Build Security In: https://buildsecurityin.us-cert.gov/bsi/home.html
- http://www.sig.eu/nl/Nieuws_en_Publicaties/Publicaties/697/__Ontwerp_versus_implementatie_–_de_kans_om_ze_niet_uiteen_te_laten_lopen__.html
- Baseline Informatiebeveiliging Rijksoverheid; 1 december 2012
  http://www.informit.com/articles/article.aspx?p=446451
- Risicoanalyse, Een verkenning, Publicatie van de CIO Interest Group Informatiebeveiliging, CIO Platform Nederland, september 2012; www.cio-platform.nl/publicaties
- Whitepaper Secure Software, Software Improvement Group, 2013:
  http://www.sig.eu/blobs/Whitepapers/Software_Improvement_Group_(SIG)_Secure_Software.pdf