Applicatieontwikkeling

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.



©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

Titel	BIO Thema-uitwerking Applicatieontwikkeling
Datum	Mei 2026
Versie en status	3.0
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CP-kernteamleden
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: CIP-kernteam Versie 2.2: CIP-kernteam Versie 2.3: CIP-kernteam (tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde enters verwijderd, doelstellingen en risico's geüniformeerd, BIO2.0-opmaat verwerkt) Versie 2.4: CIP-kernteam

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.

Wijzigingsbeheer

In de onderstaande tabel worden alle relevante wijzigingen in dit document bijgehouden, om eenvoudig inzicht te krijgen in de uitgevoerde aanpassingen.

Versie	Datum	Wijziging	Door
1.0	Februari 2021		CIP-kernteam
2.0	Februari 2021	Verwijzingen naar andere ISO-standaarden zonder specifieke controls (Applicatie thema Cobit (U.04.1 e.v.), ISO 27017	CIP-kernteam
2.1	Oktober 2021	Reviewers vervangen in CIP-kernteam	CIP-kernteam
2.2	Maart 2023	Verwijzingen op control-niveau	CIP-kernteam

		aangepast in B.04/05/06 en U.01/12.	
2.3	November 2023	Tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde enters verwijderd, doelstellingen en risico's geüniformeerd, BIO2.0-opmaat verwerkt)	CIP-kernteam
3.0	Mei 2026	BIO2 1.3 verwerkt	CIP-kernteam

Leeswijzer

Voorafgaand aan hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein, de kern van dit document, heeft elke BIO Thema-uitwerking een inleiding met een standaard paragraafindeling.

Aanvullend geldt:

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- De controls en maatregelen vermeld in deze thema-uitwerking zijn in het beleids-, uitvoerings- en control-domein georganiseerd, waarmee ze bij de overeenkomstige functionarissen kunnen worden geadresseerd. Deze functionarissen zijn niet benoemd omdat dit organisatie-afhankelijk is.
- Bijlagen zijn opgenomen alleen voor specifieke informatie uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en/of 5 Control-domein.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.
- Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

Leeswijzer		4
1	Inleiding	10
1.1	Context applicatieontwikkeling	10
1.2	Doel van dit document	11
1.3	Scope en begrenzing applicatieontwikkeling	11
1.4	Ontwikkelcyclus applicatieontwikkeling	12
1.4.1	Perspectieven	13
1.4.2	Analyseren	14
1.4.3	Specificeren	14
1.4.4	Ontwerpen	14
1.4.5	Ontwikkelen (implementeren)	14
1.4.6	Valideren	15
1.4.7	Gebruiken	15
1.4.8	Onderhouden en beheren	15
1.5	Ontwikkelmethoden	15
1.6	Applicatieobjecten in relatie tot ontwikkelmethode	16
2	Beveiligingsobjecten applicatieontwikkeling	17
2.1	Organisatie van applicatieontwikkelingsobjecten	17
2.2	Observatie bij objectidentificatie	17
2.3	Objecten geprojecteerd op domein en gesorteerd naar invalshoek	18
3	Beleidsdomein	19
3.1	Doelstelling	19
3.2	Risico’s	19
3.3	Objecten, controls en maatregelen	19
3.3.1	B.01 Beleid voor (beveiligd) ontwikkelen	20
Objectdefinitie		20
Objecttoelichting		20
3.3.2	B.02 Systeem-ontwikkelmethode	20

Objectdefinitie 20
Objecttoelichting 21
3.3.3 B.03 Classificatie van informatie 22
Objectdefinitie 22
Objecttoelichting 22
3.3.4 B.04 Veilige systeemarchitectuur en technische uitgangspunten 23
Objectdefinitie 23
Objecttoelichting 23
3.3.5 B.05 Uitbestede systeemontwikkeling 24
Objectdefinitie 24
Objecttoelichting 24
3.3.6 B.06 Privacy en bescherming persoonsgegevens 25
Objectdefinitie 25
Objecttoelichting 25
3.3.7 B.07 Kwaliteitsmanagementsysteem 26
Objectdefinitie 26
Objecttoelichting 26
3.3.8 B.08 Toegangsbeveiliging op programmacode 27
Objectdefinitie 27
Objecttoelichting 27
3.3.9 B.09 Projectorganisatie 28
Objectdefinitie 28
Objecttoelichting 28
4 Uitvoeringsdomein 30
4.1 Doelstelling 30
4.2 Risico's 30
4.3 Objecten, controls en maatregelen 30
4.3.1 U.01 Wijzigingsbeheerprocedure voor applicaties en systemen 31
Objectdefinitie 31
Objecttoelichting 31
4.3.2 U.02 Beperking software-installatie 32

Objectdefinitie 32

Objecttoelichting 32

4.3.3 U.03 Richtlijn programmacode 33

Objectdefinitie 33

Objecttoelichting 33

4.3.4 U.04 Analyse en specificatie informatiesysteem 34

Objectdefinitie 34

Objecttoelichting 34

4.3.5 U.05 Informatiebeveiliging in projectmangement 36

Objectdefinitie 36

Informatiebeveiliging maakt integraal onderdeel uit van het management van alle projecten, ongeacht type, omvang, duur of discipline, zodat informatiebeveiligingsrisico's effectief worden beheerd gedurende de gehele projectlevenscyclus. 36

Objecttoelichting 36

4.3.6 U.06 Applicatie-ontwerp 37

Objectdefinitie 37

Objecttoelichting 37

4.3.7 U.07 Applicatiefunctionaliteit 38

Objectdefinitie 38

Objecttoelichting 38

4.3.8 U.08 Applicatiebouw 39

Objectdefinitie 39

Objecttoelichting 39

4.3.9 U.09 Systeemacceptatietest 40

Objectdefinitie 40

Objecttoelichting 40

4.3.10 U.10 Beschermen testgegevens 42

Objectdefinitie 42

Objecttoelichting 42

4.3.11 U.11 Scheiding van ontwikkel-, test- en productieomgevingen 43

Objectdefinitie 43

Objecttoelichting 43

4.3.12 U.12 Applicatiekoppeling 45
Objectdefinitie 45
Objecttoelichting 45
4.3.13 U.13 Logging en monitoring 45
Objectdefinitie 45
Objecttoelichting 46
4.3.14 U.14 Applicatie-architectuur 46
Objectdefinitie 46
Objecttoelichting 46
4.3.15 U.15 Tooling ontwikkelmethode 47
Objectdefinitie 47
Objecttoelichting 47
5 Control-domein 49
5.1 Doelstelling 49
5.2 Risico's 49
5.3 Objecten, controls en maatregelen 49
5.3.1 C.01 Richtlijn evaluatie ontwikkelactiviteiten 49
Objectdefinitie 49
Objecttoelichting 50
5.3.2 C.02 Versiebeheer 51
Objectdefinitie 51
Objecttoelichting 51
5.3.3 C.03 Patchmanagement 52
Objectdefinitie 52
Objecttoelichting 52
5.3.4 C.04 (Software)configuratiebeheer 53
Objectdefinitie 53
Objecttoelichting 53
5.3.5 C.05 Quality assurance 53
Objectdefinitie 53
Objecttoelichting 53

5.3.6 C.06 Compliance-management 54
Objectdefinitie 54
Objecttoelichting 55
5.3.7 C.07 Beheersorganisatie applicatieontwikkeling 55
Objectdefinitie 55
Objecttoelichting 56
Bijlage 1: Objecten ingedeeld naar invalshoeken 57
Bijlage 2: Invalshoeken gekoppeld aan het V-model 58

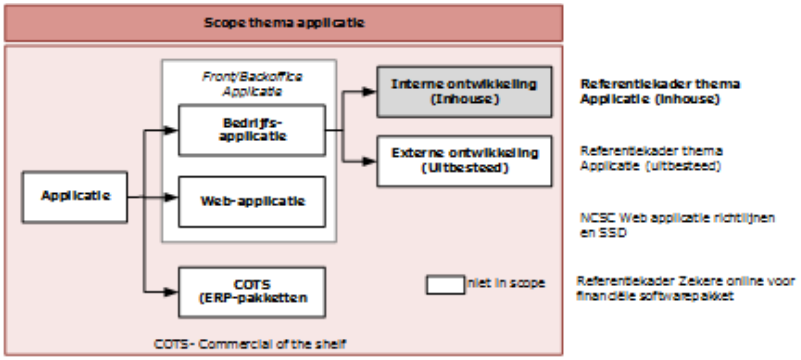
1 Inleiding

De BIO Thema-uitwerking Applicatieontwikkeling is opgesteld om overheidsorganisaties een beeld te geven van de meest relevante onderwerpen die een rol spelen bij applicatieontwikkeling. Deze BIO Thema-uitwerking bevat de beveiligingseisen voor applicatieontwikkeling. Deze zijn tot stand gebracht door de toepasselijke controls en onderliggende maatregelen uit de BIO2 en NEN-EN-ISO/IEC 27002:2022 (hierna genoemd ISO 27002), in een samenhangende context te plaatsen en waar nodig aan te vullen met controls en maatregelen uit andere ISO-standaarden, National Institute of Standards and Technology (NIST), The Standard of Good Practice (SoGP) 2018 e.d.

1.1 Context applicatieontwikkeling

Het belang en de risico's die de organisatie aan het bedrijfs- of beheerproces stelt, bepalen inherent de eisen die gesteld moeten worden aan de applicatie(s) die het betreffende proces ondersteunen. De risicobeoordeling van de functionaliteit, de gevoeligheid van de gegevens en het belang van de applicatie voor de organisatie bepalen welke normen van toepassing zijn.

Een applicatie kan worden verworven door interne ontwikkeling, uitbesteding of inkoop van een commercieel product. Dit kan ook door een combinatie van interne ontwikkeling en uitbesteding (zie afbeelding 1). Hierbij kan het voortraject (het specificeren) door de klant zelf worden verricht, terwijl het technische deel (het ontwikkelen) door de externe partij wordt uitgevoerd. Hierbij zullen extra afspraken over de beveiligingsaspecten gemaakt moeten worden.



Afbeelding 1: Overzicht typen applicaties

Gedurende de ontwikkelcyclus van de applicatie moet voldaan worden aan functionele en beveiligingseisen. Ook moeten bij de ontwikkeling het informatiebeveiligingsbeleid, wet- en regelgeving (onder andere de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG)) en eisen van de technische omgeving worden betrokken.

Om de voor applicatieontwikkeling relevante objecten en hun controls en maatregelen te kunnen identificeren en goed in context te kunnen plaatsen, is aangesloten bij de fasen van de ontwikkelcyclus. De beschrijving van deze fasen vindt plaats in paragraaf 1.4 Ontwikkelcyclus van applicatieontwikkeling.

1.2 Doel van dit document

Deze BIO Thema-uitwerking is opgesteld voor de interne en externe leverancier, als instrument gericht op de implementatie van applicaties in de technische omgeving van de leverancier of van de klant zelf.

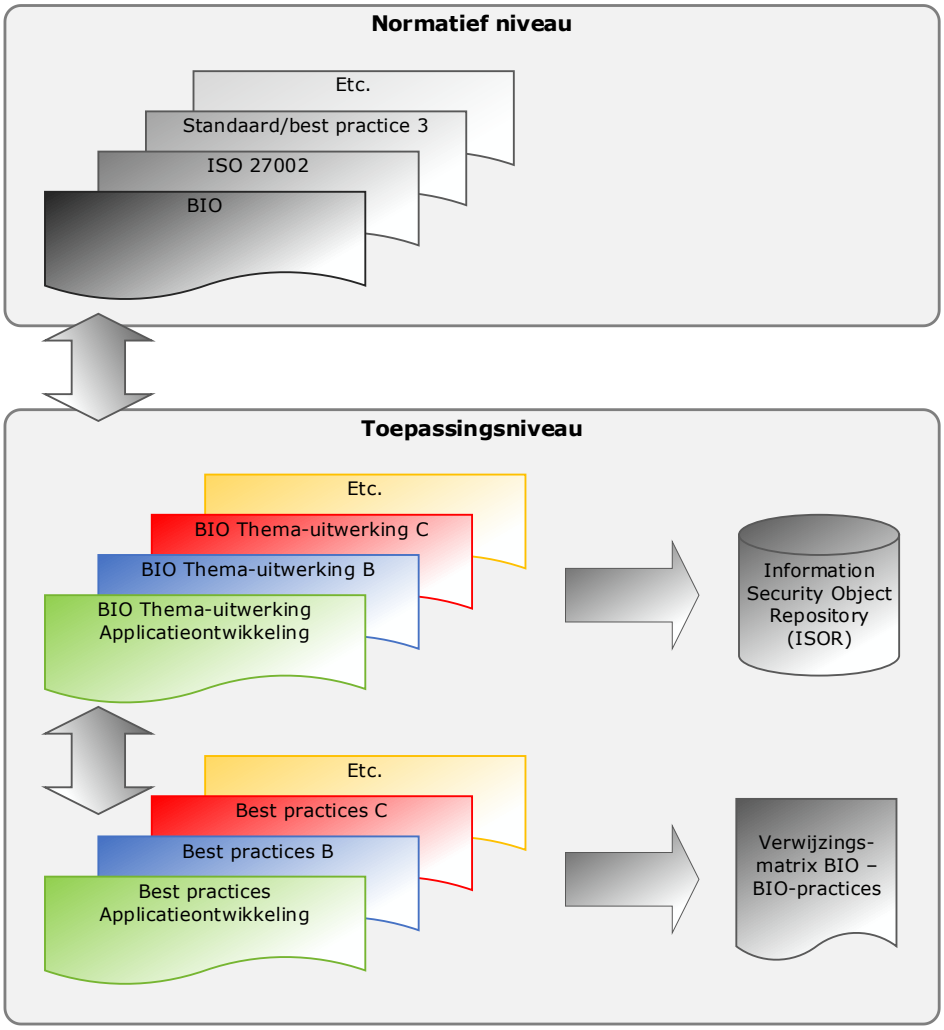
De thema-uitwerking geeft hiermee inzicht in de kwaliteitszorg die de leverancier dient toe te passen en in wat de klant kan verwachten bij het opleveren van nieuwe software. Het geeft tegelijkertijd de verplichte activiteiten weer van de klant. Hiernaast kan het als instrument dienen voor het geven van inzicht in het beveiligings- en beheersingsniveau van de ontwikkel- en onderhoudsorganisatie van de leverancier.

