centrum informatiebeveiliging en privacybescherming

Grip op Secure Software Development (Grip op SSD)

De methode

'Omdat "veilige software" niet vanzelfsprekend is'

November 2022 [versie 3.0 concept]

Titel	Grip op Secure Software Development (SSD)
Datum	November 2022
Versie en status	3.0 concept
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	Marcel Koers (CIP), Rob van der Veer(SIG), Michael Kuipers (Centric)
Reviewers	Domeingroep SSD van het CIP, Reviewgroep VVSG

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Voorwoord

Voor je ligt de handreiking Grip op Secure Software Development (SSD) - de methode. Deze handreiking is opgezet vanuit het perspectief van een opdrachtgever die regisseert en stuurt op beveiliging tijdens ontwikkeling van software, zonder te willen inbreken in het ontwikkelproces van interne/externe softwareleveranciers/ opdrachtnemers. Daarmee verrijkt Grip op SSD de internationaal erkende modellen voor 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.

De bestaansreden van dit document

Deze handreiking is om twee redenen geschreven.

Ten eerste is het een uitdaging om als opdrachtgever van IT-projecten sturing te geven aan het inbouwen van informatiebeveiliging bij het ontwikkelen van software. Het uitbesteden van ontwikkeling, onderhoud en beheer aan externe leveranciers maakt deze sturing complexer. Tussen opdrachtgever en opdrachtnemer zijn er dikwijls onuitgesproken verwachtingen rondom informatiebeveiliging. De opdrachtgever verwacht een deskundige opdrachtnemer die spontaan de juiste maatregelen treft. Daarentegen verwacht de opdrachtnemer 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 referenties (best practices, handboeken en methodieken) voor softwareontwikkeling van systemen geen houvast aan opdrachtgevers. In de informatiebeveiliging ligt de nadruk op lange lijsten met passende technische en organisatorische beveiligingsmaatregelen; in de IT-beheerbibliotheken ligt de nadruk op het perfectioneren van processen. Dat biedt geen praktisch toepasbare hulpmiddelen voor een opdrachtgever die kwaliteit, veiligheid en resultaat voor zijn/haar organisatie wil waarborgen.

Relevantie voor opdrachtgever/ opdrachtnemer

Voor opdrachtgevers die aan de slag gaan met Grip op SSD zijn alle hoofdstukken, met de bijlagen als naslag, relevant. Verdiepingen van onderwerpen zijn voorzien van kopteksten en kunnen zo worden overgeslagen als deze minder relevant zijn voor de lezer.

Voor opdrachtnemer (intern of extern) die willen weten wat zij van hun opdrachtgevers zouden moeten verwachten qua veilige software zijn hoofdstukken 1, 2 en met name 5 het meest relevant, met de bijlagen als naslag. Verdiepingen van onderwerpen zijn voorzien van kopteksten en kunnen zo worden overgeslagen als minder relevant voor de lezer. Nota bene: als uw opdrachtgever niet stuurt op veilige software, nodig deze er dan toe uit. Uiteindelijk is een vruchtbare samenwerking op kwaliteit ook in uw belang.

Dankbetuiging

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, SIG, Centric, Noordbeek, Capgemini, Ordina, DKTP, VVSG, ICTU en BKWI.

Amsterdam, november 2022

Leeswijzer

De handreiking is opgedeeld in 4 delen

Deel 1 behandelt de inleiding, doelstelling en definities van Grip op SSD en geeft een beknopt overzicht van Grip op SSD. Om opdrachtgevers te helpen hoe Grip te krijgen op de veiligheid van software wordt in hoofdstuk 3 een aanpak beschreven om te beginnen met Grip op SSD.

Deel 2 beschrijft in hoofdstuk 4 t/m 9 de contactmomenten tussen opdrachtnemer en opdrachtgever. Voor ieder van de contactmomenten is beschreven welke volwassenheidsniveaus er zijn.

Deel 3 gaat dieper in op processen van de opdrachtgever en is erop gericht de sturing door de opdrachtgever op de veiligheid verder te vergroten en is met name nuttig om als organisatie verder te kunnen groeien in zijn volwassenheid.

Deel 4 bevat in de vorm van bijlagen nadere informatie over Grip op SSD.

Addendum

Grip op SSD is geschreven met als doel een zo makkelijk mogelijke instap te bieden om met de methode aan de slag te gaan. Om tegemoet te komen aan de behoefte aan een verdiepingsslag op bepaalde onderwerpen, is er aan het document een bijlage D toegevoegd. In deze bijlage wordt meer informatie en referenties naar additionele documentatie geboden.

DEEL 1: Grip op SSD

1 Inleiding en doelstelling

1.1 Waarom deze methode?

Omdat "veilige software"
niet vanzelfsprekend is

Veilige software is een breed technisch gebied met veel afhankelijkheden. Daarom zijn verwachtingen tussen opdrachtgever en opdrachtnemer niet vanzelfsprekend. Wat voor de één voldoende veilige software is, is voor de ander niet veilig genoeg. Een dialoog met de opdrachtnemer is daarvoor noodzakelijk. De Grip op SSD 'methode' beschrijft hoe die gezamenlijke verantwoordelijkheid verdeeld is: eisen opstellen, communiceren, daarover in overleg gaan, opvolgen en toetsen. De doelmatigheid van de Grip op SSD samenwerking vatten we zo samen:

Duidelijke dialoog met een opdrachtnemer is nodig voor het balanceren van wensen en technische consequenties, die kunnen veranderen door voortschrijdend inzicht.

Vroege sturing en afspraken zijn goedkoper, leiden tot veiligere software en een hechtere relatie tussen opdrachtgever en opdrachtnemer.

Balans tussen "niet te veel, niet te weinig beveiliging" vraagt om een dialoog

Ervaring leert dat een gebalanceerde beveiliging alleen mogelijk is door beveiligingseisen vroeg mee te nemen in een dialoog met een opdrachtnemer in het proces van ontwerp en ontwikkeling. Te weinig beveiliging klinkt evident, maar te veel beveiliging is zeker mogelijk door een onbalans met bedrijfsrisico's. Beveiliging kan oneindig duur worden, omdat het nooit "af" is, maar hogere uitgaven staan niet per se in verhouding tot problemen die beveiliging probeert te voorkomen.

Met het zo vroeg mogelijk inbrengen en meenemen van beveiligingseisen wordt schade door incidenten voorkomen, zoals imagoschade, onderbreking van bedrijfsvoering en boetes. Het maken van deze afspraken is niet voor niets verplicht in veel securityraamwerken, waaronder de ISO/IEC 27002, de Nederlandse Baseline Informatiebeveiliging Overheid (BIO) en de Belgische Minimale normen informatieveiligheid en privacy (MNM).

Beveiliging zo vroeg mogelijk inbrengen voorkomt "reparaties"

Kwetsbaarheden laat ontdekken is pijnlijk en kostbaar. Een security-incident is het meest pijnlijk, maar een (routine) penetratietest kan ook al te laat zijn voor degelijk herstel – in het ideale geval dat de kwetsbaarheid überhaupt wordt ontdekt. In een laat stadium zijn de kosten voor het oplossen van een kwetsbaarheid vele malen groter dan de kosten om het meteen goed te doen. Bovendien is het bij dit soort 'reparaties' (de opdrachtnemer vindt het misschien een "wijzigingsverzoek") altijd de vraag wie de rekening betaalt.

1.2 Doel van de methode

Dit document presenteert een methode voor afstemming tussen opdrachtgever en opdrachtnemer als het gaat om het realiseren van veilige software, zonder daarbij de precieze invulling van de ontwikkelprocessen bij de opdrachtnemer voor te schrijven. De methode is toepasbaar bij verschillende ontwikkelmethodieken (waterval, agile) en is geschikt voor maatwerk- én standaardpakketten.

Grip op SSD gaat dus met name over de 'Grip', de controle over de veilige software ontwikkeling

(SSD), en niet over hoe die softwareontwikkeling moet plaatsvinden.

1.3 De Grip op SSD-familie van documenten

De Grip op SSD-familie bestaat naast dit document uit nog 4 documenten. Twee daarvan bevatten normen en zijn geschreven om de beveiliging concreet bespreekbaar te maken. Het Testraamwerk gaat in op hoe de normen getest kunnen worden.

De Grip op SSD-familie biedt zo handvaten om het beveiligen van applicaties praktisch mogelijk te maken.

- **Grip op SSD: De methode** – dit document over samenwerking opdrachtgever-opdrachtnemer
- **Grip op SSD: De normen** – basis technische beveiligingseisen om toe te passen in de methode bij het laten ontwikkelen van applicaties, met per aspect wie daarvoor zorg moet dragen (opdrachtgever, opdrachtnemer, of hostingpartij).
  Het normen document is relevant voor de lezers van dit document. Het geeft een startpunt voor een minimum set van technische beveiligingseisen (baseline) die direct afstembaar is met de opdrachtnemer. Hoewel de nadruk van dit normen-document ligt op webapplicaties zijn de normen grotendeels breder toepasbaar.
- **Grip op SSD: De normen voor mobiele apps** – basis technische beveiligingseisen om toe te passen in de methode, specifiek voor mobiele applicaties. De scope van dit document dekt met name "native" mobiele apps, maar de "Grip op SSD – de normen" is nog steeds relevant voor de backend (verwerkende logica en servering).
- **Grip op SSD: Testraamwerk** – over hoe de normen kunnen worden getest.
- **Grip op SSD: Agile securitymanagement** – hoe een agile ontwikkelproces kan zorgen voor het inbouwen van informatiebeveiliging. Deze is het meest relevant voor de samenwerking tussen ontwikkelaars en informatiebeveiligers.

De Grip op SSD familie is geschreven onafhankelijk van de ontwikkelmethodiek. Het werken met Agile ontwikkelteams vraagt echter om een specifieke manier van samenwerken.

Zowel de methode als de normen zijn tot stand gekomen door een intensieve samenwerking tussen opdrachtgevers, opdrachtnemers en securityspecialisten: voor de community, door de community.

De documenten zijn te vinden op cip-overheid.nl/contact.

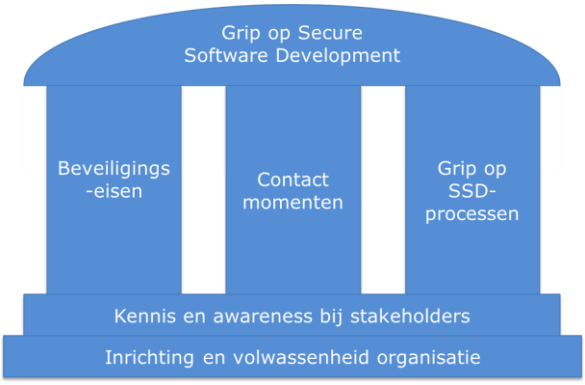
2 Overzicht Grip op SSD

2.1 Pijlers en het fundament

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

- De beveiligingseisen
- De contactmomenten
- De Grip op SSD-processen

Het fundament onder de pijlers is kennis en awareness bij de beveiligingsadviseurs, procesdeskundigen, architecten, ontwerpers en testers. De inrichting van de organisatie bij de opdrachtgever maakt onderdeel uit van dit fundament. Via een groeiproces wordt awareness/bewustzijn gecreëerd bij de stakeholders en belanghebbenden en wordt kennis en ervaring opgedaan over de te hanteren eisen en processen. Hierbij dient de opdrachtgever te toetsen/meten of de kennis en bewustzijn daadwerkelijk groeien. Voor dit meetproces zijn volwassenheidsniveaus gedefinieerd die overeenkomen met die van het Capability Maturity Model (CMM). Voor de meeste organisaties is volwassenheidsniveau 3 voor SSD afdoende.



Afbeelding 1: pijlers van de SSD-methode

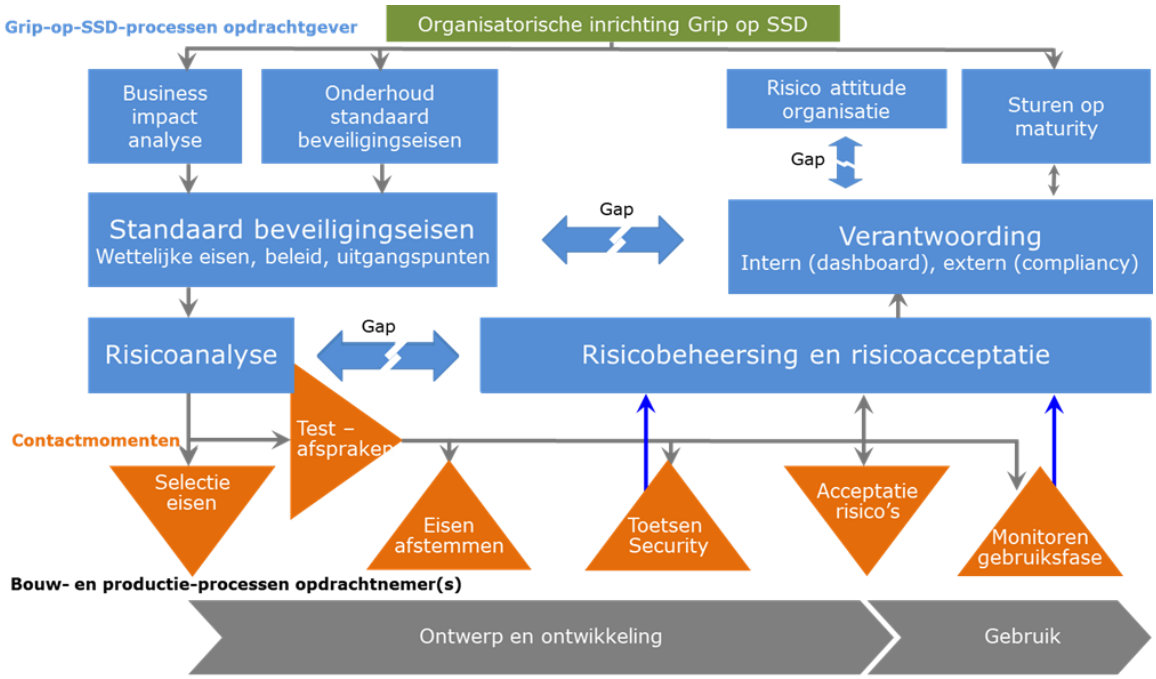
2.2 Invulling van de pijlers

De relatie van de pijlers met het ontwikkelproces is in afbeelding 2 weergegeven. Centraal daarin staan de contactmomenten. Sturing vanuit de opdrachtgever vindt daarbij plaats vanuit de Grip op SSD processen. Dit door enerzijds het zo risicogebaseerd mogelijk meegeven van beveiligingseisen en anderzijds door het zo bewust mogelijk beheersen van risico's.

De opdrachtgever geeft op basis van risico's sturing door het meegeven van beveiligingseisen (de processen links in afbeelding 2). De mate waarin dit gebeurt hangt af van de kennis en ervaring van de opdrachtgever. De sturing neemt toe als de opdrachtgever meer ervaring heeft met het maken van risicoanalyses en de organisatie beter op de hoogte is met welke standaard beveiligingseisen wel of niet van toepassing zijn. Veelal gebeurt dit door gegevens en systeem een classificatie mee te geven (zie hoofdstuk 11).

Een Business Impact Analyse (BIA) (zie hoofdstuk 12) geeft additionele informatie over hoe bedrijfskritisch een applicatie is. Een BIA wordt uitgevoerd door een opdrachtgever op een volwassenheidsniveau, waar bedrijfsbreed naar risico's wordt gekeken.

Afhankelijk van de volwassenheid van een organisatie van de opdrachtgever wordt risicomanagement (de processen rechts in afbeelding 2) meer of minder organisatiebreed uitgevoerd. Op een laag volwassenheidsniveau vindt de risicobeheersing en de risicoacceptatie per applicatie plaats, terwijl dit bij een hoger volwassenheidsniveau organisatiebreed gebeurt. Bij een bedrijfsbrede aanpak past de inzet van een dashboard en de vastlegging van de risico attitude van de organisatie (zie hoofdstuk 10).



Afbeelding 2: Grip op SSD vanuit opdrachtgever gezien

Toepassing op agile software ontwikkeling

Bij de klassieke aanpak van softwareontwikkeling ("waterval") geeft de opdrachtgever een volledig gespecificeerde opdracht aan de opdrachtnemer en ontvangt na enige tijd het complete product. Na een acceptatieproces wordt dit product daarna in productie genomen.

Voor informatiebeveiliging is deze aanpak in de praktijk niet ideaal, zeker niet in de context van web-ontwikkeling waarin korte reactietijden nodig zijn voor het oplossen van beveiligings- en gebruikersklachten.

In een ontwikkelproces volgens "agile" uitgangspunten gebeuren de taken rond ontwerp, ontwikkeling en toetsing in korte cycli. Vereenvoudigd gezien worden bijvoorbeeld ontwerpen niet systeem breed uitgewerkt voordat de eerste regel code geschreven wordt (de "klassieke" ontwikkelwijze). De contactmomenten van Grip op SSD blijven voor een agile proces in de kern gelijk. Voor 'security toetsen' mag een opdrachtgever meer tussentijdse en voorlopige resultaten verwachten. De korte cycli die bij agile horen betekenen ook dat niet elke langdurende of niet-geautomatiseerde test of toets bij elke iteratie wordt uitgevoerd.

Agile security Management

Voor agile ontwikkelprocessen is in de Grip op SSD-familie de publicatie 'Agile security management' beschikbaar, die aangeeft hoe 'shift left' kan worden georganiseerd door de opdrachtnemer en de informatiebeveiligers van de opdrachtgevers.

Wanneer een project wordt uitbesteed aan een opdrachtnemer is er tijdens agile ontwikkeling typisch sprake van een Product Owner. Als deze ook door de opdrachtnemer wordt vervuld, dan is het voor de opdrachtgever belangrijk dat de beveiligingsadviseurs als een belangrijke stakeholder op het vizier van de Product Owner blijven staan gedurende het hele

ontwikkeltraject. Ook kan gekozen worden voor een meer hybride situatie waarbij de opdrachtgever de Product Owner levert. De Product Owner kent de (eigen) organisatie goed en kan optimaal gebruik maken van de aanwezige (security) kennis en inzichten.

Automatisch en handmatig testen

Testen die automatiseerbaar zijn mogen zo vaak mogelijk in het ontwikkelproces worden uitgevoerd als dat praktisch haalbaar is. Voor handmatige testen, zoals penetratietesten en code reviews, dient een beleid te worden vast-gesteld. Bijvoorbeeld: penetratietesten bij grotere releases, peer code reviews (door het team zelf) op alle nieuwe en aangepaste code en code review door security experts afhankelijk van de ingeschatte risico's van een wijziging. Triggers hiervoor zijn o.a. architectuele wijzigingen, wijzigingen op de authenticatie en autorisatie mechanismen, cryptografische toepassingen en het toevoegen van wijzigingen van specifieke (maatwerk) beveiligingsmaatregelen.

Organisatorische eisen aan de opdrachtnemer

De Grip op SSD-methode verandert het ontwikkelproces niet, maar brengt er een uitbreiding op aan met de contactmomenten. Daarmee vereist de methode dat er een gestructureerd ontwikkelproces bestaat bij de leverancier waardoor het mogelijk is eisen in te brengen, daar gevolg aan te geven en daarop te toetsen. Hoe eerder de leverancier in het ontwikkelproces stuurt op de eisen, hoe eerder afstemming over eisen kan plaatsvinden en onnodig herstelwerk in een latere fase kan worden voorkomen. Voor dit aspect wordt ook wel de term 'shift left' gebruikt: meenemen van eisen en toetsen meer 'links' in de tijd, dus eerder in het ontwikkelproces. 'Shift-left' betekent ook dat bij het ontwerp wordt gewerkt volgens het secure-by-design principe en dat testen zo vroeg mogelijk begint; in plaats van een pentest achteraf wordt pro-actief met tooling al tijdens het ontwikkelproces getest. Tools als o.a. SAST en DAST zijn hier een goed voorbeeld van. De 'shift' is daarmee van achteraf naar vooraf en tijdens, waarbij achteraf een laatste verificatie plaatsvindt. Aangezien opdrachtgever hierbij is gebaat, kan de leverancier gevraagd worden om te onderbouwen hoe hier procesmatig aan wordt voldaan of eventueel hierop worden ge-audit. Daarnaast is het van belang om afspraken te maken om de software zelf te kunnen auditen, dus het recht op inzage van de broncode (desnoods beperkt tot onafhankelijke derde partijen) en de mogelijkheid om de software werkend te testen.

Andere onderwerpen voor organisatorische afspraken zijn volwassenheid van werkproces-sen, relevant (veiligheids)beleid en formele accreditatie (bijvoorbeeld ISO 27xxx). Daarnaast kan toetsing van betrokken personen worden geëist (certificering, integriteitstoetsen). Zie Bijlage A voor een overzicht van organisatorische eisen.

Organisatorische eisen spelen een rol bij bestaande opdrachtnemers en uiteraard ook bij selectie van nieuwe leveranciers.

Tot slot: Moderne software bestaat uit een samenstelling van componenten afkomstig van een keten van leveranciers – de software supply chain. Open source raamwerken en bibliotheken zijn een goed voorbeeld hiervan.

In de praktijk is de supply chain complex en dynamisch. Een Software Bill of Materials (SBoM) is daarbij een elektronisch document dat de onderdelen beschrijft, de keten transparant maakt en inzicht biedt in de kwetsbaarheden in de softwarecomponenten.

3 Beginnen met Grip op SSD

Grip op SSD is niet bedoeld als een 'big bang', een grote verandering ineens. Een geleidelijke groei is nodig omdat meerdere rollen binnen de organisatie betrokken zijn. De groei gaat over "samenwerken"; samen werken aan het ontwikkelen van ervaring, routines, standaard werkprocessen en de opbouw van gedocumenteerde kennis én het delen van de kennis. Het gebruik van volwassenheidsniveaus geeft de mogelijkheid om gebruik makend van de kennis in de organisatie stappen te maken naar een grotere volwassenheid van de organisatie. De volwassenheidsniveaus maken het mogelijk de volwassenheid van de organisatie te bepalen en ambitieniveaus te definiëren.

In dit hoofdstuk worden stapsgewijs tips gegeven over hoe met Grip op SSD kan worden gestart.

SSD-volwassenheidsniveaus

Op niveau 1 is veiligheid van software ad hoc ingericht. Op niveau 2 wordt meer samengewerkt in een gedeelde aanpak die in niveau 3 organisatiebreed wordt vastgesteld. Op niveau 4 is sprake van meetbaarheid inclusief vergelijking met andere organisaties. Op niveau 5 is sprake van geoptimaliseerde processen.

Om als organisatie succesvol Grip op SSD te kunnen toepassen zou idealiter een volwassenheidsniveau van 3 behaald moeten worden. Op dit niveau zijn de Grip op SSD processen gestandaardiseerd en worden ze organisatiebreed uitgevoerd, waarbij alle kennis en ervaring wordt gedeeld.

3.1 Stap 1 – Wijs een regievoerder aan om te groeien in volwassenheid.

Waar de eindverantwoordelijkheid moet worden belegd, om als organisatie grip te krijgen op de veiligheid van software, verschilt per organisatie. Deze verantwoordelijkheid moet bij voorkeur op organisatieniveau liggen en niet worden gezien als verantwoordelijkheid van een specifieke afdeling. Veelal is de aangewezen rol hiervoor de Chief Information Security Officer (CISO).

3.2 Stap 2 – Nulmeting volwassenheidsniveau (IST)

Een nulmeting betekent het vaststellen waar de organisatie nu staat. Bij het uitvoeren van de nulmeting gaat het niet om "de score", maar om te ontdekken waar verbeteringen mogelijk zijn. Zodoende start al bij de nulmeting het leren van elkaar.

Tijdens de nulmeting wordt aan de hand van de beschrijvingen van de volwassenheidsniveaus het volwassenheidsniveau van de organisatie bepaald. In feite geeft de mate van volwassenheid daarbij aan in hoeverre kennis is vastgelegd en kennis wordt gedeeld. Typisch voor organisaties is dat bij een nulmeting de volwassenheid zich beperkt tot gemiddeld niveau 1.

Bepaal in een nulmeting de volwassenheid van de organisatie in huidige situatie, ofwel de IST-situatie. Het advies is om helder te krijgen of de juiste kennis en ervaring aanwezig is en welke taken, verantwoordelijkheden en bevoegdheden al zijn belegd. Dit is mogelijk door het uitvoeren van een analyse van de volwassenheid van de organisatie en dit te doen door middel van interviews. Juist die gesprekken geven duidelijkheid over waar verantwoordelijkheden liggen en misschien nog wel belangrijker wie welke kennis en ervaring heeft in de IST-situatie.

Het (beoogde) resultaat van de interviews is antwoord krijgen op de volgende vragen:

- Hoe worden beveiligingseisen opgesteld, onderhouden, en afgestemd met opdrachtnemer;
- Hoe worden beveiligingseisen getest en getoetst;

- Hoe vindt het monitoren van beveiliging plaats tijdens de gebruiksfase;
- Hoe worden risico's geanalyseerd, inclusief DPIA, gemanaged en hoe wordt daar verantwoording over afgelegd en opvolging aan gegeven;
- Hoe worden gegevens geclassificeerd;
- Is er sprake van beveiligingsarchitectuur;
- Overzicht van de bestaande functies en hun taken en verantwoordelijkheden en hun raakvlakken met het applicatie(beveiligings) domein;
- Overzicht van hun onderlinge verhoudingen, zoals hiërarchische relaties;
- Overzicht van de taken binnen het applicatie(beveiligings) domein, de omvang van de taken en de kennis die aanwezig is;
- Overzicht welke taken aan welke functies en personen kunnen worden toegewezen en eventueel welke aanvullende functies nodig zijn (zie bijlage B over rollen). Waar nodig moeten de bevoegdheden en verantwoordelijkheden van bestaande functies worden aangepast aan de nieuwe taken;
- Inzicht in welke taken wel en niet worden uitgevoerd en of daarvoor voldoende tijd, kennis en vaardigheden aanwezig zijn.