1.3 Scope en begrenzing applicatieontwikkeling

Deze BIO Thema-uitwerking behelst de conditionele beveiligings- en beheersingsaspecten die gerelateerd zijn aan het ontwikkelen van applicaties. Aan de volgende onderwerpen wordt geen aandacht besteed:

- activiteiten die gerelateerd zijn aan onderhoud van applicaties, webapplicaties en Enterprise Resource Planning (ERP)-pakketten (zie afbeelding 1);
- typen gebruikers en bedrijfseisen (deze zijn namelijk organisatieafhankelijk);
- toegangsbeveiligingsaspecten (deze zijn geadresseerd in de thema-uitwerking ‘Toegangsbeveiliging’).

De begrenzing van dit document is weergegeven in afbeelding 2.



Afbeelding 2: Relatie BIO Thema-uitwerking Applicatieontwikkeling met aanpalende documenten

1.4 Ontwikkelcyclus applicatieontwikkeling

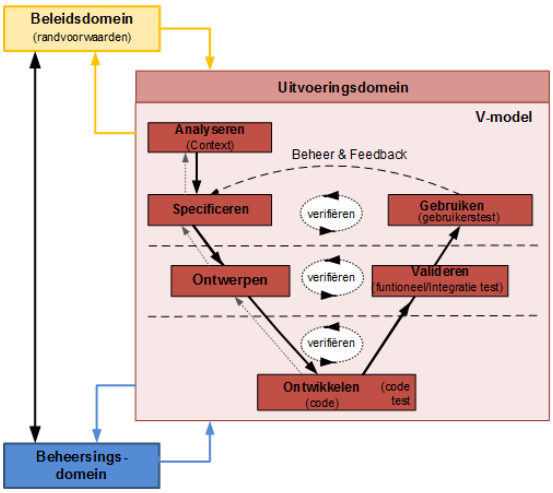
Een applicatie (software) wordt ontwikkeld om een (bedrijfs-)proces effectief te ondersteunen. Hiervoor dient eerst een contextanalyse te worden gemaakt om de juiste functionele vereisten te identificeren. De applicatie moet voldoen aan de behoeften van gebruikers en stakeholders in de vorm van wet- en regelgeving, eisen en requirements, ofwel een programma van eisen (PvE). Het PvE wordt ontwikkeld in samenwerking met informatieanalisten, softwareontwikkelaars en -gebruikers.

De kwaliteit en het succes van een applicatie wordt onder andere bepaald door de mate waarin:

- het PvE de gebruikerseisen en -wensen weerspiegelt;
- de gebruikerseisen en -wensen de reële situatie (daadwerkelijke noodzakelijkheden) weerspiegelen;
- de applicatie het vastgestelde PvE weerspiegelt.

Slechte kwaliteit van het PvE wordt onder andere veroorzaakt door onjuistheden, verkeerde aannames, inconsistenties, taalgebruik en ontoereikendheid. Bij applicatieontwikkeling is een goede inrichting van projectmanagement en de te hanteren systeem-ontwikkelmethode (System Development Life Cycle) essentieel.

Het applicatieontwikkelingsproces wordt verdeeld in activiteiten die niet noodzakelijk als sequentiële stappen doorlopen behoeven te worden[1] (zie ook paragraaf 1.5 Ontwikkelmethoden). De onderkende activiteiten zijn: analyseren, specificeren, ontwerpen, ontwikkelen, valideren, gebruiken en beheren. Afbeelding 3 geeft een schematische weergave van een ontwikkelproces in de vorm van het V-model. De activiteiten uit dit model worden in de volgende paragrafen toegelicht. Ze verschaffen mogelijkheden om de geïdentificeerde operationele objecten uit de BIO en overige best practices te rubriceren.



Afbeelding 3: Software-ontwikkelactiviteiten en indeling essentiële elementen in domeinen

Naast operationele elementen spelen ook essentiële randvoorwaardelijke en beheersingselementen een rol bij ontwikkel- en onderhoudsactiviteiten. De randvoorwaardelijke, operationele en beheersingselementen voor applicatieontwikkeling zijn daarom ingedeeld in het beleids-, uitvoerings- en control-domein. Ook deze indeling wordt weergegeven in afbeelding 3.

1.4.1 *Perspectieven*

De linkerkant van het bovenstaande V-model beschrijft het ontwikkelperspectief en de rechterkant het gebruikersperspectief. Als applicatieontwikkeling plaatsvindt bij een externe organisatie of een aparte businessunit zijn deze op perspectieven gescheiden. Afhankelijk van de afspraken tussen de klant en leverancier wordt bij uitbesteding de rechterkant aangeduid als het leveranciersperspectief en de linkerkant als het klantperspectief. Hierover maken de klant en leverancier heldere afspraken. De afspraken zijn gericht op:

[1] Bij Agile worden in ieder geval het ontwikkelen en een deel van het valideren als één activiteit uitgevoerd. Een deel van het ontwerpen kan daar ook bij horen. Ook wordt het andere deel van valideren en gebruiken wel gelijktijdig gedaan. Hiervoor zijn verschillende modellen bekend.

- het uitwisselen van kennis, specifiek over de overdracht van proceskennis van de (gebruiks-) organisatie naar de ontwikkelorganisatie;
- het tijdens het ontwikkelproces niet verstoren van het primaire proces;
- het toezien op de bescherming van intellectuele eigendommen en van gevoelige informatie.

De verantwoordelijken binnen het ontwikkelproces moeten verantwoording kunnen afleggen over de kwaliteit van het geleverde product. Voor een goede beheersing, is het vanuit best practices noodzakelijk de verschillende fasen van de levenscyclus te isoleren in een eigen omgeving zodat gegarandeerd kan worden dat het primaire proces niet wordt verstoord. Daarbij vindt een expliciete afsluiting van een fase plaats zodat een gecontroleerde overgang mogelijk wordt. Dit concept wordt een OTAP-straat genoemd. OTAP staat voor Ontwikkel, Test, Acceptatie en Productie.

1.4.2 *Analyseren*

In deze fase wordt het bedrijfsproces, dat door de te ontwikkelen applicatie ondersteund moet worden, geanalyseerd. Hierbij worden de noodzakelijke requirements, waaronder de bedrijfsfuncties, gegevens en veranderwensen vanuit de bedrijfsprocessen geïdentificeerd en vastgelegd. De focus ligt op de 'waarom'-aspecten. Onder andere de volgende activiteiten worden uitgevoerd:

- onderzoeken en brainstormen over de te ontwikkelen software om duidelijkheid te krijgen wat het doel is van de software;
- analyseren van eisen en wensen van gebruikers, beheerders en partners betreffende functionele en niet-functionele aspecten.

1.4.3 *Specificeren*

Deze activiteit richt zich op de 'wat'-aspecten. De business-, gebruikers-, stakeholders- (non)functionele en data-requirements worden gespecificeerd. Ook worden de noodzakelijke business rules en de noodzakelijke beperkingen in de vorm van constraints vastgelegd in een functioneel ontwerp.

1.4.4 *Ontwerpen*

Bij deze activiteit vindt de uitwerking plaats van de in eerdere fasen verkregen informatie. Deze fase richt zich op de relaties en afhankelijkheden tussen de te bouwen componenten. Hierbij worden de bedrijfs- en procesvereisten gemodelleerd in een ontwerp (architectuur) voor het te bouwen informatie(deel)systeem. Aandacht dient besteed te worden aan de kwaliteitseisen gerelateerd aan gebruikers, functionaliteit en beveiliging.

1.4.5 *Ontwikkelen (implementeren)*

In deze fase worden de softwarecomponenten geconstrueerd (gecodeerd). De relaties en afhankelijkheden van de te automatiseren processen en modules worden vastgelegd in een software-architectuur. Uiteindelijk zullen de programma's geschreven worden binnen het kader van deze (applicatie-/software-)architectuur. Hierbij moet ook rekening worden gehouden met enkele ontwikkeleisen, zoals:

- reproduceerbaarheid van code;

- effectieve testbaarheid;
- toepassing van externe programmabibliotheek;
- toepassing van tools en gebruik van licenties;
- toepassing van gestandaardiseerde vocabulaire (zie de NEN-ISO/IEC 25010 Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models);
- inzicht in relaties en afhankelijkheden tussen software-objecten;
- software-functies, waaronder interfaces, koppelingen en Application Programming Interfaces (API's);
- richten op aantoonbaar veilig programmeren.

1.4.6 *Valideren*

In deze fase worden de ontwikkelde modules/programma's getest en uiteindelijk geaccepteerd. Gecontroleerd wordt of de software volgens de ontwerprichtlijnen is gebouwd. Ook kunnen fouten, gemaakt in eerdere stadia, boven water komen. Er wordt aandacht besteed aan eisen als:

- de applicatie biedt slechts die functionaliteit die in de specificaties/het ontwerp zijn opgenomen (anders gezegd, geen functionaliteit buiten de specificaties/het ontwerp);
- er is conformiteit aan de gespecificeerde functionaliteit (gebruikerseisen en -wensen), het ontwerp (security by design) en de AVG (privacy by design).

1.4.7 *Gebruiken*

Als de software voltooid en getest is, zal het in gebruik worden genomen volgens een standaardprocedure van de OTAP-straat.

1.4.8 *Onderhouden en beheren*

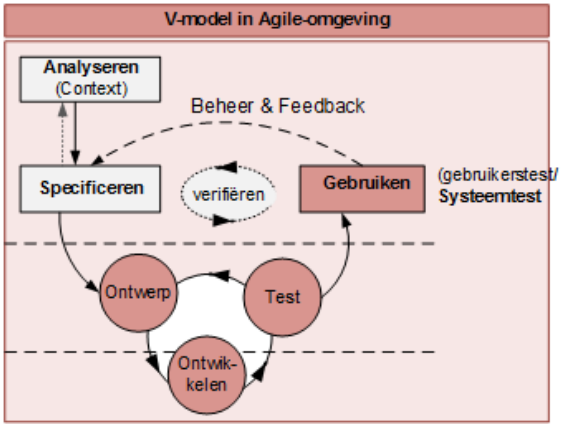
Tenslotte wordt de software periodiek onderhouden en (weer) in beheer genomen. Nieuwe functionele eisen zijn uitgewerkt en/of voorkomende fouten worden hersteld.

1.5 Ontwikkelmethoden

Er zijn verschillende modellen voor het ontwikkelen van applicaties. Hieronder de meest voorkomende:

- Lineaire methode
  Het meest bekende voorbeeld is de Watervalmethode (zie paragraaf 1.4 Ontwikkelcyclus van applicatieontwikkeling). In deze ontwikkelmethode wordt het eindproduct (softwareproduct) in een aantal fasen opgeleverd. In elke fase wordt een concreet gedefinieerd deelproduct uitgevoerd. De requirements zijn duidelijk en vooraf vastgelegd. Kennisoverdracht en monitoring vinden plaats met specifieke documenten en formats.
- Iteratieve methode
  De iteratieve ontwikkeling is een methode waarbij het eindproduct niet in één keer wordt opgeleverd, maar gefaseerd tot stand komt, waarbij fasen herhaaldelijk worden doorlopen. Na elke zogenaamde iteratie wordt het proces geëvalueerd en zo nodig aangepast. In de praktijk worden de iteratieve en lineaire ontwikkelmethode met elkaar gecombineerd.

- Agile-methode
  De Agile-methode wordt gekenmerkt door korte, in tijd gelimiteerde sprints. De inhoud van een sprint wordt bij de start ervan bepaald. De gevolgde werkwijze kan (dagelijks) worden aangepast al naar gelang de wensen van de zelfsturende teams. Er wordt gebruik gemaakt van een geordende lijst van productfuncties die gedurende het gehele project wordt bijgewerkt op basis van de behoefte van de klant. Daarmee worden in feite de productspecificaties opgebouwd. De nadruk ligt op samenwerking en mondelinge kennisoverdracht. De prioriteit ligt bij het opleveren van sprints en producten met de op dat moment hoogste toegevoegde waarde. De sprints worden gedaan door zelfsturende teams met multidisciplinaire teamleden en zonder vastgelegde taken, rollen en verantwoordelijkheden. Afbeelding 4 geeft een schematische weergave van een iteratie-/Agile-ontwikkelproces met het V-model.



Afbeelding 4: Schematische weergave iteratie-/Agile-ontwikkelproces met het V-model

1.6 Applicatieobjecten in relatie tot ontwikkelmethode

Bij de selectie van applicatieobjecten uit de BIO en overige best practices is in eerste instantie uitgegaan van de lineaire/iteratieve aanpak van applicatieontwikkeling. Ook in de onderhoudsfase en in Agile werkmethoden zijn de in dit document geïdentificeerde objecten, controls en maatregelen relevant. Het borgen van de toepassing ervan in de applicatie is daarin lastiger vanwege het ontbreken van de natuurlijke faseovergangen van de lineaire aanpak. Met name geldt dit bij Agile ontwikkeling.

2 Beveiligingsobjecten applicatieontwikkeling

Bij de vaststelling van de objecten die een rol spelen bij applicatieontwikkeling zijn de verschillende ontwikkelfasen als referentiekader gebruikt. Aan de hand van drie onderzoeksvragen die vanuit de optiek van de BIVC-criteria (Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid) gesteld zijn, zijn de objecten afgeleid en ingedeeld in het beleids-, uitvoerings- en control-domein.