3.3 Stap 3 – Bepaal het ambitieniveau van de organisatie (SOLL)

De nulmeting heeft de zogenaamde IST-situatie opgeleverd. Het gewenste volwassenheidsniveau, ofwel de "SOLL-situatie". De "Gap" is het verschil tussen beiden. Inzicht in de IST-situatie geeft ook beeld van de effort die nodig is om een bepaalde ambitie waar te kunnen maken. Als de Gap tussen IST en SOLL groot is zijn één of meerdere tussenstappen nodig. Door het uitspreken en op organisatieniveau vastleggen van het ambitieniveau in de Grip op SSD volwassenheid (de SOLL-situatie) wordt een groeipad uitvoerbaar en haalbaar.

De IST, SOLL en de Gap kunnen worden opgenomen in een informatiebeveiligingsplan en de initiatieven/projecten daarvoor. Indien de Gap te groot is om op afzienbare termijn te dichten, is het advies het beoogde doel naar beneden bij te stellen. Per project(stap) kan het volgende SOLL worden bepaald. Zo kan de organisatie stapsgewijs groeien naar een volwassen organisatie. Het typisch te ambiëren volwassenheidsniveau ligt voor kleine organisaties op 2, voor middelgrote organisaties op 3 en voor grotere organisaties op 4.

3.4 Stap 4 – Voer een pilot uit

Start de kennismaking met Grip op SSD met een pilot voor één systeem. Selecteer hiervoor een belangrijk systeem zodat meteen waarde voor de organisatie wordt gecreëerd. Bij meerdere opdrachtnemers: prefereer degene waar al zoveel mogelijk sprake is van wederzijds vertrouwen zodat de kans op complicaties door de relatie bij de pilot minimaal is. Een systeem waar de tijdslijnen kort zijn is niet ideaal, omdat ervaring opdoen met Grip op SSD de eerste keer meer tijd kost.

Eénmaal geselecteerd: ga voor dit systeem aan de slag met de handreikingen om inhoud te geven aan de contactmomenten (zie de volgende hoofdstukken).

Kijk tijdens de pilot of binnen de organisatie de juiste personen gekoppeld zijn aan de taken voor SSD. Zeker in grotere organisaties moeten zij voldoende mandaat (besliskracht) hebben. De volgende rollen vormen daarbij het minimum:

- Een sturende rol richting opdrachtnemer (bijvoorbeeld projectmanager, systeemeigenaar, inkoopfunctionaris);
- Het "technisch geweten" die consistentie en haalbaarheid inschat (systeemarchitect, beveiligingsadviseur);
- Sturende rollen intern (management rond sturen van werkprocessen, richting geven op organisatieniveau, beheren van interne documenten/producten).

3.5 Stap 5 – Stel samen het plan van aanpak op en voer dit uit.

Stel met behulp van de nulmeting en het ambitieniveau een plan van aanpak op.

Een belangrijk onderdeel van het plan is het duidelijk beleggen van de verschillende rollen. Door de Taken, Verantwoordelijkheden en Bevoegdheden (TVB) aan te laten sluiten op de ambitie van de organisatie kunnen de in de TVB vastgelegde taken, verantwoordelijkheden en bevoegdheden meegroeien met de groei in volwassenheid van de organisatie. Zo voorkom je dat taken en verantwoordelijkheden neergelegd worden bij organisatieonderdelen die daar niet de kennis en expertise voor hebben. De in bijlage B beschreven SSD-rollen helpen de TVB's af te stemmen op de behoefte van de organisatie (IST door te laten groeien naar de SOLL situatie).

Tijdens uitvoer van het plan is het belangrijk om op de mijlpalen te evalueren. Het steeds verder vergroten van de samenwerking is essentieel om alle applicaties binnen de organisatie veilig te maken. Er zijn 2 manieren om te bepalen of de organisatie grip op SSD heeft (zie hoofdstuk 10):

1. Het sturen op compliance:
   Compliance geeft aan in welke mate een opdrachtgever, of beter gezegd de interne opdrachtgevers, en de opdrachtnemers zich aan de gestelde beveiligingseisen houdt. Hiertoe wordt een dashboard bijgehouden en vindt sturing plaats op basis van het ontbreken van compliance en de onderlinge verschillen.

2. Het sturen op volwassenheid:
   Sturing op volwassenheid is een continu proces om de samenwerking binnen de organisatie van de opdrachtgever verder te vergroten.

DEEL 2: SSD contactmomenten

4 Opstellen van beveiligingseisen

De beveiligingseisen zijn een belangrijke kennisbron binnen Grip op SSD. Ze dienen om te voorkomen dat bij elk project weer opnieuw alles over beveiliging moet worden bedacht. Ze vormen de basis voor het samenstellen van de juiste specifieke beveiligingseisen per situatie.

Een beveiligingseis kan bijvoorbeeld zijn dat twee-factor authenticatie verplicht is voor toegang tot een portaal waar klantgegevens inzichtelijk zijn. De "tweede factor" is (naast het kenniskenmerk, in dit geval een wachtwoord) doorgaans een bezitskenmerk. Je kunt hierbij onder andere denken aan hardware tokens of een authenticator app.

4.1 Belangrijk onderscheid functionele en non-functionele eisen

Het is belangrijk om het onderscheid te kennen tussen functionele eisen en non-functionele eisen. Een functionele beveiligingseis gaat over wat het systeem voor de gebruiker moet doen - bijvoorbeeld twee-factor authenticatie. Deze wordt typisch als functionele specificatie opgenomen en bijvoorbeeld in een agile ontwikkelproces tot een user story vertaald. Een non-functionele beveiligingseis definieert niet een gebruikersfunctie maar de kwaliteit van de implementatie – bijvoorbeeld dat gegevens die getoond worden op een website worden geschoond van eventuele ongewenste code. Deze eisen vinden hun weg als criteria voor het ontwikkelwerk – die bijvoorbeeld in een agile ontwikkelproces worden getoetst via de "definition of done" of acceptatiecriteria van "user stories".

4.2 Standaard beveiligingseisen

De baseline security beschrijft een set relevante standaardeisen die een "minimaal niveau van beveiliging" vertegenwoordigen. De baseline security wordt afgestemd met de opdrachtnemer bij wijze van verificatie, bijvoorbeeld door te toetsen "Is deze set van normen haalbaar? Zijn er problemen voorzien om deze te realiseren?".

Een overzichtelijke lijst van standaardeisen is te vinden in het werk "Grip op SSD – de normen" op https://www.cip-overheid.nl/. Zie bijlage C voor een beknopt overzicht. Naast deze lijst bestaat ook een versie van deze normen specifiek voor mobiele applicaties.

Overige bronnen van beveiligingseisen zijn[1]:

- ISO/IEC 27002:2017, welke met name documentatie- en procescontroles beschrijven.
- BIO: https://bio-overheid.nl/category/producten#BIO
  De Baseline Informatiebeveiliging Overheid (BIO) is een best practice voor overheden en is afgeleid van de ISO 27002:2017 en bevat een 30-tal aandachtspunten met een 180-tal beveiligingsmaatregelen. De maatregelen die in de BIO zijn genoemd gelden als verplicht voor alle Nederlandse overheidsorganisaties en aan de overheid gelieerde organisaties. De BIO vereist de beheersmaatregelen, zoals vermeld in de Bijlage A van de ISO 27001 en uitgewerkt in de ISO 27002 en niet het management-systeem voor informatiebeveiliging (ISMS), zoals de ISO 27001 dat wel doet.
- OWASP Application Security Verification Standard (ASVS):

[1] Daar waar referenties gegeven worden, zijn deze ter illustratie en vormen zeker geen uitputtende lijst.

De OWASP ASVS biedt een basis om de beveiligingsmaatregelen van (web)applicaties te testen. De ASVS eisen zijn door hij technische inhoud met name gericht op ontwikkelaars, terwijl de SSD-normen zijn opgesteld om ook gebruikt te worden door opdrachtgevers.

- Een overzicht van eisen en hoe ze binnen OWASP, NIST en Mitre worden beschreven is te vinden op https://www.opencre.org/
- Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens, van de Gegevensbeschermingsautoriteit (België): https://www.gegevensbeschermingsautoriteit.be/professioneel/thema-s/informatieveiligheid
- Minimale normen informatieveiligheid en privacy, van de KSZ (België): https://www.ksz-bcss.fgov.be/nl/gegevensbescherming/informatieveiligheidsbeleid

4.3 Afstemming beveiligingseisen op beveiligingsarchitectuur

In de context van Grip op SSD betreft de beveiligingsarchitectuur een beschrijving van de al bestaande technische beveiligingsmaatregelen. Meestal zijn dit specifieke groepen componenten in de infrastructuur. Dergelijke componenten voorkomen dat bedrijfsbrede beveiligingsmaatregelen versnipperd worden ingericht en beheerd. Voorbeelden hiervan zijn een centraal mechanisme voor toegangscontrole, zoals Active Directory voor IAM, de netwerkcomponenten en diverse vormen van middleware en platformen.

De risico's die al zijn afgedekt met standaard beveiligingsmaatregelen hoeven dus niet nogmaals te worden afgedekt in de te bouwen applicatie. Wel maken ze onderdeel uit van de beveiligingseisen, omdat anders niet controleerbaar is of ze juist zijn toegepast.

In ketenverband kunnen sommige van de componenten ook buiten de eigen organisatie liggen, zoals de voorzieningen voor digitale identiteit (zoals DigID of eID).

4.4 Relatie dataclassificatie en beveiligingseisen

De classificatie van systemen en gegevens (zie hoofdstuk 11) kan resulteren in inzichten waarmee bepaalde standaardeisen kunnen vervallen en eventueel nieuwe standaardeisen worden toegevoegd, afhankelijk van de specifieke situatie. Voorbeeld: een strengere eis om direct uit te loggen zodra een gebruikerstransactie klaar is bij een applicatie die werkt met zeer vertrouwelijke gegevens.

De beveiligingsarchitectuur documenteert de beschikbare technische faciliteiten voor de organisatie. Deze dient up-to-date te worden gehouden en regelmatig worden gecontroleerd of deze marktconform is en aansluit bij eventuele ketenpartners. Mogelijk kunnen bepaalde faciliteiten worden gedeeld met andere organisaties.

4.5 Toepassing op bestaande systemen en standaardpakketten

Voor bestaande systemen en standaardpakketten geldt dat er per definitie geen ruimte is om eisen voorafgaand en tijdens de ontwikkeling te communiceren. Daarnaast zijn de mogelijkheden voor testing (bijvoorbeeld automatische testrapporten of code review) bij standaardpakketten typisch beperkt. Als bestaande systemen of standaardpakketten in een laat stadium niet blijken te voldoen aan bepaalde eisen dan kan de opdrachtnemer typisch niet verantwoordelijk worden gehouden. In zo'n situatie is het mogelijk dat de inspanningen om de software veilig te krijgen zo groot zijn, dat andere maatregelen moeten worden verkozen zoals strengere monitoring. Het toepassen van Grip op SSD is nodig voor bestaande systemen en standaardpakketten, met de volgende doelstellingen:

- Adressering van de eisen met opdrachtnemer - Het communiceren van en afstemmen over eisen maakt in elk geval bespreekbaar wat beide partijen doen als aan verwachtingen niet volledig voldaan wordt. Een mogelijk gevolg is het herzien van (eventueel contractuele) afspraken in de huidige samenwerking voor nieuw ontwikkelwerk. Eventueel meerwerk kan dan in kaart worden gebracht en worden geprioriteerd met de opdrachtgever. Risico's door eisen waar niet aan kan worden voldaan, kunnen mogelijk met andere tegenmaatregelen worden gecontroleerd – technisch of organisatorisch, zoals bijvoorbeeld het inregelen van meer strikte monitoring (operationeel volgen van systeemgedrag).
- Interne adressering van de eisen - Een deel van de eisen kan betrekking hebben op zaken die onder regie van de eigen organisatie vallen, zoals bepaalde onderdelen van de infrastructuur en het beheer.
- Selectie van standaardpakketten - Als een bestaand systeem aangeschaft moet worden, dan kan Grip op SSD ondersteunen bij de keuze. Dit betreft het inbrengen, afstemmen en toetsen van en bespreking van wat de opdrachtnemer wil en kan doen met afwijkingen.

4.6 SSD volwassenheidsniveaus voor opstellen beveiligingseisen

U.01 Het opstellen van de beveiligingseisen	
De organisatie stelt beveiligingseisen op	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	(Standaard) normenkaders met beveiligingseisen, zoals bijvoorbeeld de SSD-beveiligingseisen, gelden als beveiligingseis.
2. Beheerst proces (managed process)	De beveiligingseisen zijn specifiek gemaakt door het uitvoeren van een risicoanalyse, inclusief een DPIA, op een wijze die op afdelingsniveau is vastgelegd. • De risicoanalyse leidt tot de specifiek voor de applicatie geldende beveiligingseisen. • Er wordt gebruik gemaakt van een beeld van de beveiligingsinrichting van de productie-omgeving.

U.01 Het opstellen van de beveiligingseisen	
3. Vastgesteld proces (established process)	De beveiligingseisen zijn specifiek gemaakt door het uitvoeren van een risicoanalyse, inclusief een DPIA, op een wijze die op organisatieniveau is vastgelegd en vastgesteld. • De risicoanalyse leidt samen met de DPIA tot de specifiek voor de applicatie geldende beveiligingseisen. Hierbij is de organisatiebreed vastgelegde kennis en ervaring meegenomen. • De beveiligingsarchitectuur van de productie-omgeving met de beveiligingsmaatregelen, waarmee de opdrachtgever en opdrachtnemer bepalen welke eisen passend zijn en welke eisen aanvullend nodig zijn, is als onderdeel van de standaard beveiligingseisen vastgelegd en door opdrachtgever en opdrachtnemer vastgesteld. • Een classificatie model van systemen en gegevens met per classificatie de te nemen maatregelen versnelt dit proces. • Voor ieder systeem is een BIA uitgevoerd.
4. Voorspelbaar proces (predictable process)	In een cyclisch kwaliteitsmanagementproces wordt het passend zijn van de beveiligingseisen getoetst en daar waar nodig wordt de beveiligingseis verbeterd. De samenhang tussen risico's en de daarvoor passende maatregelen liggen vast en is beschikbaar in de vorm van best practices. • Ook bij standaardpakketten zijn de eisen geadresseerd en worden er mitigerende maatregelen genomen. • De standaard beveiligingseisen worden aangepast als er nieuwe vormen van aanvallen worden gesignaleerd of als betere technieken voor beveiliging beschikbaar komen. • Bij een aanpassing van configuratie of een nieuwe kwetsbaarheid wordt een inschatting gemaakt van de mogelijke gevolgen. • De resultaten van de uitgevoerde BIA's zijn opgenomen als onderdeel van het Business Continuity Plan (BCP).

U.01 Het opstellen van de beveiligingseisen	
5. Geoptimali-seerd proces (optimized process)	In een cyclisch kwaliteitsmanagementproces wordt het passend zijn van de beveiligingseisen en de best practices continu getest en daar waar nodig verbeterd. • Het management van de organisatie heeft het BCP goedgekeurd. • De aanpak hoe de veiligheid te verbeteren sluit aan op de bedrijfsstrategie en maakt onderdeel uit van de bedrijfsuitingen.

5 Afstemmen beveiligingseisen met opdrachtnemer

5.1 Selectie eisen en voorleggen aan opdrachtnemer

De beveiligingseisen voor een specifiek systeem bestaan uit:

1. De baseline security (zie 4.2);
2. De vereisten volgens de classificatie (zie hoofdstuk 11) van betrokken gegevens en andere systemen (specifieke maatregelen die passen bij een classificatie van data, bijvoorbeeld het type versleuteling of toegangscontrole voor een bepaalde brongegevens). De bijbehorende onderbouwing van het belang om die gegevens en systemen te beveiligen (zoals een risicoanalyse) kan de opdrachtnemer helpen mee te denken over een optimale aanpak;
3. Eventueel additionele eisen die voortkomen uit een risicoanalyse voor het systeem (zie paragraaf 8.3);
4. Eventuele aanwezige beveiligingsarchitectuur om te gebruiken of mee rekening te houden.

Het is belangrijk om de opdrachtnemer(s) vóór de contractering te informeren over de inhoud van de eisen. Bij hun prijsstelling kunnen zij daar rekening mee houden. Ook kunnen opdrachtnemers vaak waardevolle aanvullingen of feedback geven op beveiligingseisen, die de kwaliteit en effectiviteit van de eisen kunnen verbeteren. Vaak hanteren opdrachtnemers zelf beveiligingseisen die zij dan kunnen vergelijken met de gestelde eisen. Deze vergelijking kan nuttige informatie zijn voor het vertrouwen van de opdrachtgever. Het opstellen van beveiligingseisen gebeurt doorgaans voorafgaand per project of deelproject. Deze eisen worden typisch meegenomen in een Project Start Architectuur (PSA) of in het Functioneel Ontwerp (FO). Bij een aanbesteding worden de eisen opgenomen in het Programma van Eisen (PvE). Belangrijk is dat de eisen niet eenmalig worden besproken, maar dat afspraken worden gemaakt over het blijven afstemmen van de eisen.

5.2 Blijf eisen afstemmen met opdrachtnemer

Eisen worden typisch gesteld in de vorm van comply or explain (pas toe of leg uit): het kan zijn dat door technisch voortschrijdend inzicht tijdens ontwerp en ontwikkeling duidelijk wordt dat een eis onevenredig veel werk met zich meebrengt, of onevenredige nadelen brengt, zoals bijzonder ongemak voor gebruikers. Ook kan blijken dat het achterliggende risico op een betere manier kan worden afgedekt. Dit vereist wederzijdse afstemming.

Als de opdrachtnemer niet wil of kan voldoen aan een bepaalde eis, moet de opdrachtgever een proces voor risicoacceptatie doorlopen, met de afwegingen van de opdrachtnemer als input.

5.3 SSD volwassenheidsniveaus voor afstemmen beveiligingseisen

U.03 Het afstemmen over de beveiligingseisen
De opdrachtgever en de opdrachtnemer dragen zorg voor dat de eisen passend zijn en er niet te weinig of juist teveel eisen worden gesteld.

U.03 Het afstemmen over de beveiligingseisen	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	Door de opdrachtgevers en opdrachtnemer is afgestemd aan welke van de SSD-eisen de applicatie moet voldoet.
2. Beheerst proces (managed process)	De opdrachtgevers en opdrachtnemer stemmen af welke SSD-eisen voor welke interface gelden. • Het is duidelijk welke beveiligingseisen meer of minder relevant zijn. • De resultaten zijn op afdelingsniveau vastgelegd, zodat duidelijk is waarop moet worden getest. • Het waarom van de gemaakte keuzen wordt vastgelegd in een risico-maatregel overzicht, zodat hergebruik van de opgedane kennis en ervaring mogelijk is.
3. Vastgesteld proces (established process)	De opdrachtgevers en opdrachtnemer stemmen af welke eisen voor welke interfaces gelden en hoe deze passend zijn binnen de geldende beveiligingsarchitectuur. • De resultaten zijn vastgelegd en op organisatieniveau vastgesteld, zodat formeel duidelijk is waarop kan worden getoetst, zodat duidelijk is hoe bij het contactmoment “het accepteren van risico’s” omgegaan moet worden met de acceptatie. • Het waarom van de gemaakte keuzen wordt in een organisatiebreed beschikbaar risico-maatregel overzicht vastgelegd en vastgesteld. Het overzicht versnelt organisatiebreed het maken van de keuzen. • Organisatiebreed werkende beveiligingsadviseurs ondersteunen de afstemming, waarbij per eis bekend is welk werk nodig is om wel aan de eis te voldoen en welke nadelen de eis brengt, zoals de gevolgen voor het gebruiksgemak. • Het is duidelijk wat de rol van de verschillende vormen van testen is, zoals code reviews, pentests en audits.

U.03 Het afstemmen over de beveiligingseisen	
4. Voorspelbaar proces (predictable process)	Er wordt naast de SSD-eisen ook gekeken naar andere normenkaders voor beveiligingseisen, waaraan voldaan moet worden. • De eisen zijn voor iedere applicatie en per interface duidelijk. • Door het benutten van de kennis van de opdrachtnemer en van andere partijen is er een samenspel tussen opdrachtgever en opdrachtnemer bij de afweging van risico's. Er is een 'shift left' beweging, waarbij het vaststellen van beveiligingseisen en afstemmen ervan zodanig plaatsvindt dat deze zo vroeg mogelijk en in alle fasen van het ontwikkelproces worden meegenomen, waarbij er continue gekeken wordt of de beveiligingseisen (nog) voldoen of dat er additionele of maatregelen moeten worden genomen.
5. Geoptimali-seerd proces (optimized process)	De 'shift left' beweging vindt zodanig plaats dat er een optimum is gevonden in de continu afstemmen van beveiligingseisen, het testen en het gebruik van tooling hiervoor. Onvolkomenheden die zich tijdens de gebruiksfase voordoen en nieuwe eisen worden volgens een voorafgaand vastgelegde procedure afgehandeld.

6 Afstemmen over testen en SLA

6.1 Maak testafspraken met opdrachtnemer

De testafspraken gaan over hoe vastgesteld gaat worden dat het systeem voldoet aan de beveiligingseisen. Daarbij wordt niet alleen gekeken naar de test voor acceptatie, maar naar tests in de gehele ontwikkel- en gebruiksfase. Bij korte ontwikkelfases ('sprints') is het gebruikelijk dat er frequent testresultaten beschikbaar zijn.

"Acceptatie" is hier breed bedoeld, inclusief het accepteren van niet-functionele eisen, dus niet alleen functionele acceptatie (typisch bekend als FAT).

Een voorbeeld van testafspraken is dat de opdrachtnemer tijdens het ontwikkelproces gebruik maakt van bepaalde statische code analyseprogramma's en inzage verschaft in de resultaten daarvan. Een ander voorbeeld is dat voor de oplevering nog een codereview wordt uitgevoerd door een externe partij en een pentest door de opdrachtgever.

Opdrachtgever en opdrachtnemer spreken af welke testaanpak wordt toegepast en welke testresultaten naar de opdrachtgever worden gecommuniceerd en hoe. Zo is het bijvoorbeeld mogelijk af te spreken dat een opdrachtgever aanwezig is bij bepaalde sessies van de opdrachtnemer waar functionele en niet-functionele testing wordt besproken, zoals een demosessie in scrum agile.

Bij het maken van testafspraken spreekt het voor zich dat niet alleen naar functionaliteit en security wordt gekeken, maar ook naar andere kwaliteitsaspecten zoals privacy, betrouwbaarheid en performance.

6.2 SSD volwassenheidsniveaus test- en SLA afspraken

U.02 Het maken van test- en SLA-afspraken	
De organisatie maakt Grip op SSD onderdeel van de contractering van IT-diensten.	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	Er is (minimaal) afgesproken dat de applicatie aan (standaard) normenkaders, inclusief de SSD-beveiligingseisen, moet voldoen.

U.02 Het maken van test- en SLA-afspraken	
2. Beheerst proces (managed process)	Contractueel is vastgelegd dat de applicatie aan beveiligingseisen moet voldoen en hoe invulling wordt gegeven aan de samenwerking. • Alleen (minstens) op SSD geteste applicaties worden in productie (gebruik) genomen. • Beschreven is hoe met geconstateerde afwijkingen moet worden omgegaan, er bestaat echter nog interpretatievrijheid, waardoor de toepassing op uitvoeringsniveau kan verschillen. • Het is duidelijk hoe het afhandelen van de incidenten moet plaatsvinden. • Het is duidelijk hoe de 'shift left' beweging wordt georganiseerd.
3. Vastgesteld proces (established process)	De contractuele afspraken over het testen gelden niet alleen ten aanzien van het in gebruik nemen, maar voor de gehele ontwikkel- en gebruiksfase, inclusief afspraken over het monitoren van de applicatie. • De afspraken worden organisatiebreed eenduidig toegepast. • De afspraken over de samenwerking waarborgen dat blijvend aan passende veiligheidseisen wordt voldaan. • De procesafspraken en de rollen van de partijen zijn in een TVB vastgelegd en gebaseerd op een visie en een vastgesteld beveiligingsbeleid. • De middelen en menskracht zijn beschikbaar gesteld.
4. Voorspelbaar proces (predictable process)	De opdrachtnemer is op de hoogte van de inhoud van de standaard beveiligingseisen waaruit de specifieke beveiligingseisen voortvloeien. • Vastgelegd is hoe de opdrachtnemer aanvullingen of feedback geeft op de inhoud van de standaard beveiligingseisen. De samenwerking tussen opdrachtgever en opdrachtnemer bij het testen en monitoren is zodanig dat deze effectief (tegen vastgelegde en overeengekomen passende testeisen) en efficiënt (zonder onnodige dubbelingen) verloopt. Bij de aanschaf van bestaande - of standaardpakketten worden afspraken gemaakt hoe aan de beveiligingseisen op basis van de geldende en toekomstige beveiligingseisen wordt voldaan.