De vragen die hierbij een rol spelen, zijn:

- Welke elementen spelen vanuit de optiek van BIVC een rol bij de conditionering en sturing op applicatieontwikkeling en wat is de consequentie bij afwezigheid hiervan?
- Welke elementen spelen vanuit de optiek van BIVC een rol bij de uitvoering van applicatieontwikkeling en wat is de consequentie bij afwezigheid hiervan?
- Welke elementen spelen vanuit de optiek van BIVC een rol bij de beheersing van applicatieontwikkeling en wat is de consequentie bij afwezigheid hiervan?

2.1 Organisatie van applicatieontwikkelingsobjecten

Zoals in paragraaf 1.4 Ontwikkelcyclus van applicatieontwikkeling is aangegeven, worden de geïdentificeerde applicatieontwikkelingsobjecten met het beleids-, uitvoerings- en control-domein georganiseerd. Hiermee worden deze aspecten in de juiste context gepositioneerd. De betekenis die aan elk domein wordt toegekend, is:

1. Beleid
   Binnen dit domein bevinden zich conditionele elementen voor applicatieontwikkeling. Hier zijn eisen opgenomen over 'geboden' en 'verboden', zoals het applicatiebeveiligingsbeleid, de te hanteren wet- en regelgeving en andere vormen van reguleringen en beperkingen.
2. Uitvoering
   Binnen dit domein bevinden zich:
   - elementen die gerelateerd zijn aan de operationele ontwikkelactiviteiten van applicaties;
   - elementen die aangeven hoe deze activiteiten georganiseerd moeten zijn;
   - elementen die gerelateerd zijn aan beveiligingsaspecten die bij de activiteiten in acht moeten worden genomen.
3. Control
   Binnen dit domein bevinden zich elementen die zorgdragen voor de beheersing van het ontwikkelproces.

2.2 Observatie bij objectidentificatie

In de BIO2 en de ISO 27002 zijn weinig controls te vinden die direct gerelateerd zijn aan de ontwikkelfasen: analyseren, specificeren, ontwerpen en ontwikkelen. Bij de ISO-norm is niet uitgegaan van de ontwikkelfasen van systeemontwikkeling. Wel bevat de ISO 27002 beveiligingscontrols en bijbehorende maatregelen die indirect te maken hebben met de ontwikkelfasen.

2.3 Objecten geprojecteerd op domein en gesorteerd naar invalshoek

Bijlage 1 Objecten ingedeeld naar invalshoeken geeft een overzicht van de applicatieontwikkelingsobjecten die in hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein zijn uitgewerkt. Met behulp van diverse baselines is een lijst van relevante objecten samengesteld. Daarnaast zijn nog enkele extra objecten als relevant voor dit thema toegevoegd.

Deze 'baseline-benadering' zorgt ervoor dat deze thema-uitwerking niet exclusief is voor de lineaire ontwikkelmethode, maar ook gehanteerd kan worden in de onderhoudsfase en bij agile ontwikkelmethoden.

Uit de inhoudelijke bestudering van de objecten vanuit de baseline-gebaseerde benadering komt naar voren dat er doublures in de objecten zijn. Met andere woorden het aantreffen van twee verschillende objecten die dezelfde inhoud kennen. Sommige objecten zijn vooralsnog bewust achterwege gelaten vanwege het geringe belang van deze objecten in relatie tot de totale scope.

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein van applicatieontwikkeling is om vast te stellen of afdoende randvoorwaarden en condities binnen de ontwikkelorganisatie zijn gecreëerd om applicaties adequaat te kunnen ontwikkelen.

In dit domein zijn objecten en daaraan gerelateerde controls en maatregelen opgenomen die het mogelijk maken de applicaties op een veilige manier te ontwikkelen.

3.2 Risico's

Wanneer de juiste beleidsaspecten voor het ontwikkelen van applicaties ontbreken, is het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van een applicatie. Dit zal een negatieve impact hebben op het bereiken van doelstellingen waarvoor de applicatie is ontworpen en ingericht.

3.3 Objecten, controls en maatregelen

Tabel 1 toont de objecten die specifiek voor dit domein een rol spelen. Het geeft een overzicht en de ordening van objecten naar de invalshoeken: Intentie, Functie, Gedrag of Structuur. De geel gemarkeerde objecten komen voor in de BIO2. De wit gemarkeerde objecten zijn betrokken uit andere best practices. Voor de identificatie van de objecten en de ordening is gebruik gemaakt van basiselementen (zie de tekst tussen haken).

Intentie	Functie	Gedrag	Structuur
B.01 Beleid voor (beveiligd) ontwikkelen ((Operationeel) beleid)	B.07 Kwaliteitsmanagement-systeem (Proces)	B.08 Toegangsbeveiliging op programmacode (Verbinding (koppeling/interactie))	B.09 Projectorganisatie (bedrijfsorganisatie-structuur)
B.02 Systeem-ontwikkelmethode ((Operationeel) beleid)	/	/	/
B.03 Classificatie van informatie ((Operationeel) beleid)	/	/	/
B.04 Veilige systeemarchitectuur en technische uitgangspunten ((Operationeel) beleid)	/	/	/
B.05 Uitbestede systeemontwikkeling ((Operationeel) beleid)	/	/	/
B.06 Privacy en bescherming persoonsgegevens (Assessment)	/	/	/

Tabel 1: Beleidsobjecten met basiselementen voor applicatieontwikkeling per invalshoek

3.3.1 *B.01 Beleid voor (beveiligd) ontwikkelen*

Objectdefinitie

Resultaat van een besluitvorming over welke regels en protocollen gehanteerd moeten worden om software en systemen te beveiligen tijdens de ontwikkelcyclus.

Objecttoelichting

De ISO 27002 2022, artikel 8.25 formuleert 'Beveiligd ontwikkelen' als een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem.

In deze BIO Thema-uitwerking wordt bij het object 'Beleid voor (beveiligd) ontwikkelen' aan applicatieontwikkelingsbeleid gerelateerde specifieke aspecten benadrukt. In zo'n beleid worden onder andere methoden en technieken voor requirementsanalyse en -richtlijnen voor beveiliging in de levenscyclus van softwareontwikkeling besproken.

Doelstelling	Bewerkstelligen dat informatiebeveiliging binnen de veilige ontwikkelcyclus van software en systemen wordt ontworpen en geïmplementeerd.		
Risico	Als geen samenhangend en vastgesteld beleid voor beveiligd ontwikkelen bestaat of dit onvoldoende richtinggevend is, bestaat het risico dat informatiebeveiliging niet structureel en consistent wordt meegenomen in de ontwikkelcyclus van software en systemen, waardoor beveiliging ad-hoc wordt toegepast en kwetsbaarheden ontstaan die pas laat of niet worden onderkend.		
Control	Voor het veilig ontwikkelen van software en systemen behoren **regels** te worden vastgesteld en toegepast.		ISO 27002:2022: 8.25
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	In het beleid voor beveiligd ontwikkelen zijn onder meer opgenomen: • scheiding van ontwikkel-, test- en productieomgevingen; • beveiligingseisen in de SDLC; • beveiligingseisen in specificatie- en ontwerpfase; • beveiligingscontrolepunten in projecten; • beveiligingstesten (regressietests, codescans en penetratietests); • beveiligde bewaarplaatsen en versiebeheer voor broncode en configuraties; • vereiste kennis, opleiding en vermogen van ontwikkelaars om kwetsbaarheden te voorkomen, detecteren en oplossen alsmede licentie-eisen en alternatieven.	ISO 27002:2022: 8.25
	2.	Bij uitbesteding van ontwikkelactiviteiten wordt gewaarborgd dat de leverancier voldoet aan de vastgestelde regels voor beveiligd ontwikkelen.	ISO 27002:2022: 8.25

3.3.2 *B.02 Systeem-ontwikkelmethode*

Objectdefinitie

Gestructureerde manier van handelen voor het ontwikkelen van applicaties.

Objecttoelichting

Ontwikkel- en onderhoudsactiviteiten worden uitgevoerd met een systeem-ontwikkelmethode. Hierdoor wordt rekening gehouden met:

- vereisten uit wet- en regelgeving;
- contractuele vereisten;
- beveiligingsvereisten;
- projectmatige aanpak.

Doelstelling	Ervoor zorgen dat applicaties die ontwikkeling worden, voldoen aan alle eisen/vereisten.		
Risico	Als geen consistente en toegepaste systeem-ontwikkelmethode wordt gehanteerd, bestaat het risico dat tijdens de ontwikkeling relevante eisen uit wet- en regelgeving, beveiliging en business niet structureel worden meegenomen, waardoor applicaties in gebruik worden genomen die niet voldoen aan gestelde vereisten en achteraf moeten worden hersteld of beperkt inzetbaar zijn.		
Control	Ontwikkelactiviteiten behoren te zijn gebaseerd op een gedocumenteerde **systeem-ontwikkelmethode**, waarin onder andere **standaarden en procedures** voor de applicatieontwikkeling, het toepassen van **beleid en wet- en regelgeving** en een **projectmatige aanpak** zijn geadresseerd.		SoGP 2018: SD 1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Systeem-ontwikkel-methode	1.	Een formeel vastgestelde ontwikkelmethodologie wordt toegepast.	SoGP 2018: SD 1.1.1
	2.	Softwareontwikkelaars zijn getraind om de ontwikkelmethodologie toe te passen.	SoGP 2018: SD 1.1.7
	3.	Adoptie van ontwikkelmethodologie wordt gemonitord.	SoGP 2018: SD 1.1.9
Standaarden en procedures	4.	Standaarden en procedures worden toegepast voor: • het specificeren van requirements; • het ontwikkelen, bouwen en testen; • de overdracht van de ontwikkelde applicatie naar de productie-omgeving; • de training van softwareontwikkelaars.	SoGP 2018: SD 1.1.2
Beleid en wet- en regelgeving	5.	De systeem-ontwikkelmethode ondersteunt de vereiste dat te ontwikkelen applicaties voldoen aan: • de eisen uit wet- en regelgeving inclusief privacy; • de contactuele eisen; • het informatiebeveiligingsbeleid van de organisatie; • de specifieke beveiligingseisen vanuit de business; • het classificatiemodel van de organisatie.	SoGP 2018: SD 1.1.3

Projectmatige aanpak	6.	Het ontwikkelen van een applicatie wordt projectmatig aangepakt. Hierbij wordt onder andere aandacht besteed aan: • het melden van de start van het project bij de verantwoordelijke voor de beveiligingsfunctie; • het gebruik van een classificatiemodel; • het toepassen van een assessment voor beschikbaarheid; • integriteit, vertrouwelijkheid en controleerbaarheid; • het creëren van een risicoregister; • het registreren van belangrijke details in een bedrijfsapplicatieregister.	SoGP 2018: SD 1.1.6

3.3.3 *B.03 Classificatie van informatie*

Objectdefinitie

Systematische indeling in categorieën van de waarde van informatie, ter bepaling van het niveau van bescherming dat de te ontwikkelen applicatie nodig heeft.

Objecttoelichting

In ISO 27002 2022 is gesteld dat een organisatie haar informatie moet classificeren om ervoor te zorgen dat informatie een passend beschermingsniveau krijgt. Hiervoor moet de organisatie een classificatieschema opstellen en dit schema communiceren binnen de organisatie. Een classificatieschema geeft beveiligingsrichtlijnen voor zowel algemene informatiemiddelen als voor informatie in het ontwikkeltraject. In het ontwikkeltraject en bij de hantering van deze thema-uitwerking moet de projectverantwoordelijke dit classificatieschema als input beschikbaar hebben. Het classificatieschema biedt specifieke richtlijnen voor het ontwikkeltraject.

Doelstelling	Het inzichtelijk maken welke mate van bescherming de informatie nodig heeft.	
Risico	Als informatie tijdens het ontwikkeltraject niet correct en consequent wordt geclassificeerd, bestaat het risico dat applicaties worden ontwikkeld met een beveiligingsniveau dat niet aansluit bij de waarde en gevoeligheid van de informatie, waardoor informatie onvoldoende wordt beschermd of onnodig zwaar wordt beveiligd, met verhoogde beveiligingsrisico's of ondoelmatige inzet van middelen tot gevolg.	
Control	**Informatie** behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	ISO 27002:2022: 5.12
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Informatie	1.	In het beleid voor informatieclassificatie zijn onder meer opgenomen: • een classificatieschema dat expliciet rekening houdt met de eisen op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid; • duidelijke classificatiecriteria, gebaseerd op bedrijfsbehoeften rondom het delen of beperken van informatie, de bescherming van beschikbaarheid, integriteit en vertrouwelijkheid, en de potentiële impact bij compromittering; • de verantwoordelijkheid van informatie-eigenaren voor het toepassen van de classificatie; • regels voor het classificeren, het periodiek herbeoordelen en het actualiseren van classificaties gedurende de gehele levenscyclus van informatie; • afstemming met het beleid voor toegangsbeveiliging.	ISO 27002:2022: 5.12
	2.	In het classificatieschema wordt rekening gehouden met de verplichtingen uit wet- en regelgevingen (onder andere privacy).	ISO 27002:2022: 5.12
	3.	Informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde impact en classificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.	BIO2: 5.12.01

3.3.4 *B.04 Veilige systeemarchitectuur en technische uitgangspunten*

Objectdefinitie

Regel, norm of beginsel voor 'goed gedrag', specifiek voor het ontwikkelen van software en systemen die beveiligd moeten worden.

Objecttoelichting

Bij het ontwikkelen van software en systemen worden engineeringsprincipes in acht genomen. In de BIO is het principe security by design expliciet genoemd. In de ISO 27033-2 2012 is het principe defence in depth expliciet genoemd. Hiernaast bestaan nog verschillende andere van belang zijnde (engineerings)principes die in andere baselines zijn opgenomen.

Doelstelling	Waarborgen dat informatiesystemen veilig worden ontworpen, geïmplementeerd en beheerd binnen de ontwikkelingslevenscyclus.	
Risico	Als bij het ontwerpen en ontwikkelen van software en systemen geen consistente veilige architectuurprincipes en technische uitgangspunten worden toegepast, bestaat het risico dat informatiebeveiligingsmaatregelen niet effectief zijn ingebed in het systeemontwerp, waardoor structurele kwetsbaarheden ontstaan die tijdens beheer en gebruik moeilijk of kostbaar te corrigeren zijn.	
Control	**Uitgangspunten** voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	ISO 27002:2022: 8.27
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Uitgangspunten	1.	Architectuurprincipes zoals 'security by design' en 'security by default' voor het ontwerpen van beveiliging van informatiesystemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten over het ontwikkelen van informatiesystemen.	BIO2: 8.27.01 ISO 27002:2022: 8.27
	2.	Voor het beveiligen van informatiesystemen zijn de volgende principes van belang: • defence in depth (beveiliging op verschillende lagen); • secure by default; • default deny; • fail secure; • input van externe applicaties wantrouwen; • secure in deployment; • bruikbaarheid en beheersbaarheid.	SoGP 2018: SD2.1.6 SoGP 2018: SD2.2.7
	3.	Beveiliging wordt als een integraal onderdeel van systeemontwikkeling behandeld.	NIST SP 800-160 Vol 1. 2016: 2.1
	4.	Ontwikkelaars zijn getraind om veilige software te ontwikkelen.	NIST SP 800-27 Rev. A 2004: 3.3.1

3.3.5 *B.05 Uitbestede systeemontwikkeling*

Objectdefinitie

De organisatie waarborgt dat informatiebeveiligingseisen worden toegepast op uitbestede systeemontwikkelingsactiviteiten en dat deze activiteiten voldoen aan de eigen beveiligingsrichtlijnen voor ontwikkeling.

Objecttoelichting

Bij uitbesteding van systeemontwikkelingsactiviteiten (zoals softwareontwikkeling, applicatieontwikkeling of systeemintegratie) blijft de organisatie verantwoordelijk voor de beveiliging van de te ontwikkelen systemen en de daarin verwerkte informatie. De organisatie dient in contracten en overeenkomsten met externe leveranciers expliciet beveiligingseisen op te nemen die aansluiten bij de interne richtlijnen voor beveiligd ontwikkelen.

Doelstelling	Garanderen dat de door de organisatie vereiste informatiebeveiligingsmaatregelen bij uitbestede systeemontwikkeling worden geïmplementeerd.	
Risico	Als bij uitbestede systeemontwikkeling onvoldoende wordt geborgd dat externe leveranciers informatiebeveiligingseisen conform de eigen richtlijnen toepassen, bestaat het risico dat de organisatie de controle over informatiebeveiliging verliest, waardoor kwetsbaarheden, beveiligingslekken, privacy-schendingen of continuïteitsproblemen in de opgeleverde systemen en software ontstaan.	
Control	De organisatie behoort de activiteiten in verband met **uitbestede systeemontwikkeling** te sturen, bewaken en beoordelen.	ISO 27002:2022: 8.30
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Uitbestede systeemontwikkeling	1.	Interne maatregelen voor systeemontwikkeling zijn onverkort van toepassing op uitbestede ontwikkeling, aangevuld met maatregelen die volgen vanuit uitbestedingen.	BIO2: 8.30.01
	2.	Bij uitbesteding van systeemontwikkeling worden de eisen en verwachtingen gecommuniceerd en overeengekomen. Het uitbestede werk wordt voortdurend gemonitord en beoordeeld om te waarborgen dat aan de verwachtingen wordt voldaan.	ISO 27002:2022: 8.30
	3.	Voor de gehele externe toeleveringsketen worden de volgende punten overwogen: • eisen rondom licentieovereenkomsten, eigendom van broncode en intellectuele-eigendomsrechten; • contractuele verplichtingen voor beveiligde ontwikkel-, coderings- en testpraktijken; • het verstrekken van een relevant dreigingsmodel aan externe ontwikkelaars; • acceptatietests voor kwaliteit, nauwkeurigheid en beveiliging van leveringen; • het eisen van bewijs dat beveiligings- en privacycapaciteiten voldoen aan een minimaal aanvaardbaar niveau (bijv. via borgingsverslagen); • het eisen van bewijs dat voldoende tests zijn uitgevoerd ter voorkoming van kwaadaardige inhoud en bekende kwetsbaarheden; • escrowovereenkomsten voor broncode bij continuïteitsrisico's; • het contractuele recht om ontwikkelprocessen en beheersmaatregelen te auditen; • beveiligingseisen voor de ontwikkelomgeving van de leverancier; • naleving van toepasselijke wet- en regelgeving, waaronder bescherming van persoonsgegevens.	ISO 27002:2022: 8.30

3.3.6 *B.06 Privacy en bescherming persoonsgegevens*

Objectdefinitie

Privacy betreft de persoonlijke levenssfeer, privésfeer of eigenruimte; de afscherming van personen of groepen voor bespieding en beïnvloeding. Bescherming persoonsgegevens draagt bij aan het voorkomen van inbreuken op de persoonlijke levenssfeer.

Objecttoelichting

Bij applicatieontwikkeling behoort de verantwoordelijke stakeholder rekening te houden met privacy en de bescherming van persoonsgegevens. Een analyse van de context waarin de desbetreffende applicatie ontwikkeld wordt, kan risico's voor inbreuken op de privacy blootleggen. Verder zal voorafgaand aan het ontwerp van de applicatie een PIA worden uitgevoerd voor waarschijnlijk hoog-risicoverwerkingen. Deze verplichting komt voort uit de AVG.

Doelstelling	Het reduceren van privacy-risico's voor de betrokkenen en het vermijden van schade die kan voortvloeien uit het niet nakomen van wet- en regelgeving betreffende de bescherming van persoonsgegevens.

Risico	Als bij applicatieontwikkeling onvoldoende rekening wordt gehouden met privacybescherming en de vereisten voor verwerking van persoonsgegevens, bestaat het risico dat persoonsgegevens ongeoorloofd of onbedoeld worden ingezien, gewijzigd, verloren, vernietigd of verstrekt, waardoor betrokkenen schade ondervinden en de organisatie niet voldoet aan wettelijke verplichtingen.		
Control	Bij het ontwikkelen van applicaties behoren de eisen met betrekking tot het behoud van **privacy en de bescherming van persoonsgegevens** volgens de toepasselijke **wet- en regelgeving** en contractuele eisen te identificeren en eraan te voldoen.		ISO 27002:2022: 5.34
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Privacy en bescherming van persoons-gegevens	1.	Om privacy en gegevensbeschermingsmaatregelen vooraf in het ontwerp mee te nemen, is een PIA uitgevoerd.	CIP De Privacy Baseline 2020: 03.01 toelichting
	2.	Voor het uitvoeren van een PIA en voor het opvolgen van de uitkomsten is een procesbeschrijving aanwezig.	CIP De Privacy Baseline 2020: 03.02
	3.	Een tot standaard verheven PIA-toetsmodel wordt toegepast. Dit model voldoet aan de in de AVG gestelde eisen.	CIP De Privacy Baseline 2020: 03.04
	4.	Privacy by design en de PIA maken onderdeel uit van een tot standaard verheven risicomanagementaanpak.	CIP De Privacy Baseline 2020: 03.05
	5.	De risicomanagementaanpak wordt aantoonbaar toegepast, bijvoorbeeld door in de vorm van een plan van aanpak aantoonbaar opvolging te geven aan de aanbevelingen/verbetervoorstellen.	CIP De Privacy Baseline 2020: 03.03
Wet- en regelgeving	6.	Volgens de AVG worden bij het ontwerp/ontwikkelen van applicaties de principes privacy by design en privacy by default gehanteerd.	De CIP Privacy Baseline 2020: 02.02

3.3.7 *B.07 Kwaliteitsmanagementsysteem*

Objectdefinitie

Samenhangend geheel van organisatiestructuren, bevoegdheden, verantwoordelijkheden, procedures, processen, voorzieningen en middelen dat nodig is voor het realiseren van de resultaten binnen de gewenste kwaliteitscriteria.

Objecttoelichting

De organisatie heeft de ontwikkelactiviteiten procesmatig ingericht en voert ook de noodzakelijke kwaliteitscontroles uit.

Doelstelling	Het zorgen dat applicatieontwikkeling en -onderhoud wordt uitgevoerd en beheerst op het juiste kwaliteitsniveau.
Risico	Als applicatieontwikkeling en -onderhoud niet structureel worden uitgevoerd en beheerst binnen een samenhangend kwaliteitsmanagementsysteem, bestaat het risico dat het kwaliteitsniveau onvoldoende aansluit op de gestelde eisen en behoeften, waardoor applicaties tekortschieten in betrouwbaarheid en beheersbaarheid of juist onnodig zwaar en inefficiënt worden ingericht.

Control	De doelorganisatie behoort volgens een uitgestippeld **ontwikkel- en onderhoudsbeleid** een **kwaliteitsmanagementsysteem** in te richten, dat ervoor zorgt dat applicatieontwikkeling en -onderhoud wordt uitgevoerd en beheerst.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Ontwikkel- en onderhouds-beleid	1.	De doelorganisatie beschikt over een ontwikkel- en onderhoudsbeleid.	ISO 27002:2022 8.25 CIP-netwerk
	2.	De doelorganisatie beschikt over een quality assurance-methodiek en Quality Security Management-methodiek.	CIP-netwerk
Kwaliteits-management-systeem	3.	De ontwikkel- en onderhoudsactiviteiten worden in samenhang georganiseerd en geïmplementeerd.	CIP-netwerk
	4.	Er zijn informatie- en communicatieprocessen ingericht.	CIP-netwerk
	5.	Op de ontwikkel- en onderhoudsactiviteiten worden kwaliteitsmetingen en inspecties uitgevoerd.	CIP-netwerk
	6.	Aan het management worden evaluatierapportages verstrekt.	CIP-netwerk
	7.	De processen voor de inrichting van de applicatieontwikkeling en het -onderhoud (impactanalyse, ontwerp, realisatietesten en beheer) zijn beschreven en maken onderdeel uit van het kwaliteitsmanagementsysteem.	CIP-netwerk

3.3.8 *B.08 Toegangsbeveiliging op programmacode*

Objectdefinitie

Geautoriseerde toegang tot gevalideerde broncode[2] (source code) van applicaties.

Objecttoelichting

Toegang tot de programmacode en samenhangende elementen, zoals ontwerpen, specificaties, verificatie- en validatieschema's is ingericht om zowel ongeautoriseerde functionaliteit als ongeautoriseerde wijzigingen te voorkomen en om de vertrouwelijkheid van intellectueel eigendom te waarborgen.

Doelstelling	Het zorgen dat alleen die personen die toegang nodig hebben voor het uitvoeren van hun werkzaamheden toegang krijgen tot de programma-broncodebibliotheken en samenhangende elementen.
Risico	Als toegang tot programmacode en bijbehorende artefacten niet strikt wordt beperkt tot geautoriseerde personen, bestaat het risico dat onbevoegden inzage krijgen in of wijzigingen aanbrengen in de broncode, waardoor ongeautoriseerde functionaliteit kan worden geïntroduceerd en de vertrouwelijkheid en integriteit van applicaties en intellectueel eigendom worden aangetast.

[2] De broncode is de gevalideerde en in de broncodebibliotheek opgeslagen programmacode.

Control	Lees- en schrijftoegang tot **broncode, ontwikkelinstrumenten en softwarebibliotheken** behoren op passende wijze te worden beheerd.		ISO 27002:2022: 8.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Broncode, ontwikkelinstrumenten en softwarebibliotheken	1.	In het beleid voor beveiligd ontwikkelen is opgenomen dat toegang tot broncode, gerelateerde documenten (zoals ontwerpen, specificaties, verificatie- en validatieplannen) en ontwikkelinstrumenten (zoals compilers, builders, integratie-instrumenten en testomgevingen) streng wordt beheerst op basis van bedrijfsbehoeften en rollen, waarbij leestoegang breder kan worden verleend dan schrijftoegang, en schrijftoegang wordt voorbehouden aan aangewezen personeel.	ISO 27002:2022: 8.4
	2.	Bij het beheer van broncode, ontwikkelinstrumenten en softwarebibliotheken worden de volgende richtlijnen in overweging genomen: • broncode wordt centraal opgeslagen in een broncodebeheersysteem; • wijzigingsbeheerprocedures worden toegepast op het bijwerken van broncode en op het verlenen van toegang tot broncode; • ontwikkelaars krijgen geen directe toegang tot de broncode, maar werken uitsluitend via gecontroleerde ontwikkelinstrumenten die activiteiten en autorisaties beheersen; • lijsten van programma's worden bewaard in een beveiligde omgeving waarin lees- en schrijftoegang op passende wijze worden beheerd en toegewezen; • een auditlog wordt bijgehouden van alle toegangspogingen tot en alle wijzigingen aan de broncode; wanneer broncode wordt gepubliceerd, worden aanvullende beheersmaatregelen zoals een digitale handtekening overwogen die bijdragen aan het waarborgen van de integriteit ervan.	ISO 27002:2022: 8.4

3.3.9 *B.09 Projectorganisatie*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen die verantwoordelijk zijn voor projectmatige softwareontwikkeling.

Objecttoelichting

Binnen de (project-)organisatie is een functionaris betrokken die verantwoordelijkheid draagt voor de beveiliging van de te ontwikkelen applicatie. Binnen het project ziet hij toe op het vervaardigen en hanteren van beveiligingsvoorschriften. De taken, verantwoordelijkheden en bevoegdheden van de beveiligingsfunctionaris zijn vooraf expliciet benoemd en vastgesteld. De beveiligingsfunctionaris ziet toe op het naleven van het informatiebeveiligingsbeleid en de architectuurvoorschriften, alsmede de rapportage daarover.

Doelstelling	Het ondersteunen van de (project-)organisatie bij informatiebeveiliging in het applicatie-ontwikkeltraject.