U.02 Het maken van test- en SLA-afspraken	
5. Geoptimali-seerd proces (optimized process)	Het in gebruik nemen, testen en monitoren is vergaand geautomatiseerd en vormt een integrale keten tussen opdrachtgever, opdrachtnemer (als ontwikkelende partij) en (opdrachtnemer als) hostingpartij. De opdracht-gever heeft de aanpak vastgelegd in hun standaard contract.

7 Security testen en toetsen

Grip op SSD hanteert de termen testen èn toetsen. Voor de acceptatie van de software door de opdrachtgever zijn testen noodzakelijk. Er kan bij de acceptatie ook uitgegaan worden van de uitgevoerde testen in het ontwikkeltraject. In dat geval hoeft de opdrachtgever alleen te toetsen of de testen met een gewenst resultaat zijn uitgevoerd, bijvoorbeeld door te toetsen of de resultaten van de testen in de "definition of done" staat.

7.1 (Laat) security testen

Het contactmoment Security testen heeft als doel voor de opdrachtgever om vertrouwen te krijgen dat de software aan de beveiligingseisen voldoet – zo veel mogelijk al tijdens realisatie in plaats van alleen bij acceptatie. Dit kan de opdrachtgever doen door het (laten) beoordelen van testresultaten van de opdrachtnemer, door het zelf uitvoeren van tests, of door het laten uitvoeren daarvan. Daarnaast kan worden gekozen voor een audit van het ontwikkelproces op de gestelde organisatorische eisen.

Eventuele afwijkingen/bevindingen uit een securitytest worden vastgelegd in een afwijkingsrapportage (exception report) en vervolgens gemitigeerd of meegenomen in de risicoacceptatie.

7.2 Soorten testen

Beveiligingseisen kunnen op verschillende manieren worden getest. Ruwweg zijn dit zes manieren:

1. **Met een automatische statische test (ook wel SAST)** die broncode en configuratie scant naar mogelijke zwakheden, te vergelijken met een spelling/grammatica-checker: bepaalde soorten fouten kunnen goed worden gevonden, maar deze aanpak kan niet de precieze werking doorgronden.
2. **Met een automatische dynamische test (ook wel DAST)** die naar typische openingen of kwetsbaarheden zoekt door het gebruiken van een werkend systeem. Deze manier van testen kan een beperkt deel van de kwetsbaarheden vinden, waaronder configuratiefouten. Omdat dit soort scans goed herhaalbaar zijn, zijn ze vaak deel van een overeenkomst om periodiek uit te voeren.
3. **Met een handmatige securitytest (ook wel penetratietest of pentest)** waarbij een werkend systeem op de proef wordt gesteld. Het werkende systeem is typisch een zodanige kopie van de productieomgeving dat de onderliggende infrastructuur, de maatregelen en de configuratie ervan identiek zijn.

   Door samenwerking opdrachtgever en opdrachtnemer, inclusief het met elkaar delen van informatie, worden mogelijke beveiligingsrisico's onderzocht en wordt er gekomen tot scherpere/betere beveiligingsmaatregelen.
4. **Met een code/design review** waarin specialisten, maar bij voorkeur eerder ook al collega-ontwikkelaars, zoeken naar kwetsbaarheden in code, ontwerp, configuratie en documentatie, door de precieze werking te doorgronden met ondersteuning van analysetools. Vaak gaat dit samen met een architectuur-review, waarbij het technische ontwerp van de software en operatie (logische en deployment architectuur) worden nagelopen op gepaste beveiliging. Een architectuurreview kan ook los worden uitgevoerd als "eerste stap", maar geeft op zichzelf beperkte garanties.
5. **Met open source versiecontrole (ook wel SCA)** waarmee gekeken wordt naar gebruikte open source componenten voor onder meer eventuele bekende kwetsbaarheden, nieuwere versies, licentie-

issues. De SBoM maakt hiertoe de gebruikte software componenten inzichtelijk, inclusief de daarvan bekende kwetsbaarheden.

6. **Procesanalyse/consistentie systeeminrichting met bedrijfsprocessen** waarin gekeken wordt of het ontwerp en de operatie van een systeem in lijn zijn met verwachtingen en taken van externe medewerkers en tooling. Hiermee worden mogelijke knelpunten in de opvolging bij problemen geïdentificeerd. Bijvoorbeeld: worden logs geanalyseerd in geval van afwijking/is deze verantwoordelijkheid belegd? Zijn er escalatieprocessen in geval van uitzonderingen/fouten/incidenten? Zijn hiervoor taken en verantwoordelijkheden afgesproken? Is er tooling ingericht die logs kan filteren of ongewenste situaties kan herkennen met hulp van heuristieken?

Red team/blue team constructies worden soms gebruikt in grotere organisaties om aanvals- en verdedigingsteams te laten concurreren met elkaar.

7.3 Verschillen pentest en code review

Over het algemeen vullen penetratietests en code reviews elkaar aan, omdat ze verschillende dingen beoordelen. Vereenvoudigd gezien zijn de belangrijke verschillen tussen een code/design review en een pentest:

- Een pentest zorgt voor inzichten in kwetsbaarheden door een werkend systeem te benaderen. Daarom heeft een pentest eerst werkende software nodig. Bevindingen uit een pentestresultaat hebben veel zeggingskracht, omdat misbruik is gedemonstreerd. Het is niet altijd duidelijk waarom een kwetsbaarheid bestaat, dat vraagt soms extra onderzoek;
- Een code review kan naast kwetsbaarheden ook zwakheden vinden. Dat zijn potentiele kwetsbaarheden die een risico vormen. Bijvoorbeeld: wachtwoorden worden niet versleuteld opgeslagen, of mislukte inlogpogingen worden niet gelogd. Code review kan worden toegepast in elke fase van de ontwikkeling. In een code review is bij een bevinding duidelijk waar de oorzaak zit.

Voor inzicht in verschillende vormen van testen, zie het ‘Whitepaper securitytesten’ van het NCSC.

7.4 Verschillende typen pentests

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. Black box testen zijn minder effectief voor grote, complexe systemen. Tevens wordt met een blackbox test veel tijd gespendeerd aan het achterhalen van informatie die anders eenvoudig had kunnen worden gedeeld.
- 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. Deze vorm leidt typisch tot meer bevindingen;
- White box testing of crystal box testing: hierbij probeert een specialist de software aan te vallen, gebruik makend van diepgaand inzicht in de applicatiecode en de onderliggende infrastructuur. Deze vorm geeft typisch het meest diepgaande resultaat. Het is echter geen code review.

7.5 SSD volwassenheidsniveaus voor Security testen en toetsen

U.04 Het testen en toetsen	
De opdrachtgever en de opdrachtnemer voeren testen uit en bepalen zo of de applicatie aan de eisen voldoet.	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	Door zowel de opdrachtnemer als de interne opdrachtgevers worden onafhankelijk van elkaar respectievelijk tijdens het ontwikkelproces en bij de acceptatie testen uitgevoerd.
2. Beheerst proces (managed process)	In een op afdelingsniveau vastgelegde gezamenlijke aanpak tussen de opdrachtnemer en de interne opdrachtgevers worden gegevens over de testen tijdens het ontwikkelproces, de acceptatie en de gebruiksfase gedeeld. • De resultaten van deze testen kunnen gebruikt worden bij de acceptatie van de software, zodat de opdrachtgever die testresultaten alleen nog hoeft te toetsen. • De testvormen, zoals code reviews, pentests en audits worden passend ingezet.
3. Vastgesteld proces (established process)	De vastgelegde en op organisatieniveau vastgestelde gezamenlijke aanpak voor het testen tijdens het ontwikkelproces, de acceptatie en de gebruiksfase wordt door alle interne opdrachtgevers op een passende wijze gebruikt. • Alle voor de acceptatie benodigde resultaten van het testen tijdens het ontwikkelproces worden beschikbaar gesteld voor het contactmoment “Het accepteren van risico’s”, zodat de opdrachtgever die testresultaten alleen nog hoeft te toetsen en zelf niet of slechts beperkt hoeft te testen. • De testvormen, zoals code reviews, pentests en audits, worden op basis van vooraf beschreven en vastgestelde scenario’s passend ingezet.

U.04 Het testen en toetsen	
4. Voorspelbaar proces (predictable process)	Het gebruik van geautomatiseerd testen is beschreven. In het (agile) ontwikkelproces zijn de onderdelen ontwerp, ontwikkeling, de gebruiksfase en testen geïntegreerd. • Al gedurende de ontwikkeling is er grote zekerheid dat bij de acceptatie en tijdens de gebruiksfase geen nieuwe afwijkingen worden geconstateerd.
5. Geoptimali-seerd proces (optimized process)	Het testen ondersteunt optimaal de ‘shift left’ beweging. • Voor alle software, inclusief die van bestaande systemen, geldt dat al gedurende de ontwikkeling grote zekerheid is dat bij de acceptatie en tijdens de gebruiksfase geen afwijkingen worden geconstateerd op basis van de bij de acceptatie geldende eisen.

8 Beheersen van risico's

Een risicoanalyse beantwoordt voor een specifieke context (bijvoorbeeld een systeem) de vraag "welke risico's zien we en wat kunnen we ertegen doen"? Het doel is om daarmee specifieke beveiligingseisen op te stellen die horen bij de risico's; het Contactmoment 'Opstellen eisen' (Zie hoofdstuk 4). De bedachte combinaties risico-maatregel worden centraal bijgehouden in het risico-maatregel overzicht (zie 8.4). Dit overzicht kan goed worden hergebruikt in volgende risicoanalyses.

Een risicoanalyse heeft altijd een beperking in scope (toepassingsgebied) en dat zijn in de meeste gevallen de functionele grenzen die bij een bedrijfsproces passen. Dat kan één systeem zijn met één functie (bijvoorbeeld een portaal/website) of het kan deel zijn van een verzameling of keten van systemen (bijvoorbeeld een systeem inclusief specifieke data-opslag, externe koppelingen/APIs of hulpscripts (losse stukken code met specifieke functie).

Wanneer het nodig is, kan een gegevensbeschermingseffectbeoordeling (DPIA) worden uitgevoerd in het kader van de Algemene Verordening Gegevensbescherming (AVG/ GDPR). Deze is vergelijkbaar met de risicoanalyse. In een DPIA wordt onderscheid gemaakt in de classificatie van type gegevens (data zoals intern administratief, financieel, persoonlijk identificerend, publieke data).

8.1 Risk appetite

Beveiligingseisen en risico-acceptatie sluiten in de ideale situatie aan bij de risicoattitude van de organisatie en geven de strategische doelstellingen van de organisatie hier duidelijkheid over, bij het beschrijven van de bedrijfswaarden. Tevens zal de risicoattitude moeten aansluiten op 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.

8.2 Stel risicoanalyse op en onderhoud deze

Een risicoanalyse is een levend document (wordt bijgewerkt bij nieuwe inzichten) en helpt besluitvorming in risicomanagement. Verantwoordelijken in een organisatie kunnen met een risicoanalyse expliciet kiezen of een risico geaccepteerd wordt of niet, en bijvoorbeeld hoeveel budget er beschikbaar mag komen voor maatregelen.

Risicoanalyse kent typisch de volgende stappen:

1. Vaststellen van de scope voor de risicoanalyse: welke informatiesystemen, gegevensverzamelingen en andere bedrijfsmiddelen, en de context. Dit bepaalt ook hierbij de zakelijke en juridische kaders en andere relevante gegevens uit de classificering;

2. Dreigingsmodellering: identificeren van dreigingsbronnen en dreigingsgebeurtenissen die relevant zijn binnen de gekozen scope;

3. Identificeren van de bekende kwetsbaarheden;

4. Bepalen van de kans van optreden van de dreigingen, onder de conditie van het bestaande of voorziene stelsel van maatregelen en de bekende kwetsbaarheden;

5. Bepalen van de inbreuken op de kwaliteitsaspecten Beschikbaarheid,

Integriteit of Vertrouwelijkheid en de omvang van de schade die daarbij kan ontstaan;

6. 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;

7. Bepalen van de bijbehorende maatregelen: de beveiligingseisen voor het risico.

8.3 Eisen aan de methode voor risicoanalyse

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 het risico-maatregel overzicht, 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 relevant zijn voor de software, uit te splitsen naar het inrichten van preventieve, detectieve (signalerende), correctieve en repressieve beveiligingsmaatregelen;
- Welke defecten en fouten leiden tot welke beveiligingsrisico's;
- Waar in de levenscyclus beveiligingseisen moeten 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.

8.4 Risico-maatregel overzicht

Het risico-maatregel overzicht verzamelt eerder geïnventariseerde risico's en de daarvoor bedachte maatregelen. Door deze centraal in de organisatie bij te houden, kunnen nieuwe risicoanalyses (zie paragraaf 8.3) voortbouwen op bestaand werk. Daarmee ontstaat een samenhangende risicobeheersing en een overzicht van gepaste standaard maatregelen (best practices).