Risico	Indien binnen projectmatige softwareontwikkeling geen expliciet aangewezen en geborgde verantwoordelijkheid bestaat voor informatiebeveiliging, bestaat het risico dat beveiligingseisen niet of onvoldoende worden meegenomen in ontwerp, uitvoering en besluitvorming. Hierdoor kunnen kwetsbaarheden ontstaan die pas na oplevering worden ontdekt, met verhoogde kans op beveiligingsincidenten, herstelkosten en niet-naleving van beleid en wetgeving.		
Control	Binnen de (project-)organisatie behoort een **beveiligingsfunctionaris** te zijn benoemd die het systeem-ontwikkeltraject ondersteunt in de vorm van het bewaken van **beveiligingsvoorschriften** en die inzicht verschaft in de samenstelling van het applicatielandschap.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-functionaris	1.	De beveiligingsfunctionaris zorgt onder andere voor: • de actualisatie van beveiligingsbeleid; • een afstemming van het beveiligingsbeleid met de afgesloten overeenkomsten met onder andere de ketenpartijen; • de evaluatie van de effectiviteit van de beveiliging van de ontwikkelde systemen; • de evaluatie van de beveiligingsmaatregelen ten aanzien van de bestaande risico's; • de bespreking van beveiligingsissues met ketenpartijen.	SoGP 2018: SG1.2.2a
Beveiligings-voorschriften	2.	De beveiligingsfunctionaris geeft onder andere inzicht in: • het beheer en integratie van ontwikkel- en onderhoudsvoorschriften (procedureel en technisch); • specifieke beveiligings- en architectuurvoorschriften; • afhankelijkheden tussen informatiesystemen.	CIP-netwerk

4 Uitvoeringsdomein

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein van applicatieontwikkeling is het zorgen dat de ontwikkel- en onderhoudsactiviteiten plaatsvinden volgens specifieke beleidsuitgangspunten en dat de werking van de applicatie voldoet aan de eisen die door de klant (doelorganisatie) zijn gesteld. Met randvoorwaarden in de vorm van beleid geeft de organisatie kaders aan waarbinnen de ontwikkel- en onderhoudsactiviteiten moeten plaatsvinden.

4.2 Risico's

Wanneer adequate normen voor applicatieontwikkeling en onderhoud ontbreken, is het risico dat deze activiteiten ongecontroleerd plaatsvinden en/of dat het eindproduct niet voldoet aan het juiste beveiligingsniveau. Het ontbreken van richtlijnen en procedures voor het werken binnen de verschillende (OTAP-)omgevingen vergroot de kans op foutieve software in de productieomgeving, met het risico op aantasting van productiegegevens.

4.3 Objecten, controls en maatregelen

Binnen het uitvoeringsdomein worden specifieke inrichtings- en beveiligingsobjecten voor applicatieontwikkeling beschreven. Elk object wordt vervolgens uitgewerkt in een control en conformiteitsindicatoren. De rode gemarkeerde objecten komen voor in de BIO. De wit gemarkeerde objecten zijn betrokken uit andere best practices, zie tabel 2. De objecten zijn ingedeeld naar de invalshoeken: intentie, functie, gedrag en structuur. In bijlage 2 Invalshoeken gekoppeld aan het V-model zijn deze gekoppeld aan het V-model.

Intentie	Functie	Gedrag	Structuur
U.01 Wijzigingsbeheerprocedure voor applicaties en systemen ((Operationeel) beleid)	U.04 Analyse en specificatie informatiesysteem (Proces)	**U.11 Beveiligde ontwikkelomgeving (Omgeving)**	U.14 Applicatie-architectuur (IT-architectuur)
U.02 Beperking software-installatie ((Operationeel) beleid)	**U.05 Informatiebeveiliging in projectmangement (Proces)**	U.12 Applicatiekoppeling (Verbinding (koppeling/interactie))	U.15 Tooling ontwikkelmethode (Faciliteit)
U.03 Richtlijn programmacode ((Operationeel) beleid)	U.06 Applicatie-ontwerp (Proces)	**U.13 Logging en monitoring (Event/historie)**	/
/	U.07 Applicatiefunctionaliteit (In-/outputfunctie)	/	/
/	U.08 Applicatiebouw (Proces)	/	/
/	**U.09 Systeemacceptatietest (Proces)**	/	/
/	**U.10 Scheiding van ontwikkel-, test- en productieomgevingen (Beschermingsfunctie)**	/	/

Tabel 2: Uitvoeringsobjecten met basiselementen voor applicatieontwikkeling per invalshoek

4.3.1 *U.01 Wijzigingsbeheerprocedure voor applicaties en systemen*

Objectdefinitie

Vastgelegde manier van handelen voor de wijziging en instandhouding van applicaties en systemen.

Objecttoelichting

Wijzigingsbeheer heeft tot doel om wijzigingen binnen het traject van applicatieontwikkeling op een beheerste en geautoriseerde wijze te laten verlopen, zodat voorkomen wordt dat de doorgevoerde wijzigingen allerlei verstoringen veroorzaken.

Doelstelling	Het gecontroleerd laten verlopen van wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling.		
Risico	Als wijzigingen aan applicaties en systemen niet volgens een vastgestelde en beheerst toegepaste wijzigingsbeheerprocedure worden doorgevoerd, bestaat het risico dat wijzigingen onvolledig, ongeautoriseerd of onvoldoende getest worden geïmplementeerd, waardoor verstoringen, beveiligingsincidenten of verminderde betrouwbaarheid van systemen ontstaan.		
Control	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan **procedures voor wijzigingsbeheer.**		BIO2: 8.32 ISO 27002:2022 8.32
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procedures voor wijzigingsbeheer	1.	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.	BIO2: 8.32.02
	2.	In het wijzigingsbeheerproces is minimaal aandacht besteed aan: • het administreren van wijzigingen, met de resultaten van het testplan; • een risicoafweging van mogelijke gevolgen van de wijzigingen, inclusief een beschreven rollbackplan; • de goedkeuringsprocedure voor wijzigingen.	BIO2: 8.32.01
	3.	De procedure voor wijzigingsbeheer omvat onder meer: • een formeel proces voor nieuwe systemen en belangrijke wijzigingen, inclusief documentatie, specificatie, impactbeoordeling, testen, kwaliteitscontrole en beheerde implementatie; • toegewezen verantwoordelijkheden en handhaving om beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen gedurende de gehele levenscyclus; • integratie van wijzigingsbeheer voor ICT-infrastructuur en -software waar mogelijk; • planning en beoordeling van impact (inclusief afhankelijkheden), autorisatie, communicatie naar belanghebbenden, testen en acceptatie, implementatie met inzet- en terugvalprocedures, registratie van wijzigingen, actualisatie van bedieningsdocumentatie, gebruikersprocedures en continuïteitsplannen.	ISO 27002:2022 8.32

4.3.2 *U.02 Beperking software-installatie*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen, bedoeld om het installeren van programmatuur door eindgebruikers te beperken.

Objecttoelichting

Het installeren van software kan betrekking hebben op 3 typen actoren:

1. Gebruikers, die daarmee een bepaald type data-analyse in de business-omgeving willen kunnen uitvoeren;
2. Softwareontwikkelaars, ten behoeve van requirements-specificatie, het creëren van datamodellen en het genereren van de programmacode;
3. Technische beheerders, voor het beheren van servers en netwerkcomponenten.

Dit object richt zich op het toekennen van 'need-to-use' rechten aan ontwikkelaars voor de installatie van additionele hulpsoftware.

Het doel hiervan is om risico's te beperken, die gerelateerd zijn aan het onbedoeld wijzigen van kritische assets als informatie, software, applicaties en system security controls.

Doelstelling	Het voorkomen dat er software wordt geïnstalleerd die schade kan veroorzaken zoals het weglekken van informatie, verlies van integriteit of andere informatiebeveiligingsincidenten of het schenden van intellectuele-eigendomsrechten.	
Risico	Als de installatie van software door gebruikers, ontwikkelaars of beheerders niet strikt wordt beperkt en beheerst op basis van need-to-use, bestaat het risico dat ongeautoriseerde of onveilige programmatuur wordt geïnstalleerd, waardoor kwetsbaarheden worden geïntroduceerd die kunnen leiden tot informatiebeveiligingsincidenten, verlies van integriteit of schending van intellectuele-eigendomsrechten.	
Control	Er behoren **procedures en maatregelen** te worden geïmplementeerd om het installeren van software op operationele systemen op beveiligde wijze te beheren.	ISO 27002:2022: 8.19
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Procedures en maatregelen	1.	De procedures en maatregelen voor het installeren van software op operationele systemen omvatten onder meer: • installatie en updates van operationele software uitsluitend door geautoriseerde en opgeleide beheerders; • installatie van alleen goedgekeurde uitvoerbare code; • installatie en updates van software pas na uitgebreide en geslaagde tests, inclusief een roll-backstrategie; • gebruik van configuratiebeheer en auditlogging voor alle wijzigingen; • archivering van oude versies voor noodtoegang tot gegevens; • risicoafweging bij upgrades, patches, niet-ondersteunde (open source) en verouderde software; • monitoring en beheersing van extern geleverde software; • beperkte en gemonitorde toegang voor leveranciers; • strikte rolgebaseerde regels voor gebruikersinstallaties op basis van least privilege, met vastlegging van toegestane en verboden softwaretypen.	ISO 27002:2022: 8.19
	2.	Het risico van installatie door gebruikers van niet geautoriseerde software moet worden beheerst.	BIO2: 8.19.01

4.3.3 *U.03 Richtlijn programmacode*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen voor de broncode van een applicatie.

Objecttoelichting

Het ontwikkelen van programmacode is geen eenmalige activiteit maar een cyclisch proces van ontwikkelen, testen en verbeteren. Voor een effectieve inrichting van dit proces nemen ontwikkelaars regels in acht, waarbij zij gebruik maken van afgesproken best practices. Zonder deze regels en afspraken is het risico dat het voortbrengingsproces van de software/applicatie verstoord wordt, met als consequentie dat het product niet onderhoudbaar is en/of niet efficiënt tot stand komt.

Doelstelling	Het zorgen voor een efficiënt en effectief voortbrengingsproces van de applicatie, mede gericht op de goede onderhoudbaarheid van de applicatie.	
Risico	Als geen eenduidige en toegepaste richtlijnen voor programmacode worden gehanteerd, bestaat het risico dat ontwikkelwerkzaamheden inconsistent en ongecontroleerd plaatsvinden, waardoor het voortbrengingsproces van de applicatie wordt verstoord en de applicatie slecht onderhoudbaar, foutgevoelig of inefficiënt wordt ontwikkeld.	
Control	Voor het ontwikkelen van de (programma)code zijn specifieke **regels** van toepassing en behoort gebruik te zijn gemaakt van specifieke **best practices**.	CIP-netwerk
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Regels	1.	De programmacode voor functionele specificaties is reproduceerbaar, waarbij aandacht wordt besteed aan: • gebruikte tools; • gebruikte licenties; • versiebeheer; • documentatie van code ontwerp, omgeving, afhankelijkheden, dev/ops en gebruikte externe bronnen.	CIP-netwerk
	2.	De (programma)code wordt aantoonbaar veilig gecreëerd.	CIP-netwerk
	3.	De (programma)code is effectief, veranderbaar en testbaar waarbij gedacht kan worden aan: • het juist registreren van bugs in de code; • het voorkomen van herintroductie van bugs in de code; • het binnen 72 uur corrigeren van beveiligingsfixes; • het vastleggen van afhankelijkheden van dev/ops van applicatie (relatie tussen software-objecten); • het adequaat documenteren van software-interface, koppelingen en API's.	CIP-netwerk
Best practices	4.	Over het gebruik van de vocabulaire, applicatie-framework en toolkits zijn afspraken gemaakt.	CIP-netwerk
	5.	Voor het ontwikkelen van programmacode wordt gebruik gemaakt van gestandaardiseerde vocabulaire zoals de NEN-ISO/IEC 25010 Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models.	CIP-netwerk
	6.	Ontwikkelaars hebben kennis van algemene beveiligingsfouten, vastgelegd in een extern Common Vulnerability and Exposures (CVE)-systeem.	CIP-netwerk
	7.	Het gebruik van programmacode uit externe programmabibliotheken mag pas worden gebruikt na getest te zijn.	CIP-netwerk

4.3.4 *U.04 Analyse en specificatie informatiesysteem*

Objectdefinitie

Systematisch onderzoek naar de functionele eisen voor een applicatie, bepaald door de business en andere stakeholders.

Objecttoelichting

Met het analyseren en specificeren van requirements wordt in kaart gebracht aan welke functionele en niet-functionele eisen de te ontwikkelen applicatie moet voldoen. Ook worden de constraints geïdentificeerd die zullen gelden in de ontwikkelfase en de operationele fase.

Het ontwikkelen van informatiesystemen wordt tegenwoordig veelal uitgevoerd volgens de iteratieve ontwikkelmethode (Agile). Onafhankelijk van de methode (traditioneel/Waterval of Agile) is sprake van een aantal ontwikkelstappen waaraan aandacht wordt besteed:

- functionele eisen onder andere: functionaliteiten, gegevens, business rules, presentatie, interactie en foutafhandelingen;
- niet-functionele eisen onder andere: betrouwbaarheid, gebruiksvriendelijkheid, efficiëntie, onderhoudbaarheid, performance en flexibiliteit in overdraagbaarheid.

In de ISO 27002 2017 wordt rond dit thema alleen focus gelegd op niet-functionele eisen, en daarvan vooral beveiligingseisen. Daarom is naast het object 'Analyse en specificatie van informatiebeveiligingseisen' ook het object 'Analyse en specificatie van informatiesystemen' toegevoegd, waarbij de nadruk gelegd wordt op functionele eisen.

Deze BIO Thema-uitwerking is baseline gebaseerd en lineair, volgens de V-model-aanpak, uitgewerkt. Aangezien bij Agile niet op deze wijze wordt gewerkt, verdient dit aspect extra aandacht.

Doelstelling	Het leggen van een basis voor de volgende fasen (de ontwerpfase en verder) met geanalyseerde en gespecificeerde functionele eisen.		
Risico	Als functionele eisen voor het informatiesysteem niet volledig, eenduidig of tijdig worden geanalyseerd en gespecificeerd, bestaat het risico dat deze eisen in het ontwerp en de daaropvolgende ontwikkelfasen niet of onjuist worden meegenomen, waardoor het systeem niet aansluit op de behoeften van de business en herstel of aanpassing in een later stadium noodzakelijk is.		
Control	De **functionele eisen** die verband houden met nieuwe informatiesystemen of voor uitbreiding van bestaande informatiesystemen behoren te worden geanalyseerd en gespecificeerd.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Functionele eisen	1.	De functionele eisen worden geanalyseerd en bepaald met verschillende invalshoeken (zoals stakeholders, business en wet- en regelgeving) en vastgelegd in een functioneel ontwerp.	CIP-netwerk
	2.	Het functioneel ontwerp wordt gereviewd, waarna verbeteringen en of aanvullingen op het functioneel ontwerp plaatsvinden.	CIP-netwerk
	3.	Met een goedgekeurd functioneel ontwerp wordt een technisch ontwerp vervaardigd dat ook ter review wordt aangeboden aan de kwaliteitsfunctionaris en beveiligingsfunctionaris.	CIP-netwerk
	4.	Alle vereisten worden gevalideerd door een peer review of prototyping (Agile-ontwikkelmethode).	CIP-netwerk
	5.	Parallel aan het vervaardigen van het functioneel ontwerp en technisch ontwerp worden acceptatie-eisen vastgelegd.	CIP-netwerk

4.3.5 *U.05 Informatiebeveiliging in projectmangement*

Objectdefinitie

Informatiebeveiliging maakt integraal onderdeel uit van het management van alle projecten, ongeacht type, omvang, duur of discipline, zodat informatiebeveiligingsrisico's effectief worden beheerd gedurende de gehele projectlevenscyclus.

Objecttoelichting

Met het object Informatiebeveiliging in projectmangement wordt gewaarborgd dat de eisen op het gebied van informatiebeveiliging in kaart worden gebracht en als onderdeel van de non-functionele eisen niet worden vergeten bij de ontwikkeling van de applicatie.

Doelstelling	Het zorgen dat informatiebeveiligingsrisico's binnen projecten en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden aangepakt..		
Risico	Als informatiebeveiliging niet integraal en structureel wordt meegenomen binnen het projectmanagement gedurende de gehele projectlevenscyclus, bestaat het risico dat informatiebeveiligingseisen onvoldoende worden geïdentificeerd, vastgelegd of bewaakt, waardoor nieuwe of gewijzigde informatiesystemen worden gerealiseerd zonder passende beheersing van informatiebeveiligingsrisico's.		
Control	**Informatiebeveiliging** behoort te worden geïntegreerd in projectmanagement.		ISO 27002:2022: 5.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Informatiebeveiliging	1.	Informatiebeveiliging is een integraal onderdeel van projectmanagement bij alle projecten (ongeacht complexiteit, omvang of discipline) en omvat onder meer: • beoordeling en behandeling van informatiebeveiligingsrisico's in een vroeg stadium en periodiek gedurende de gehele projectlevenscyclus, als onderdeel van het projectrisicobeheer; • vaststelling van informatiebeveiligingseisen voor door het project te leveren producten of diensten, gebaseerd op nalevingseisen uit informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels, regelgeving en andere methoden; • beheersing van informatiebeveiligingsrisico's gerelateerd aan de projectuitvoering, waaronder interne en externe communicatie; • periodieke beoordeling van de voortgang en effectiviteit van de risicobehandeling door geschikte personen of de projectstuurgroep; • definitie en toewijzing van verantwoordelijkheden en bevoegdheden voor informatiebeveiliging aan gespecificeerde projectrollen.	ISO 27002:2022: 5.8

	2.	Bij alle projecten worden informatiebeveiligingseisen vastgesteld, waarbij wordt gehouden met: • welke informatie het betreft (vaststelling en classificatie), de bijbehorende beveiligingsbehoeften en mogelijke bedrijfsimpact bij ontoereikende beveiliging; • bescherming van beschikbaarheid, integriteit en vertrouwlijkheid van informatie en gerelateerde bedrijfsmiddelen; • authenticatie-eisen op basis van vereiste betrouwbaarheid van identiteiten; • processen voor toegangsverlening en autorisatie voor klanten, gebruikers, technische gebruikers en externe leveranciers; • informeren van gebruikers over hun plichten en verantwoordelijkheden; • eisen afgeleid uit bedrijfsprocessen; • eisen vanuit andere informatiebeveiligingsbeheersmaatregelen; • naleving van wettelijke, regelgevende en contractuele verplichtingen; • het vereiste niveau van vertrouwen dat derden zullen voldoen aan de beleidsregels, met inbegrip van relevante beveiligingsclausules in overeenkomsten of contracten.	ISO 27002:2022: 5.8
	3.	Bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging op basis van de door de organisatie vastgestelde risicomanagementmethodiek worden uitgevoerd, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de beveiligingseisen.	BIO2: 5.8.01

4.3.6 *U.06 Applicatie-ontwerp*

Objectdefinitie

Geheel van specificaties van de te ontwikkelen applicatie, vastgelegd in tekst en beeld.

Objecttoelichting

Tijdens de ontwerpfase worden de (niet-)functionele requirements omgezet naar een concreet ontwerp (bouwplan) voor de applicatie. Een high level architectuur wordt ontwikkeld om de software te kunnen bouwen. Hierbij wordt onder andere aandacht besteed aan de gebruikte data door het systeem, de functionaliteit die geboden moeten worden, de interfaces tussen componenten binnen het systeem en aan koppelingen met andere systemen. Ook worden constraints die voortvloeien uit specifieke beveiligingseisen verder uitgewerkt.

Doelstelling	Het opstellen van een veilig en gedegen/solide applicatieontwerp.
Risico	Als het applicatieontwerp niet volledig en consistent is uitgewerkt op basis van de vastgestelde functionele, niet-functionele en beveiligingseisen, bestaat het risico dat essentiële ontwerpkeuzes ontbreken of onjuist zijn, waardoor tijdens realisatie en gebruik kwetsbaarheden ontstaan en herontwerp of kostbare aanpassingen noodzakelijk worden.

Control	Het applicatieontwerp behoort gebaseerd te zijn op informatie, die is verkregen uit verschillende invalhoeken, zoals: **business-vereisten en reviews**, **omgevingsanalyse** en **(specifieke) beveiliging**.	SoGP 2018: SD2.2
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**
Business-vereisten en reviews	1. Het ontwerpen van applicaties is gebaseerd op eisen voor verschillende typen informatie, zoals: • gebruikers-, beveiligings- en kwaliteitseisen; • business-vereisten (onder andere nut, noodzaak en kosten); • eisen die voortvloeien uit risico-assessments, dreigingsanalyse en prioritering ervan en technische beveiligingsreviews (en de prioritering daarvan); • eisen die voortvloeien uit de BIA en PIA.	SoGP 2018: SD2.2.1
Omgevings-analyse	2. Bij het ontwerp van applicaties is informatie verkregen uit verschillende mogelijke connecties met de te ontwerpen applicatie, zoals: • mogelijke invoerbronnen voor data en connecties met andere applicaties (componenten); • connecties tussen modules binnen de applicatie en connecties met andere applicaties; • gebruik van opslagmechanisme voor informatie, toegang tot databases en ander type storage; • uitvoer van informatie naar andere applicaties en beveiliging hiervan; • mogelijke transmissie van data tussen applicaties.	SoGP 2018: SD2.2.2
(Specifieke) beveiliging	3. Het ontwerp is mede gebaseerd op een beveiligingsarchitectuur, waarin aandacht is besteed aan: performance, capaciteit, continuïteit, schaalbaarheid, connectiviteit en comptabiliteit.	SoGP 2018: SD2.2.3

4.3.7 *U.07 Applicatiefunctionaliteit*

Objectdefinitie

Geheel van toepassingsfuncties die ondersteuning bieden aan de bedrijfsprocessen.

Objecttoelichting

De functies kunnen worden onderverdeeld in invoer-, verwerking- en uitvoerfuncties. Binnen de functies worden controles en rekenregels ingebouwd om de gewenste acties te kunnen uitvoeren en gewenste resultaten te kunnen leveren. Het totaal aan functionaliteiten moet aan bepaalde eisen voldoen. Zo moeten functionaliteiten:

- voldoen aan de behoefte van de gebruikers;
- de gebruikerstaken afdekken;
- resultaten leveren die nauwkeurig zijn;
- geschikt zijn om bepaalde taken te kunnen ondersteunen.

Doelstelling	Het optimaal ondersteunen van het bedrijfsproces.

Risico	Als de applicatiefunctionaliteit niet volledig aansluit op de vastgestelde gebruikersbehoeften en bedrijfsprocessen, bestaat het risico dat het informatiesysteem taken onvoldoende of onjuist ondersteunt, waardoor processen inefficiënt verlopen, fouten ontstaan en de beoogde ondersteuning van de bedrijfsvoering niet wordt gerealiseerd.		
Control	Informatiesystemen behoren zo te worden ontworpen, dat de **invoerfuncties**, **verwerkingsfuncties** en **uitvoerfuncties** van gegevens (op het juiste moment) in het proces worden gevalideerd op juistheid, tijdigheid en volledigheid om het bedrijfsproces optimaal te kunnen ondersteunen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Invoerfuncties	1.	Bereikcontroles worden toegepast en gegevens worden gevalideerd.	CIP-netwerk
Verwerkings-functies	2.	Geprogrammeerde controles worden ondersteund.	CIP-netwerk
	3.	Het uitvoeren van onopzettelijke mutaties wordt tegengegaan.	CIP-netwerk
	4.	Voorzieningen voor het genereren van een fout- en uitzonderingsrapportage zijn beschikbaar.	CIP-netwerk
	5.	Voorzieningen voor het achteraf vaststellen van een betrouwbare verwerking (JVT) zijn beschikbaar (onder andere audit trail).	CIP-netwerk
	6.	Opgeleverde/over te dragen gegevens worden gevalideerd.	CIP-netwerk
	7.	De controle op de juistheid, volledigheid en tijdigheid van de input (ontvangen gegevens) en op de verwerking en de output van gegevens (versterkte gegevens) worden uitgevoerd.	CIP-netwerk
	8.	Met vastgestelde en geautoriseerde procedures wordt voorkomen dat gegevens buiten de applicatie om (kunnen) worden benaderd.	CIP-netwerk
Uitvoer-functies	9.	Gegevens worden volgens vastgestelde beveiligingsklasse gevalideerd op plausibiliteit, volledigheid en bedrijfsgevoeligheid.	CIP-netwerk

4.3.8 *U.08 Applicatiebouw*

Objectdefinitie

Vertaling van het ontwerp in door de computer executeerbare programmacode.

Objecttoelichting

Na de eerste twee ontwikkelfasen waarbij de nadruk ligt op de analyse van requirements en op het ontwerp van het product, volgt de derde fase, de applicatiebouw. In deze derde fase wordt de programmacode gecreëerd met gebruik making van good practices, methoden/technieken en volgens bepaalde beveiligingsuitgangspunten.

Doelstelling	Het zorgen voor een robuust werkende programmacode met veiligheidsmaatregelen die kwaadaardige aanvallen kunnen worden weerstaan.

Risico	Als bij de applicatiebouw beveiligingsuitgangspunten, good practices en vastgestelde ontwikkelrichtlijnen niet consequent worden toegepast, bestaat het risico dat de opgeleverde programmacode kwetsbaar is voor misbruik of aanvallen, waardoor de vertrouwelijkheid, integriteit en beschikbaarheid van het informatiesysteem worden aangetast.		
Control	De bouw van applicaties inclusief programmacode behoort te worden uitgevoerd met **(industrie) good practice** en door individuen die beschikken over de **juiste vaardigheden en tools** en behoort te worden gereviewd.		SoGP 2018: SD2.4a en d
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
(Industrie) good practice	1.	Gedocumenteerde standaarden en procedures worden beschikbaar gesteld voor het bouwen van programmacode, waarin ook is gespecificeerd dat • een goedgekeurde methode voor applicatiebouw wordt gehanteerd; • mechanismen worden gebruikt waarmee zekerheid wordt verkregen dat de applicatie voldoet aan good practices voor applicatiebouw (methode voor het ontwikkelen van veilige programmacode).	SoGP 2018: SD2.4.1
	2.	Veilige methodes worden toegepast om te voorkomen dat veranderingen kunnen worden aangebracht in de basiscode of in software-packages.	SoGP 2018: SD2.4.2
	3.	Voor het creëren van programmacode wordt gebruik gemaakt van best practices (gestructureerde programmering).	SoGP 2018: SD2.4.3
	4.	Het gebruik van onveilig programmatechnieken is niet toegestaan.	SoGP 2018: SD2.4.3
	5.	De programmacode is beschermd tegen ongeautoriseerde wijzigingen.	SoGP 2018: SD2.4.3
	6.	Activiteiten van applicatiebouw worden gereviewd.	SoGP 2018: SD2.4.1
Juiste vaardigheden en tools	7.	De ontwikkelaars zijn adequaat opgeleid en zijn in staat om binnen het project de noodzakelijke en in gebruik zijnde tools te hanteren.	SoGP 2018: SD2.4.3

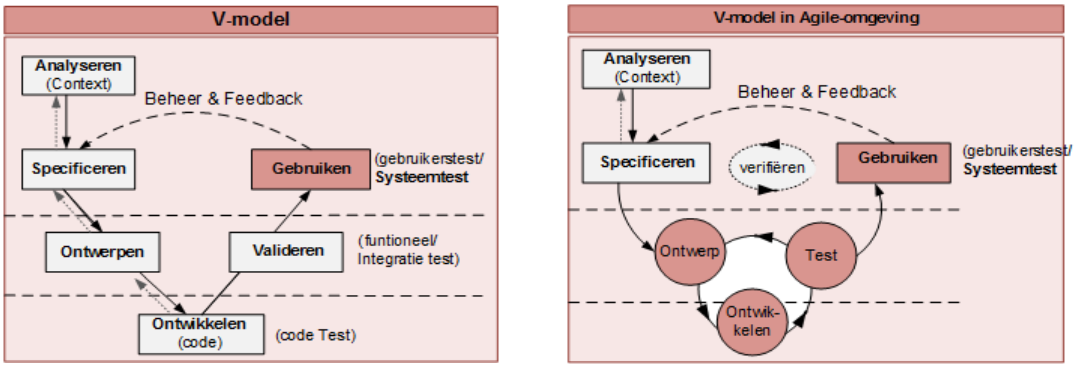
4.3.9 *U.09 Systeemacceptatietest*

Objectdefinitie

Gebruikers-eindtoets op basis waarvan een applicatie al dan niet geaccepteerd zal worden.