8.5 Risicobeheersing en risicoacceptatie

Tijdens het ontwikkelproces zijn er verschillende contactmomenten waarop risico's inzichtelijk worden gemaakt. Deze risico's kunnen door (aanvullende) beveiligingsmaatregelen onder controle worden gebracht of geaccepteerd worden. In dit proces wordt dit per project centraal bijgehouden. Hierdoor heeft de opdrachtgever inzicht in welke risico's "onder controle zijn" of nog "open staan". Meestal zal een openstaande status van een risico het gevolg zijn van een bewuste keuze.

8.6 Accepteer de oplevering en bijbehorende risico's

Tijdens de realisatie wordt voortdurend afgestemd over risico's. Bij een oplevering vindt de formele acceptatie plaats van de software en de risico's. Dit valt onder de verantwoordelijkheid van de opdrachtgever. Risicoacceptatie is relevant wanneer aan beveiligingseisen onvoldoende voldaan is. De afweging voor acceptatie kan bijvoorbeeld als de ernst van de bevindingen laag is of de kosten van een eventueel herstel niet opwegen tegen de opbrengst.

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. Het mankement wordt tijdelijk gedoogd en er wordt een plan opgesteld om de afwijking te herstellen en/of een mitigerende maatregel in te voeren; Bij gedogen gelden de volgende afspraken: Er is een uitgewerkt, goedgekeurd plan (inclusief budget) met een business case beschikbaar, waarin wordt beschreven hoe en wanneer een formeel goedgekeurde situatie zal ontstaan;
- **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.

8.7 SSD volwassenheidsniveaus voor risicoacceptatie

U.05 Het accepteren van risico's	
De eindverantwoordelijke voor het bedrijfsproces heeft inzicht in de beveiligingsrisico's en accepteert tijdelijk eventuele restrisico's en neemt hierop actie.	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	Door de eindverantwoordelijke voor het bedrijfsproces wordt een goedkeuring, een gedoog of verbod voor een release gegeven. • Het is, indien van toepassing, duidelijk welke afwijkingen voorafgaand aan de ingebruikname van een release aanwezig zijn.

U.05 Het accepteren van risico's	
2. Beheerst proces (managed process)	Door de eindverantwoordelijke voor het bedrijfsproces wordt een overzicht bijgehouden aan welke eisen de applicaties voldoen en welke risico's bestaan op basis van vastgelegde afwijkingen, die door de eindverantwoordelijke voor het bedrijfsproces zijn geaccepteerd. • Er wordt volgens een op afdelingsniveau vastgelegd proces bepaald welke afwijkingen voorafgaand aan de ingebruikname van een release aanwezig zijn en welke risico's daarmee worden gelopen. • Per tijdelijk geaccepteerde afwijking is de gedoogperiode bekend. • De eindverantwoordelijke voor een bedrijfsproces stuurt in een vastgelegd cyclisch proces op het verminderen van het aantal afwijkingen en het voldoen aan de afspraken over de gedoogperiode.

U.05 Het accepteren van risico's	
3. Vastgesteld proces (established process)	Organisatiebreed wordt een overzicht bijgehouden aan welke eisen de applicaties binnen de organisatie voldoen en welke risico's bestaan op basis van vastgestelde afwijkingen, die door de eindverantwoordelijke voor het bedrijfsproces formeel zijn geaccepteerd. • Er wordt volgens een vastgelegd en op organisatieniveau vastgesteld proces bepaald welke afwijkingen voorafgaand aan de ingebruikname van een release aanwezig zijn en welke risico's daarmee gelopen wordt. • Per tijdelijk geaccepteerde afwijking is de gedoogperiode vastgelegd en door de eindverantwoordelijke voor een bedrijfsproces onderschreven en formeel geaccepteerd. • Het SSD-dashboard (zie paragraaf 10.1) geeft aan hoe de risicoacceptatie van de eindverantwoordelijken voor een bedrijfsproces zich verhoudt tot de risicoclassificatie van hun bedrijfsprocessen. • Iedere eindverantwoordelijke voor een bedrijfsproces stuurt in een vastgelegd cyclisch proces op het verminderen van het aantal afwijkingen en het voldoen aan de gedoogperiode. • Iedere eindverantwoordelijke voor de bedrijfsprocessen kan verantwoording afleggen, zowel intern (middels een dashboard) als extern (middels een compliancy statement). • Organisatiebreed vindt controle en sturing plaats op het verminderen van het aantal afwijkingen en het voldoen aan de afspraken over de gedoogperiode. • Daar waar nodig worden maatregelen elders binnen de beveiligingsarchitectuur genomen.

U.05 Het accepteren van risico's	
4. Voorspelbaar proces (predictable process)	Er is sprake van een optimaal werkende 'shift-left', waardoor er bij de acceptatie geen verrassingen meer voordoen en aan alle geldende beveiligingseisen wordt voldaan. • De risicoacceptatie maakt integraal onderdeel uit van de risicomanagementprocessen van de organisatie. Een compliancy statement geeft aan hoe de beveiliging van de software zich verhoudt tot één of meerdere gekozen standaarden. De interne (goedkeurings)processen van de opdrachtgever sluiten aan op de ontwikkelmethodiek van de opdrachtnemer. Vanuit de bedrijfsbrede controle wordt, door het uitwisselen van kennis en ervaring met peer-organisaties, gekeken hoe de organisatie zich verhoudt tot de risicoacceptatie van vergelijkbare organisaties. • Daar waar nodig wordt de aansturing aangescherpt.
5. Geoptimali-seerd proces (optimized process)	Het acceptatieproces is een proces, waarbij er steeds een actueel beeld is van de aanwezige afwijkingen en risico's. Het acceptatieproces ondersteunt optimaal de 'shift left' beweging. Bij een uitbreiding of verandering in de gehanteerde eisen worden betrokken eigenaren geïnformeerd over de betekenis ervan.

9 Monitoren van gebruik

9.1 Monitor/volg systeemgedrag tijdens de gebruiksfase

Tijdens de gebruiksfase kunnen zich incidenten voordoen of kunnen nieuwe risico's ontstaan door bijvoorbeeld aanpassing van configuratie, een nieuwe kwetsbaarheid in een open source component dat wordt gebruikt, of een hacker ontdekt een nog onbekende kwetsbaarheid in het systeem.

Incidenten kunnen worden waargenomen via onder meer de helpdesk en door:

- **Logging:**
  Hierbij wordt geautomatiseerd informatie over gebeurtenissen /en handelingen vastgelegd, zodat achteraf actief informatie uit de logs gehaald kan worden op het moment dat het nodig is.
- **Monitoring:**
  Hierbij is door middel van visualisaties in dashboards informatie getoond, zodat uit de logs bepaald kan worden welke gebeurtenissen of handelingen gevaar (kunnen) opleveren.
- **Alerting:**
  Hierbij wordt geautomatiseerd gewaarschuwd dat er grenswaarden bereikt worden in de monitoring.

Monitoring vindt veelal in een Security Operations Center (SOC) plaats. Het SOC monitort en analyseert de informatie op een continue basis en reageert op (mogelijke) gevaren. Het opzetten en bemensen van een SOC vraagt om expertise en tijd en brengt kosten met zich mee. Hierdoor kan het nuttig zijn het SOC uit te besteden of samen te werken tussen SOC's, bijvoorbeeld tussen die van de opdrachtgever en de opdrachtnemer. Het is aan te raden duidelijk te specificeren wat op welk vlak onderling verwacht wordt en deze afspraken in een Service Level Agreement (SLA) ofwel Diensten Niveau Overeenkomst (DNO) vast te leggen, zodat er duidelijkheid is over het afhandelen van de incidenten in de incidentmanagementprocessen. Hierbij is duidelijk wat de verwachte reactie- en oplostijden zijn van verschillende typen problemen en op welke manier er wordt gerapporteerd.

Monitoren van systeemgedrag tijdens operatie kan met tooling grotendeels automatisch gevolgd worden. Belangrijk is om vast te stellen welke kenmerken relevant zijn, wat beschouwd wordt als een uitzondering, en wat daarmee moet gebeuren (wie doet wat). Dit heeft invloed op de eisen van het systeem met betrekking tot logging.

Nieuwe risico's kunnen worden gedetecteerd door bijvoorbeeld regelmatig automatische vulnerability scans uit te voeren en met enige regelmaat een penetratietest (pentest) of code review uit te voeren. Verder is het belangrijk om te weten welke (open source) componenten worden gebruikt in een systeem en welke versies, zodat kan worden gemonitord op de noodzaak voor het patchen of vervangen van een component – bijvoorbeeld als nieuwe kwetsbaarheden bekend worden en als input voor het software lifecycle managementproces (LCM). Het is belangrijk om daar afspraken over te maken: wie doet wat.

9.2 Monitoren op oneigenlijk gebruik

Logging en monitoring is een wezenlijk activiteit die vanuit de BIO en ISO 27002 plaatsvindt. Hierbij is er aandacht voor activiteiten op het netwerk. Het is echter ook van belang dat dit ook gebeurt op applicatieniveau, daarom moet de opdrachtgever hier eisen aan stellen en moeten de ontwikkelaars van applicaties dit meenemen. Voor (kritische) applicaties dient loggingbeleid te bestaan en te worden nageleefd.

9.3 Terugkoppelen van bevindingen

Het controleren op oneigenlijk gebruik van applicaties kan door middel van logging en monitoring plaatsvinden. Een andere aanpak is het registreren van meldingen van gebruikers over vermeend oneigenlijk gebruik via bijvoorbeeld een helpdesk. Belangrijk hierbij is dat er afspraken over responsible disclosures zijn vastgelegd. Het terugkoppelen van oneigenlijk gebruik zal moeten plaatsvinden naar de ontwikkelaars, de opdrachtgever en mogelijk zelfs bij een autoriteit als de applicatie onderdeel uitmaakt van een digitale dienst in het kader van de EU regelgeving NIS.

9.4 SSD volwassenheidsniveaus van Monitoren van gebruik

U.06 Het monitoren tijdens de gebruiksfase	
De organisatie monitort tijdens de gebruiksfase op het voorkomen van incidenten.	
Niveau	Criterium (wie en wat)
1. Informeel uitgevoerd (performed process)	Op het niveau van de beheerders van de applicaties vindt incidentafhandeling plaats.
2. Beheerst proces (managed process)	Afhandeling van incidenten vindt plaats via op afdelingsniveau vastgelegde processen. • Afhandeling van incidenten waargenomen door gebruikers vindt plaats via helpdesk-processen. • Afhandeling van incidenten waargenomen door het loggen en monitoren van de productiesystemen vindt plaats volgens vastgelegde processen. • Nieuwe risico's kunnen worden gedetecteerd door met regelmaat uitvoeren van pentesten.
3. Vastgesteld proces (established process)	Afhandeling van incidenten vindt plaats via vastgelegde processen, die op organisatieniveau zijn vastgesteld. • De helpdesk-processen zijn organisatiebreed. • Het loggen en monitoren vindt organisatiebreed in samenhang plaats. • Kennis over geaccepteerde risico's is organisatiebreed beschikbaar ten behoeve van de incidentafhandeling.

U.06 Het monitoren tijdens de gebruiksfase	
4. Voorspelbaar proces (predictable process)	Bij de incidentmanagementprocessen, inclusief probleemmanagement, is de keten van opdrachtgever, ontwikkelaar en de hostingpartij betrokken. Voorafgaand aan het aanpassen van configuraties en bij veranderde omstandigheden is bepaald wat de impact hiervan op het voldoen aan de beveiligingseisen
5. Geoptimali-seerd proces (optimized process)	Voor alle software, inclusief die van bestaande systemen, geldt dat bij nieuw ontstane risico's er tijdig/snel een mitigatieplan is ontwikkeld en tot uitvoer gebracht. • Sturing is mogelijk op basis van een actueel risicobeeld afkomstig van de SSD-processen en het monitoren van de systemen De SSD-processen, het monitoren van de systemen en de incidentmanagementprocessen zijn vergaand geautomatiseerd en maken onderdeel uit van organisatiebrede beveiligingsprocessen, zodat er steeds een actueel beeld is van gebeurtenissen of handelingen gevaar die (kunnen) opleveren en van de status van de afhandeling van de incidenten.

DEEL 3: Vergroten van de sturing

10 Verantwoording afleggen

Het afleggen van verantwoordelijkheid over de mate waarin grip is op de veiligheid gebeurt op twee manieren. Deze manieren hebben ieder een eigen doelstelling, maar versterken elkaar wel.

1. **Het sturen op compliance:**
   Compliance geeft aan in welke mate aan de gestelde beveiligingseisen wordt voldaan en gaat dus over de applicatieveiligheid en heeft dus tot doel de applicatie daadwerkelijk veiliger te krijgen.

2. **Het sturen op volwassenheid:**
   Sturing op volwassenheid is een continu proces om de samenwerking binnen de organisatie van de opdrachtgever verder te vergroten en gaat dus over de organisatie van de opdrachtgever en heeft tot doel te komen tot een gezamenlijke aanpak in het vergroten van de informatieveiligheid.