Objecttoelichting

De systeemacceptatietest is zowel in de Waterval- als in de Agile-ontwikkelmethode de afsluitende test. Voor beide methoden gelden een aantal eisen waarmee tijdens de systeemacceptatietest rekening gehouden moet worden. Bij de acceptatietest wordt door gebruikers getoetst of de requirements adequaat in het uiteindelijke product zijn verwerkt. Hierbij gaat het niet alleen om de beveiligingseisen maar ook om de functionele eisen, gebruikerseisen, businesseisen en business rules. De systeemtest wordt in afbeelding 5 geïllustreerd voor beide methoden.



Afbeelding 5: Systeemtest bij de Waterval- en Agile-methode

Doelstelling	Het toetsen of de requirements adequaat in het uiteindelijke product, het nieuwe informatiesysteem, zijn verwerkt.		
Risico	Als de systeemacceptatietest niet volledig of onvoldoende representatief wordt uitgevoerd, bestaat het risico dat afwijkingen ten opzichte van beveiligingseisen, functionele eisen, gebruikerseisen en business rules pas na ingebruikname aan het licht komen, waardoor het informatiesysteem tekortschiet in betrouwbaarheid en beheersbaarheid en correctieve maatregelen met grotere impact nodig zijn.		
Control	Processen voor het **testen van de beveiliging** behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.		ISO 27002:2022: 8.29
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Testen van de beveiliging	1.	Het testen van de beveiliging wordt uitgevoerd op basis van een verzameling van functionele en niet-functionele eisen en omvat onder meer: • beveiligingsfuncties zoals authenticatie van gebruikers, toegangsbeperking en cryptografie; • toepassing van de regels voor veilig coderen; • toepassing van beveiligde configuraties zoals besturingssystemen, firewalls en andere beveiligingscomponenten.	ISO 27002:2022: 8.29
	2.	Testplannen worden vastgesteld en staan in verhouding tot het belang, de aard en mogelijke impact van de verandering. Het testplan omvat onder meer: • een gedetailleerd schema van de activiteiten en tests; • input en verwachte output onder allerlei omstandigheden; • criteria om de resultaten te evalueren; • een besluit over verdere acties naarmate nodig is.	ISO 27002:2022: 8.29
	3.	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	BIO2: 8.29.01

	4.	Bij de acceptatietest wordt getoetst of het geleverde product overeenkomt met hetgeen is afgesproken. Hierbij is de testfocus onder andere gericht is op: • het testen van de functionele requirements; • het testen van de business rules voor de betrokken bedrijfsprocessen; • de beveiligingseisen die verband houden met betrokken bedrijfsprocessen.	CIP-netwerk
	5.	Testresultaten worden formeel geëvalueerd en door de betrokken informatiesysteemeigenaar beoordeeld, waarna - na te zijn goedgekeurd - overgegaan wordt naar de volgende fase.	CIP-netwerk

4.3.10 *U.10 Beschermen testgegevens*

Objectdefinitie

Bescherming van gegevens die gebruikt worden om aan te tonen dat een applicatie werkt volgens de vastgestelde eisen en wensen.

Objecttoelichting

Voor het testen van informatiesystemen wordt gebruik gemaakt van verschillende soorten gegevens. Het gebruik van operationele databases met persoonsgegevens of enige andere vertrouwelijke informatie moet worden vermeden. Testgegevens dienen zorgvuldig te worden gekozen, beschermd en gecontroleerd.

Doelstelling	Het vermijden van het gebruik van persoonsgegevens of enige andere vertrouwelijke informatie voor testdoeleinden en het beschermen van gegevens die voor het testen van informatiesystemen zijn gebruikt.	
Risico	Als testgegevens onvoldoende worden geselecteerd, beschermd of gecontroleerd, bestaat het risico dat persoonsgegevens of andere vertrouwelijke informatie onbedoeld worden gebruikt of blootgesteld, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van testgegevens en onderliggende informatie worden aangetast en privacy- en beveiligingsincidenten ontstaan.	
Control	**Testgegevens** behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	ISO 27002:2022: 8.33
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Testgegevens	1.	De volgende richtlijnen worden toegepast om operationele gegevens die voor testdoeleinden worden gebruikt, te beschermen: • de toegangsbeveiligingsprocedures die worden toegepast op operationele omgevingen, ook op testomgevingen toepassen; • voor elke keer dat besturingsgegevens naar een testomgeving worden gekopieerd, een afzonderlijke autorisatie verkrijgen; • logbestanden van het kopiëren en gebruiken van besturingsgegevens bijhouden om in een audittraject te voorzien; • gevoelige gegevens beschermen door deze te verwijderen of te maskeren bij gebruik voor testen; • operationele gegevens naar behoren uit een testomgeving wissen onmiddellijk nadat het testen is afgerond; • testgegevens worden veilig opgeslagen en alleen voor testdoeleinden gebruikt.	ISO 27002:2022: 8.33

4.3.11 *U.11 Scheiding van ontwikkel-, test- en productieomgevingen*

Objectdefinitie

Identificatie en implementatie van het benodigde scheidingsniveau tussen ontwikkel-, test- en productieomgevingen om operationele problemen, ongeautoriseerde wijzigingen en beveiligingsincidenten te voorkomen.

Objecttoelichting

Het ontwikkeltraject van applicaties en het in productie nemen van de resultaten hiervan vindt gefaseerd plaats in specifieke omgevingen. Bij de ontwikkeling worden 4 omgevingen onderscheiden:

1. Ontwikkelomgeving
   Hierin wordt de programmacode ontwikkeld. Om te voorkomen dat ontwikkelingen het productieproces kunnen beïnvloeden, is deze omgeving gescheiden van de productie-omgeving.
2. Testomgeving
   Hierin worden de uit de ontwikkelomgeving afkomstige producten getest door professionele testteams. In de testomgeving gesignaleerde onvolkomenheden in de software worden weer via ontwikkelomgeving aangepast. Dit is een iteratief proces totdat uit de test naar voren komt dat het product geschikt is om in productie te nemen.
3. Acceptatieomgeving
   Hierin worden de software-producten (nog eenmaal) grondig getest en bij positief resultaat door de gebruikers en beheerders geaccepteerd. Bij eventuele onvolkomenheden worden de software-producten niet geaccepteerd (no-go) en teruggestuurd naar de test- of ontwikkelomgeving.
4. Productieomgeving
   Hierin wordende nieuwe software-producten uitgerold. De productieomgeving is de omgeving waarin de nieuwe software-producten functioneel en actief zijn. De in de voorgaande omgevingen uitgevoerde stappen moeten zo veel mogelijk garanderen dat nieuw ontwikkelde software geen fouten bevat die de productiegegevens kunnen corrumperen.

In principe zijn alle omgevingen los van elkaar ingericht en vindt behalve via formele overdrachten geen contact plaats tussen de verschillende omgevingen.

Doelstelling	Het voorkomen dat door ontwikkelactiviteiten het productieproces negatief beïnvloed wordt.		
Risico	Als ontwikkel-, test-, acceptatie- en productieomgevingen niet voldoende van elkaar zijn gescheiden, bestaat het risico dat ongeautoriseerde wijzigingen, testactiviteiten of fouten uit eerdere fasen invloed hebben op de productieomgeving, waardoor productiegegevens worden aangetast, beveiligingsincidenten ontstaan en de continuïteit van de dienstverlening wordt verstoord.		
Control	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.		ISO 27002:2022: 8.31
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Ontwikkel-, test- en productieomgevingen	1.	Het scheidingsniveau tussen de ontwikkel-, test- en productieomgevingen is geïdentificeerd en geïmplementeerd, waarbij rekening is gehouden met de volgende aspecten: • fysieke of logische scheiding van omgevingen (bijv. verschillende domeinen); • gedocumenteerde regels en autorisaties om software naar andere omgevingen te verplaatsen; • geen toegang tot ontwikkelinstrumenten of systeemhulpmiddelen vanuit productie, tenzij noodzakelijk; • duidelijke identificatielabels voor omgevingen om fouten te voorkomen; • geen gevoelige informatie naar ontwikkel- of testomgevingen kopiëren zonder gelijkwaardige beveiliging; • bescherming van ontwikkel- en testomgevingen door patching van tools en bibliotheken, beveiligde configuraties, toegangsbeveiliging, monitoring van veranderingen en omgevingen, alsmede regelmatige back-ups; • scheiding van taken zodat één persoon niet zelfstandig wijzigingen in ontwikkeling én productie kan doorvoeren.	ISO 27002:2022: 8.31
	2.	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	BIO2: 8.31.01
	3.	Significante wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	BIO2: 8.31.02
	4.	De taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen in de ontwikkel-, test-, acceptatie- en productie-omgevingen worden uitgevoerd volgens onderkende rollen.	CIP-netwerk
	5.	Voor remote-werkzaamheden is een werkwijze vastgelegd.	SoGP 2018: PM1.3.1
	6.	Ontwikkelaars hebben geen toegang tot de productieomgeving.	CIP-netwerk
	7.	Voor het kopiëren/verplaatsen van configuratie-items tussen de omgevingen gelden overdrachtsprocedures.	CIP-netwerk
	8.	De overdracht van de ontwikkel- naar de testomgeving vindt gecontroleerd plaats met een implementatieplan.	CIP-netwerk

	9.	De overdracht van de test- naar de acceptatie-omgeving vindt procedureel door daartoe geautoriseerde personen plaats.	CIP-netwerk
	10.	De overdracht naar de productie-omgeving vindt procedureel door daartoe geautoriseerde personen plaats.	CIP-netwerk

4.3.12 *U.12 Applicatiekoppeling*

Objectdefinitie

Verbinding tussen twee of meer applicaties waarmee gegevens tussen deze applicaties uitgewisseld kunnen worden.

Objecttoelichting

Bij het ontwikkelen van applicaties kunnen mogelijk koppelingen tussen de applicatie die in ontwikkeling is en andere applicaties noodzakelijk zijn. Vanuit beveiligingsoogpunt dient dit soort koppelingen aan bepaalde eisen te voldoen.

Doelstelling	Het kunnen leveren van de juiste services en waarborgen van de informatiebeveiliging van de betrokken applicaties.		
Risico	Als applicatiekoppelingen niet zorgvuldig en beveiligd worden ontworpen en geïmplementeerd, bestaat het risico dat gegevensuitwisseling tussen applicaties onbeheerst plaatsvindt, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van data van de ontwikkelde applicatie en gekoppelde systemen worden aangetast.		
Control	De koppelingen tussen applicaties behoren te worden uitgevoerd volgens geaccordeerde **koppelingsrichtlijnen**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Koppelings-richtlijnen	1.	Koppelingen tussen applicaties worden uitgevoerd met vastgestelde procedures en richtlijnen.	CIP-netwerk
	2.	Van het typen koppelingen is een overzicht aanwezig.	CIP-netwerk
	3.	Koppelingen worden uitgevoerd via geautoriseerde opdrachten.	CIP-netwerk
	4.	De uitgevoerde koppelingen worden geregistreerd.	CIP-netwerk

4.3.13 *U.13 Logging en monitoring*

Objectdefinitie

Vastlegging van aan informatiebeveiliging gerelateerde gebeurtenissen en het bewaken en onderkennen van afwijkingen op beleidsregels.

Objecttoelichting

In de te ontwikkelen software moeten faciliteiten voor logging en monitoring zijn ingebouwd, ter detectie en vastlegging van pogingen om de applicatie of de database te verminken of onterecht te benaderen.

Doelstelling	Het tijdig detecteren en vastleggen van ongeoorloofde en/of onjuiste activiteiten van medewerkers en storingen binnen de applicatie.		
Risico	Als in de applicatie onvoldoende voorzieningen voor logging en monitoring zijn ingebouwd, bestaat het risico dat ongeoorloofde, foutieve of afwijkende activiteiten en storingen niet tijdig worden gedetecteerd of gereconstrueerd, waardoor beveiligingsincidenten onopgemerkt blijven en onderzoek en herstel worden bemoeilijkt.		
Control	Applicaties behoren faciliteiten te bieden voor **logging** en **monitoring** om ongeoorloofde en/of onjuiste activiteiten van medewerkers en storingen binnen de applicatie tijdig te detecteren en vast te leggen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Logging	1.	Welke ongeoorloofde en onjuiste activiteiten gelogd moeten worden, is vastgelegd.	CIP-netwerk
	2.	Informatie over autorisatie(s) wordt vastgelegd.	CIP-netwerk
	3.	De loggegevens zijn beveiligd.	CIP-netwerk
	4.	De locatie van de vastlegging van de loggegevens is vastgesteld.	CIP-netwerk
Monitoring	5.	De applicatie geeft signalen aan de beveiligingsfunctionarissen dat loggegevens periodiek geëvalueerd en geanalyseerd moeten worden.	CIP-netwerk
	6.	De frequentie (wanneer) van monitoring en het rapporteren hierover (aan wie wat) is vastgelegd.	CIP-netwerk

4.3.14 *U.14 Applicatie-architectuur*

Objectdefinitie

Modelmatige beschrijving van de samenhang van het applicatielandschap.