10.1 Sturen op compliance

Compliance geeft aan in welke mate een opdrachtgever, of beter gezegd de interne opdrachtgevers, en de opdrachtnemers zich aan de gestelde beveiligingseisen houdt. Hiertoe wordt een dashboard bijgehouden en vindt sturing plaats op basis van het ontbreken van compliance en de onderlinge verschillen.

Het afleggen van verantwoording kan zowel intern (middels een dashboard/centraal overzicht) als extern (middels een compliancy statement, een uiting van verantwoording vergeleken met heersende regels of standaarden).

SSD-dashboard

Een SSD-dashboard kan management inzicht geven in de status en effectiviteit van de risicobeheersing op basis van Grip op SSD. In het dashboard wordt de risicoclassificatie van de software afgezet tegen restrisico's: 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 (zie hoofdstuk 11).

In het SSD-dashboard wordt met een kleurcodering bijgehouden in hoeverre applicaties aan de beveiligingseisen voldoen.

Het gebruik van kleuren in het SSD-dashboard

De rapportages zijn steeds gericht op applicaties. Uitspraken of een applicatie aan de 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:

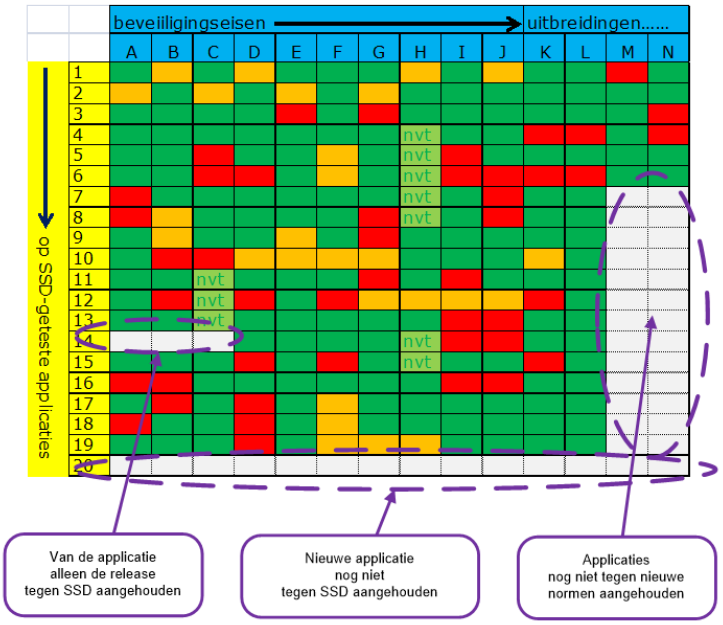
- **Groen** - De gehele applicatie voldoet aan deze eis.
- **Lichtgroen** - De eis is voor deze applicatie niet van toepassing (n.v.t.). Hierover is uitleg (comply) en overeenstemming verkregen.
- **Oranje** - Met de kleur oranje kan worden aangeduid dat met de applicatie-eigenaar afspraken zijn gemaakt over de eindigheid van de afwijking. (Dit conform de gedoogaanpak in het document van de SSD-methode.)
- **Rood** - In de applicatie is op één of meerdere plekken een afwijking geconstateerd. Welke afwijking dat is, wordt bijvoorbeeld in een commentaarveld opgeslagen.

- **Wit** - Er is nog geen constatering, bijvoorbeeld bij een recent toegevoegde eis of bij een applicatie die nog niet of slechts gedeeltelijk tegen de SSD-normen is aangehouden.

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.



Afbeelding 3: Voorbeeld van een SSD dashboard

Gap-analyse

Met het dashboard kan een verschil worden geconstateerd tussen vereiste en geïmplementeerde maatregelen. Dit suggereert een restrisico. Belanghebbenden moeten bepalen of dit restrisico acceptabel is voor de organisatie.

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 beveiligingseisen passen bij de beleving van risico's door de belanghebbenden in de organisatie.

10.2 Sturen op volwassenheid

Om voortgang te herkennen in het inrichten van Grip op SSD kent de methode volwassenheidsniveaus, waarmee een organisatie de methode stapsgewijs kan invoeren en realistische verwachtingen/groeidoelstellingen kan formuleren.

De volwassenheidsdoelstellingen zijn gebaseerd op een volwassenheids-standaard model (Capability Maturity Model, CMM) en specifieker gedefinieerd voor de SSD-processen.

Volwassenheidsmodellen zijn een manier om de mate van controle en voorspelbaarheid van processen te classificeren. Als standaard wordt daarbij typisch verwezen naar CMM of haar

variant CMMI. Deze staan voor Capability Maturity Model (Integration). Deze volwassenheidsniveaus zijn formeel toetsbaar met een standaard aanpak, zoals de Standard CMMI Appraisal Method for Process Improvement (SCAMPI).

Het doel van CMM is om overzicht te krijgen en mogelijke risico's/verbeterkansen te identificeren. Het is niet gezegd dat iedere organisatie per se op alle punten maximaal volwassen moet zijn. Maar volwassenheid is een vereenvoudigde, abstracte inschatting van hoe voorspelbaar, en met welke garanties, een organisatie haar producten en diensten kan leveren. Als we CMM toepassen op SSD geeft dit een indruk van deze verschillende niveaus.

11 Classificatie van systemen en gegevens

Door een systeem of een gegevensverzameling toe te kennen aan een beveiligingsklasse, kan snel worden bepaald welke beveiligings-maatregelen van toepassing zijn. Daarvoor is het dus noodzakelijk dat er beschikking is over een classificatieschema waarin elke klasse is voor-zien van de benodigde maatregelen, zoals het wel of niet versleutelen van gegevens.

11.1 Classificeer systemen & gegevens

Om te bepalen hoe moet worden omgegaan met de beveiliging van specifieke systemen en gegevens is het zaak dat de proceseigenaar die systemen en gegevens classificeert naar het benodigde beveiligingsniveau voor Beschikbaar-heid, Integriteit en Vertrouwelijkheid (BIV). Een deel hiervan bestaat uit een Business Impact Analyse, waarin IT-middelen (systemen en gegevens) worden geïnventariseerd, samen met de algemene dreigingen en de bijbehorende risico's.

Een voorbeeld van een classificatie is: de vertrouwelijkheid van voorbereidende bestem-mingsplannen worden geclassificeerd als 'geheim'. Bij de klasse 'geheim' horen dan weer vaste passende beveiligingseisen, voorbeelden zijn least privilege en dat toegang via twee-factor identificatie gaat.

De definities van de drie BIV kwaliteitsaspecten zijn:

- **Beschikbaarheid:**
  Beschikbaarheid betreft het zorgen voor een ongestoorde voortgang van de informatie-voorziening voor gebruikers.
- **Integriteit:**
  Integriteit betreft het waarborgen van de juistheid en volledigheid van informatie en de verwerking daarvan.
- **Vertrouwelijkheid:**
  Vertrouwelijkheid betreft het waarborgen dat informatie alleen voor geautoriseerde toegankelijk is.

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

- **Controleerbaarheid:**
  Controleerbaarheid betreft de mate waarin bovenstaande kwaliteitskenmerken (BIV) gecontroleerd kunnen worden. Dit betreft met name logging, documentatie en openheid voor audits (bijvoorbeeld het beschikbaar stellen van broncode voor onderzoek).

Classificatieschema's zijn vaak voorgeschreven of een best practice binnen de organisatiesoort van de opdrachtgever. Een typische constructie daarbij is dat een klasse die 'Midden' is kan volstaan met de baseline aan security-maatregelen en dat voor hogere klassen een risicoanalyse moet plaatsvinden om additionele maatregelen te bepalen.

11.2 Stappenplan voor het classificeren

1. Beschrijf de doelstelling van het bedrijfsproces;
2. Bepaal de scope van het bedrijfsproces: welke stappen worden doorlopen en welke informatiestromen/informatieverzamelingen worden daarbij aangesproken;
3. Stel zakelijke randvoorwaarden (beleid en architectuur) en juridische eisen (relevante wet- en regelgeving) vast;
4. Stel de algemene risico's vast voor de betrokken systemen en gegevens op de aspecten BIV (bijvoorbeeld een hack, uitval van een rekencentrum, lekken van een database, technische storing, of een netwerkaanval die een systeem onbeschikbaar maakt). Start hiervoor met het centrale risico-maatregel overzicht om

een eerste selectie te maken. Bedenk daarna nieuwe risico's die specifiek zijn voor het onderzochte bedrijfsproces. Beschrijf de impact/consequentie voor die risico's. Dat kan bijvoorbeeld zijn: reputatieschade, onderbreking van dienstverlening, boetes, schade bij individuen of derden. Bijbehorende overwegingen zijn:

- Op welke technische wijze kan een bedrijfsproces verstoord of onderbroken worden?
- Als een deel van de techniek verstoord wordt (bijvoorbeeld een portaal, technische koppeling of database), werkt die verstoring dan door naar andere systemen of processen?
- Hoe lang kan het bedrijfsproces onderbroken of verstoord zijn voordat dit leidt tot ernstige consequenties voor de organisatie?
- Welke compenserende maatregelen zijn beschikbaar om een onderbreking of verstoring van een systeem/informatiestroom tijdelijk of permanent op te vangen?
- Van welke gegevens is de vertrouwelijkheid van belang en in welke mate?
- Ken de gewenste klassen (beveiligingsniveaus) voor de relevant systemen en gegevens. Bijvoorbeeld: de klasse 'geheim' voor uitkeringsgegevens van burgers).

5. Specificeer per beveiligingsniveau de relevante beveiligingseisen (bijvoorbeeld 2 factor authenticatie voor toegang tot gegevens met de klasse 'geheim').
6. Het is van belang de classificatie periodiek te her evalueren, bijvoorbeeld bij grote veranderingen.

11.3 Aanpassen van classificatie door nieuwe inzichten

De baseline is een 'basis-selectie' en kan worden aangepast door nieuwe inzichten (uit classificatie, risicoanalyse, nieuwe dreigingen, ervaringen met beveiligingseisen die wel of niet effectief blijken te zijn). Tot slot is periodiek onderhoud nodig, waarbij bijvoorbeeld jaarlijks de externe bronnen van de eisen worden nagelopen om wijzigingen te verzamelen en te beoordelen of die moeten worden verwerkt.

12 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. Een Business Impact Analyse (BIA) is daarbij een belangrijk proces.

Input voor de risicoanalyse

Een BIA geeft voor de (kritische) bedrijfs-processen enerzijds de impact aan van de uitval van een applicatie en een bedrijfsproces en vormt daarmee een nuttige basis voor het uitvoeren van risicoanalyses, anderzijds vormt het inzicht over wat er moet gebeuren om te voorkomen dat de bedrijfsvoering in gevaar komt en vormt daarmee een nuttige input voor het Business continuïteitsplan (BCP). Deze informatie over de impact maakt zo een betere inschatting van risico's in de betekenis van kans x impact mogelijk:

- 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.

Privacy

De AVG vormt input voor de eisen die voor de applicatie moeten gelden. De AVG vereist het nemen van passende maatregelen. Een belangrijk onderdeel bij het nemen van die passende maatregelen is het uitgangspunt van Privacy by Design: door een slim ontwerp worden dure (extra) maatregelen voorkomen. Het document Privacy by Design[2] van het CIP beschrijft hoe privacy meegenomen kan worden. Het document Privacy supplement[3] van het CIP beschrijft de eisen waaraan aanvullende op de beveiligingseisen minimaal voldaan moet worden om aan de AVG te kunnen voldoen. Een Data Protection Impact Assessment (DPIA), ofwel gegevensbeschermingseffectbeoordeling, is daarbij een wettelijk verplicht instrument om privacy risico's van een gegevensverwerking in kaart te brengen.

Input voor BCP

Op basis van een expliciete Business Impact Analyse (BIA) zijn de kwaliteitseisen, voor de binnen een bedrijfsproces gebruikte informatie-systemen, vast te stellen. De bedrijfsprocessen verschaffen de context waarin de onder-steunende IT-middelen zich bevinden en zijn bepalend voor de BIV-classificatie per IT-middel. Dit gebeurt door op basis van de BIA inzicht te vormen over:

- De primaire en secundaire bedrijfs-processen, die noodzakelijk zijn voor de uitvoering van de kerntaken;
- De doelstellingen van ieder bedrijfsproces;

[2] https://www.cip-overheid.nl/media/1574/20170507-handleiding-privacy-by-design-v3_0.pdf

[3] https://www.cip-overheid.nl/media/1733/20220104-uitwerking-privacymaatregelen.pdf

- 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.

Input voor beveiligingseisen

De uiteindelijke uitkomst van de BIA door de organisatie is een lijst van relevante IT-middelen met bijbehorende BIV-classificaties (hoofdstuk 11). Deze uitkomst dient als basis voor de standaard beveiligingseisen (zie paragraaf 4.2). De risicoanalyse (zie paragraaf 8.2) leidt tot specifieke beveiligingseisen en beveiligings-maatregelen per IT-middel.

Deel 4: Bijlagen

Bijlage A: Organisatorische eisen opdrachtnemer

Organisatorische eisen aan opdrachtnemers spelen een rol bij selectie van externe leveranciers en bij afspraken die worden gemaakt bij bestaande opdrachtnemers. Het onderdeel informatiebeveiliging is vooral van belang als de opdrachtnemer samen met het ontwikkelen van veilige software ook moet zorgdragen voor de hosting van de software, de beveiliging van broncode en de documentatie. Hieronder staan enkele voorbeelden van onderwerpen waar eisen over gesteld kunnen worden.

Informatiebeveiliging en beleid

- De leverancier kan een volwassen informatiebeveiligingsbeleid aantonen i.e. certificering;
- De leverancier heeft een volwassen incidentafhandelingsplan;
- De leverancier is bereid om deel te nemen aan audits i.e. code review, pentests;
- De leverancier houdt zich aan de GDPR-wetgeving en implementeert mechanismen hiervoor om dit te garanderen;
- De leverancier beschermt gevoelige informatie met de nodige maatregelen i.e. encryptie;
- De leverancier implementeert processen om data te kunnen herstellen in geval van verlies;
- Operaties en toegang tot gevoelige informatie en functies worden gemonitord en gelogd;
- Werknemers bij leverancier zijn getoetst op hun integriteit.

Toegangsbeheer

- De leverancier biedt transparantie over wie binnen het bedrijf toegang heeft tot de afgeleverde gegevens;
- De leverancier zorgt voor toegangsbeheermechanismen die enkel toegang tot het systeem/informatie verleend aan gebruikers die gemachtigd zijn;
- De leverancier integreert autorisatie en authenticatie mechanismen, gebruikmakende van de huidige industriestandaarden;
- De leverancier logt en monitort relevante beveiligingsgebeurtenissen en minimaal gefaalde login pogingen en gefaalde data toegangs- en aanpassingsoperaties.

Software ontwikkeling en veiligheid

- De leverancier gebruikt de laatste versie van softwarebibliotheken en software-ontwikkeltools of legt uit als een andere versie gebruikt wordt;
- De leverancier toetst de software tijdens ontwikkeling op kwetsbaarheden gebruik makend van statische code-analyse tools, automatische securitytests, handmatige code review en handmatige penetratietests;
- Secure coding is deel van het ontwikkelingsproces gebruikmakende van bekende industriestandaarden.

Kennisdeling en opleiding

- Medewerkers betrokken bij software-ontwikkeling krijgen minimaal jaarlijks een security awareness training.
- De leverancier heeft een ‘center of excellence’ georganiseerd die zich bezighoudt met het faciliteren van veilige software-ontwikkeling met kennis, richtlijnen en tools.
- Developers gebruiken actief secure coding guidelines en requirements tijdens hun werk.

Bijlage B: Rollen binnen Grip op SSD

Het volledig grip op SSD krijgen vraagt om een organisatie met een duidelijke structuur. Hiervoor moeten een aantal functies/rollen zijn belegd. Binnen verschillende organisaties kunnen hiervoor verschillende namen in gebruik zijn, maar er moeten medewerkers zijn die de taken behorende bij deze rollen uitvoeren.

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 een heldere mandatering zijn naar de actuele opdrachtgever, omdat Grip op SSD met gezag moet worden aangestuurd.

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 informatie-beveiliging en geven daarover gevraagd en ongevraagd advies aan de opdrachtgever en aan andere betrokkenen.

Een beveiligingsadviseur is degene die de opdrachtgever adviseert over de beveiligings-eisen, 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 informatie-beveiliging.

Binnen de SSD-methode zijn de beveiligings-adviseurs betrokken bij het opstellen van de standaard beveiligingseisen, het adviseren van de opdrachtgevers, het uitvoeren van de risico-analyses, het opstellen van ‘misuse and abuse cases’, het invullen van de contactmomenten en het interpreteren van rapportages over testactiviteiten, incidenten en verstoringen.

(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 beveiligings-maatregelen. 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.

Binnen de SSD-methode zijn de Security architecten zijn verantwoordelijk voor het ondersteunen van de keuze welke beveiligingsmaregelen niet binnen de applicatie genomen moeten worden, omdat voor de hiermee samenhangende risico's elders binnen de architectuur al afdoende maatregelen zijn genomen.

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.

Binnen de SSD-methode zijn de Security Officers enerzijds verantwoordelijk voor het signaleren van risico's bij het niet opvolgen van een beveiligingseis en anderzijds kunnen zij adviseren bij het maken van een keuze voor het accepteren van een risico (zie paragraaf 8.6). Zij doen dit met kennis die zij hebben van de organisatie, de bedrijfsvoering en bedrijfsbelangen.

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 hosting-partij. 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 analyseren 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.

Binnen de SSD-methode zijn de Technische Security Officers enerzijds verantwoordelijk voor de uitleg van de technische implementatie van de maatregelen en anderzijds kunnen de technische implicaties van de maatregelen inschatten. Zij doen dit in tegenstelling tot de Security Officers primair met de kennis die zij hebben van de techniek. De rol van security officer en van technisch security officer kunnen door één persoon worden ingevuld als de security officer de benodigde technische kennis bezit.

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.

Bijlage C: Technische eisen in de Grip op SSD Normen

In onderstaande tabel staat een overzicht van de globale criteria uit de Grip op SSD normen versie 3.0 – de laatste versie ten tijde van het schrijven van dit document. Zie https://www.cip-overheid.nl/. Naast deze lijst bestaat ook een versie van deze normen specifiek voor mobiele applicaties.

De globale criteria in deze bijlage geven een beeld van de normen maar zijn door hun beknoptheid niet specifiek. Daarvoor worden ze verder in detail uitgewerkt in het desbetreffende document.

Datacommunicatie

- **SSD-4 Veilige communicatie:**
  De applicatie past versleuteling toe op de communicatie van gegevens die passend is bij het classificatieniveau van de gegevens, zowel over interne als externe netwerken en controleert hierop. Van te beschermen gegevens worden alleen de noodzakelijke gecommuniceeerd

Opslag

- **SSD-2 Veilige gegevensopslag:**
  Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.

Authenticatie

- **SSD-5 Authenticatie van gebruikers en systemen:**
  Applicaties stellen de identiteit van gebruikers en systemen vast op basis van een mechanisme voor identificatie en authenticatie, waarbij de authenticatiegegevens in een centrale authenticatievoorziening worden beheerd.

Autorisatie

- **SSD-8 Autoriseer toegang:**
  De applicatie dwingt de door de opdrachtgever voorgeschreven beperkende set van rechten en privileges af met alleen de voor de gebruiker en systemen noodzakelijke toegang.

Gebruikersbeheer

- **SSD-7 Gebruikersrechtenbeheer:**
  De rechten die gebruikers hebben binnen een applicatie (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.

Sessiebeheer

- **SSD-12 Sessie-beëindiging:**
  De applicatie beëindigt een sessie na een vooringestelde periode van inactiviteit van de gebruiker via automatische sessie-beëindiging,.

- **SSD-14 Borgen van Sessie Authenticiteit:**
  De applicatie hanteert voor sessie-identifiers onvoorspelbare tekenreeksen en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.

Logging

- **SSD-30 Applicatie logging:**
  In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie)

actief en efficiënt, effectief en beveiligd ingericht.

- **SSD-13 Onweerlegbaarheid:**
  De applicatie ondersteunt de onweerlegbaarheid voor daartoe aangewezen transacties via cryptografische technieken.

- **SSD-9 Registreren van (on)succesvolle login-pogingen:**
  De applicatie registreert gelukte en mislukte login-pogingen

Invoer/uitvoer validatie

- **SSD-19 Invoer-normalisatie:**
  De applicatie voorkomt manipulatie door alle ontvangen invoer te normaliseren alvorens die te valideren. De richtlijnen voor invoerbehandeling zijn van toepassing voor alle invoer die van buiten de applicatie komt. Dus niet alleen (eind)gebruikers, maar ook externe systemen en applicaties.

- **SSD-20 Uitvoer-schoning (output sanitization):**
  De applicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren naar de juiste context.

- **SSD-21 Beperkte commando/query-toegang:**
  De applicatie legt beperkingen aan queries en commando's op daar waar met achterliggende systemen wordt gecommuniceerd en deze communicatie wordt alleen ingericht indien strikt noodzakelijk.

- **SSD-22 Invoer-validatie:**
  De applicatie controleert invoer (bijvoorbeeld een HTTP-request) door deze te valideren alvorens die te gebruiken.

- **SSD-23 Beperkte file Includes:**
  De applicatie voorkomt de mogelijkheid van dynamische file includes.

- **SSD-24 Beperking van te versturen HTTP-headers:**
  De webserver stuurt bij een antwoord aan een gebruiker alleen die informatie in de HTTP-headers mee die van belang is voor het functioneren van HTTP.

- **SSD-27 Discrete foutmeldingen:**
  De applicatie neemt in een foutmelding geen inhoudelijke foutinformatie op die misbruikt kan worden.

- **SSD-28 Discreet commentaar:**
  De aan de gebruiker aangeboden scripts / code bevat geen commentaar dat tot misbruik kan leiden.

- **SSD-32 Bescherming tegen XML externe entiteit injectie:**
  De applicatie beperkt de mogelijkheid tot manipulatie door alle externe XML invoer te beschermen tegen entiteit injectie.

Externe componenten

- **SSD-3 Veilige externe componenten:**
  Applicaties maken gebruik van veilige en actief onderhouden externe componenten.

Architectuurprincipes

- **SSD-15 Scheiding van presentatie, applicatie en gegevens:**
  De architectuur van een applicatie is gebaseerd op een gelaagde structuur door de presentatie-laag, de applicatielaag en de gegevens te scheiden, zodat de lagen beschermd kunnen worden binnen de netwerkzones.

- **SSD-17 Gescheiden beheerinterface:**
  Beheeractiviteiten vinden plaats via een van

de standaard gebruikersinterface gescheiden beheerinterface.

Infrastructuur

- **SSD-1 Hardening:**
  De applicatie voldoet aan het hardeningbeleid. De software en het platform zijn daartoe geconfigureerd volgens de bijbehorende hardeningrichtlijn. Het configureren is procesmatig en procedureel ingericht.
- **SSD-26 Beperkte HTTP-methoden:**
  De webserver faciliteert alleen de HTTP-functionaliteiten die nodig zijn voor het functioneren van de applicatie.
- **SSD-29 Voorkom directory listing:**
  De aan de gebruiker getoonde informatie bevat geen directory listings, zodat die niet kunnen worden misbruikt.
- **SSD-31 Standaard stack:**
  De (web-)applicatie(-omgeving) maakt gebruik van systeemcomponenten en voorzieningen die onderdeel zijn van een formeel gespecificeerde stack.
- **SSD-33: Veilige HTTP response headers:**
  De applicatie maakt gebruik van veilige response headers.

Bijlage D: Referenties

Procesraamwerken veilige software ontwikkeling:

- NIST SSDF - Secure Software Development Framework: https://csrc.nist.gov/projects/ssdf
- OWASP SAMM - Software Assurance Maturity Model: https://owaspsamm.org/
- BSIMM – Building Security In Maturity Model: https://www.bsimm.com/
- Software Security: Building Security In, Gary McGraw, ISBN: 0-321-35670-5, Januari 2006
- Microsoft SDL - Microsoft Security Development Lifecycle; https://learn.microsoft.com/nl-NL/windows/security/threat-protection/msft-security-dev-lifecycle

Technische Eisen:

- CIS Controls - Critical Security Controls: https://www.cisecurity.org/controls/
- OWASP ASVS - Application Security Verification Standard: https://github.com/OWASP/ASVS
- Grip op SSD Normen: https://www.cip-overheid.nl/
- OWASP Mobile ASVS- Mobile Application Security Verification Standard: https://github.com/OWASP/owasp-masvs
- Open CRE – verzameling van eisen en richtlijnen: https://www.opencre.org/
- Mitre CWE - Common Weakness Enumeration: https://cwe.mitre.org/

Dreigingenanalyse en risicoanalyse:

- Publicatie van de CIO Interest Group Informatiebeveiliging, CIO Platform Nederland, september 2012; https://docplayer.nl/2163428-Risicoanalyse-een-verkenning-publicatie-van-de-cio-interest-group-informatiebeveiliging.html
- Procedure Risicoanalyse, Standaard methodiek Groep ICT, RABO-groep, 4 januari 2011
- ISO 25010: https://nl.wikipedia.org/wiki/ISO_25010
- Risicoanalyse, Een verkenning, https://www.informit.com/articles/article.aspx?p=446451%20
- Mitre CAPEC - Common Attack Pattern Enumerations and Classifications: https://capec.mitre.org/

Divers:

- Grip op Secure Software Development: via https://www.cip-overheid.nl/
- NCSC Whitepaper securitytesten: https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten
- BIO - Baseline Informatiebeveiliging Overheid; https://bio-overheid.nl/