Objecttoelichting

De applicatie-architectuur beschrijft de samenhang tussen functionele eisen en beveiligingseisen. Ook wordt aandacht besteed aan de integratie-aspecten met de infrastructuur. Vanuit een eenduidig beeld wordt de applicatie met deze architectuur gerealiseerd. Richtlijnen, instructies, architectuur- en beveiligingsvoorschriften en procedures worden zodanig toegepast dat een samenhangend geheel ontstaat. Op deze manier wordt ook zeker gesteld dat de applicatie aan de vereiste functionele en beveiligingseisen voldoet.

Doelstelling	Het richting geven aan de te ontwikkelen applicatie en een betrouwbare werking van de applicatie te garanderen.

Risico	Als de applicatie-architectuur onvoldoende richtinggevend, consistent of actueel is, bestaat het risico dat ontwerp- en implementatiekeuzes niet goed op elkaar aansluiten, waardoor de applicatie onbetrouwbaar functioneert en niet aantoonbaar voldoet aan de gestelde functionele en beveiligingseisen.		
Control	De functionele en beveiligingseisen behoren in een **applicatie-architectuur**, volgens architectuurvoorschriften, in **samenhang** te zijn vastgelegd.		NCSC 2015: U/WA.09.01
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Applicatie-architectuur	1.	De architect heeft een actueel document van het te ontwikkelen informatiesysteem opgesteld. Het document: • heeft een eigenaar; • is voorzien van een datum en versienummer; • bevat een documenthistorie (wat is wanneer en door wie aangepast); • is actueel, juist en volledig; • is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.	NCSC 2015: U/WA.09.01
	2.	Het architectuurdocument wordt actief onderhouden.	NCSC 2015: U/WA.09.01
	3.	De voorschriften, methoden en technieken voor applicatiearchitectuur worden toegepast.	NCSC 2015: U/WA.09
Samenhang	4.	Tussen in- en uitstroom van gegevens en de inhoud van de gegevensberichten bestaat een aantoonbare samenhang.	CIP-netwerk
	5.	Het is aantoonbaar dat de onderliggende infrastructuurcomponenten beveiligd zijn met beveiligingsbaselines (onder andere uitschakeling van overbodige functionaliteiten).	CIP-netwerk
	6.	De relatie tussen de persoonsgegevens die gebruikt worden binnen de applicatie en de persoonsgegevens, van interne en externe ontvangers van de door de applicatie opgeleverde gegevens, is inzichtelijk.	CIP-netwerk

4.3.15 *U.15 Tooling ontwikkelmethode*

Objectdefinitie

Hulpmiddelen die bepaalde ontwikkelactiviteiten ondersteunen of geheel of gedeeltelijk overnemen.

Objecttoelichting

Tijdens het ontwikkelproces is sprake van continue veranderingen in de onderkende omgevingen. Daarom is het noodzakelijk om de omgevingen daadwerkelijk te reguleren en is de inzet van een tool die alle fasen, inclusief het testen, ondersteunt noodzakelijk. Het tool moet alle veranderingen en onderlinge relaties tussen de componenten ondersteunen.

Doelstelling	Het effectief uitvoeren van de ontwikkelcyclus van een applicatie met de continue veranderingen in de onderkende fasen.

Risico	Als tooling die de ontwikkelmethode ondersteunt onvoldoende geschikt, geïntegreerd of consequent wordt gebruikt, bestaat het risico dat wijzigingen, afhankelijkheden en testactiviteiten niet goed worden beheerst, waardoor de ontwikkelcyclus minder effectief verloopt en fouten of inconsistenties pas laat worden onderkend.		
Control	De ontwikkelmethode moet worden ondersteund door een tool dat de noodzakelijke **faciliteiten** biedt voor het effectief uitvoeren van de ontwikkelcyclus.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Faciliteiten	1.	Het tool ondersteunt alle fasen van het ontwikkelproces voor het documenteren van analyses, specificaties, programmatuur, testen en rapportages.	CIP-netwerk
	2.	Het tool biedt een bepaald framework voor het structureren van de ontwikkelfasen en het bewaken van afhankelijkheden.	CIP-netwerk
	3.	Het tool beschikt over faciliteiten voor versie- en releasebeheer.	CIP-netwerk
	4.	Het tool beschikt over faciliteiten voor: • het registreren van eisen en wensen; • het afhandelen van fouten; • het beveiligen van registraties (programmacode); • het continu integreren van componenten; • het kunnen switchen tussen de fasen: specificeren, ontwikkelen en testen.	CIP-netwerk
	5.	Het tool beschikt over faciliteiten voor de koppelingen met externe bronnen.	CIP-netwerk

5 Control-domein

5.1 Doelstelling

De doelstelling van het control-domein van applicatieontwikkeling is vast te stellen of:

- de uitvoerings-controls afdoende zijn ingericht voor het garanderen van een beheersbare applicatieomgeving en/of
- de applicatie functioneel en technisch op het juiste niveau wordt gehouden.

Dit houdt onder meer in dat binnen de organisatie een adequate beheerorganisatie moet zijn ingericht waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

Door het ontbreken van noodzakelijke maatregelen binnen de ontwikkelorganisatie is het niet zeker of de ontwikkel- en onderhoudsadministratie aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet en de governance daarop toereikend is ingericht. Evenmin kan worden vastgesteld of de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Tabel 3 toont de objecten die specifiek voor dit domein een rol spelen. Het blauw gemarkeerde object komt voor in de BIO. De wit gemarkeerde objecten zijn betrokken uit andere best practices. De objecten zijn ingedeeld naar de invalshoeken: intentie, functie, gedrag of structuur.

Intentie	Functie	Gedrag	Structuur
C.01 Richtlijn evaluatie ontwikkelactiviteiten ((Operationeel) beleid)	C.02 Versiebeheer (Proces)	/	C.07 Beheersorganisatie applicatieontwikkeling (IT-organisatiestructuur)
/	C.03 Patchmanagement (Proces)	/	/
/	C.04 (Software)configuratiebeheer (Proces)	/	/
/	C.05 Quality assurance (Proces)	/	/
/	C.06 Compliance-management (Proces)	/	/

Tabel 3: Control-objecten met basiselementen voor applicatieontwikkeling per invalshoek

5.3.1 *C.01 Richtlijn evaluatie ontwikkelactiviteiten*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen voor het achteraf beoordelen van ontwikkelactiviteiten.

Objecttoelichting

De ontwikkelorganisatie moet tijdig een softwareproduct realiseren dat aan de gestelde eisen voldoet. Hiertoe verricht deze organisatie periodiek controle- en reviewactiviteiten op de producten die in de ontwikkelfase tot stand komen, zoals requirements, specificaties, intern ontwikkelde programmacode en delen die uit externe bibliotheken worden verworven. De verantwoordelijke functionarissen moeten voor deze activiteiten beschikken over de nodige controlerichtlijnen.

Doelstelling	Het adequaat kunnen opstellen van controle-activiteiten en rapportages, gericht op ontwikkelactiviteiten.		
Risico	Als geen eenduidige en toegepaste richtlijnen bestaan voor het evalueren van ontwikkelactiviteiten, bestaat het risico dat controle- en reviewactiviteiten onvolledig of inconsistent worden uitgevoerd, waardoor tekortkomingen in requirements, ontwerp of programmacode niet tijdig worden onderkend en de kwaliteit en beveiliging van het ontwikkelresultaat onvoldoende zijn geborgd.		
Control	De projectorganisatie behoort **richtlijnen** voor de **controle-activiteiten en rapportages** te hebben geformuleerd, gericht op de evaluaties van **ontwikkelactiviteiten**, zoals requirements, specificaties en programmacode.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Richtlijnen	1.	De projectorganisatie beschikt over controlerichtlijnen voor de evaluatie van de producten die uit de ontwikkelfasen voortvloeien, zoals een requirementsanalyse en de specificatie van software.	CIP-netwerk
	2.	De projectorganisatie beschikt over evaluatierichtlijnen voor het evalueren van intern ontwikkelde en extern verworven code die zijn opgeleverd tijdens de ontwikkelfasen: requirementsanalyse, specificatie en programmacode.	CIP-netwerk
	3.	De projectorganisatie beschikt over controlerichtlijnen die binnen de relevante beheerprocessen, versiebeheer, quality assurance en quality control worden toegepast voor het evalueren van de ontwikkelactiviteiten.	CIP-netwerk
	4.	De projectorganisatie beschikt over een kwaliteitshandboek waarin procedures zijn opgenomen voor het toepassen van quality assurance- en quality control-methodiek en reviewrichtlijnen voor de ontwikkelde producten.	CIP-netwerk
	5.	De quality assurance-methodiek wordt volgens de richtlijnen nageleefd.	CIP-netwerk
Controle-activiteiten en rapportages	6.	De projectorganisatie voert controle-activiteiten uit over de ontwikkelactiviteiten en beheerprocessen gerelateerd aan het ontwikkelproces en stelt hierover rapportages op.	CIP-netwerk
Ontwikkel-activiteiten	7.	Periodiek worden het applicatieontwikkelingsproces, de testcycli en de kwaliteit van de programmacode beoordeeld volgens de opgestelde richtlijn.	CIP-netwerk

5.3.2 *C.02 Versiebeheer*

Objectdefinitie

Instandhoudingsproces voor de registratie van verschillende fasen van een document, programma of andere informatie.

Objecttoelichting

Versiebeheer houdt in het organiseren van versies van applicatie-objecten tijdens het ontwikkel- en onderhoudstraject. Het betreft versies van documenten, zoals functionele en technische ontwerpen en versies van programmacode in de verschillende fasen van het ontwikkel- en onderhoudstraject.

Een goed versiebeheerproces zorgt ervoor:

- dat iedere medewerker de juiste en meest recente versie van de functionele eisen hanteert bij het ontwikkelen van software-specificaties;
- dat binnen het ontwikkel- en onderhoudsproces de juiste versie van de programmacode wordt gebruikt.

Hierdoor kunnen releases van applicaties met de juiste code en relevante bestanden worden samengesteld. Vanuit efficiëntie kan versiebeheer geautomatiseerd ondersteund worden.

Doelstelling	Iedereen met een rol in het systeem-ontwikkeltraject kan op ieder moment beschikken over de juiste versie van een document, programma e.d.		
Risico	Als versiebeheer binnen het ontwikkel- en onderhoudstraject onvoldoende is ingericht of niet consequent wordt toegepast, bestaat het risico dat wordt gewerkt met onjuiste of verouderde versies van documentatie of programmacode, waardoor fouten in software-specificatie en -ontwikkeling ontstaan en incorrecte of inconsistente releases worden opgeleverd.		
Control	De projectorganisatie behoort in het systeem-ontwikkeltraject versiebeheer **procesmatig** en **efficiënt** ingericht te hebben.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procesmatig	1.	Het versiebeheerproces is beschreven, vastgesteld door het management en toegekend aan een verantwoordelijke functionaris.	CIP-netwerk
	2.	In het versiebeheerproces is vastgelegd welke applicatie-objecten in het ondersteunend tool, zoals het functioneel en technisch ontwerp en resultaten van sprints bij Agile-ontwikkeling, worden vastgelegd.	CIP-netwerk
	3.	Het versiebeheerproces wordt ondersteund met procedures en werkinstructies.	CIP-netwerk
Efficiënt	4.	Een versiebeheertool wordt toegepast die onder andere: • het vastleggen van versies van ontwikkelproducten ondersteunt; • het vastleggen van versies van programmacode ondersteunt; • het vastleggen van versies voorkomend in verschillende omgevingen (zoals OTAP) ondersteunt; • toegangsmogelijkheden voor verschillende rollen ondersteunt.	CIP-netwerk

5.3.3 *C.03 Patchmanagement*

Objectdefinitie

Besturingsproces voor het verwerven, testen en installeren van patches op een computersysteem.

Objecttoelichting

Naast zelfontwikkelde programmacode wordt ook veelvuldig gebruik gemaakt van code uit externe programmabibliotheken. Deze externe code kan fouten bevatten. Uit beveiligingsoogpunt is het raadzaam om code uit externe bibliotheken te testen en na te gaan of deze code beveiligd moet worden met door de codeleverancier beschikbaar gestelde patches.

Doelstelling	Het zekerstellen dat technische en softwarekwetsbaarheden tijdig en effectief worden aangepakt, om een stabiele omgeving te creëren.		
Risico	Als patches voor zelfontwikkelde en externe software niet tijdig worden verworven, getest en geïnstalleerd, bestaat het risico dat bekende kwetsbaarheden blijven bestaan, waardoor de stabiliteit en betrouwbaarheid van systemen worden aangetast en misbruik of verstoring van de dienstverlening kan optreden.		
Control	Patchmanagement behoort **procesmatig en procedureel** zodanig uitgevoerd te worden, dat van de gebruikte code tijdig vanuit externe bibliotheken informatie wordt ingewonnen over **technische kwetsbaarheden**, zodat **tijdig** de laatste (beveiligings)patches kunnen worden geïnstalleerd.		NSCS 2015: C.09
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procesmatig en procedureel	1.	Het patchmanagementproces en de noodzakelijke patchmanagementprocedures zijn beschreven, vastgesteld door het management en bekendgemaakt aan de ontwikkelaars.	NCSC 2015: C.09.01
	2.	De ontwikkelaars zijn bekend met hun formeel vastgelegde verantwoordelijkheden voor patchmanagement.	CIP-netwerk
	3.	Het al dan niet uitvoeren van patches voor programmacode is geregistreerd.	NCSC 2015: C.09.04
Technische kwetsbaar-heden	4.	Het beheer van technische kwetsbaarheden in de code uit externe bibliotheken omvat minimaal een risicoanalyse van de kwetsbaarheden en eventueel penetratietests en patching.	CIP-netwerk
	5.	Bij het ontwikkelen van code installeert de ontwikkelaar, tenzij risicoanalyses anders uitwijzen, alle noodzakelijke patches en fixes die door fabrikanten beschikbaar worden gesteld.	CIP-netwerk
Tijdig	6.	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik en ontstane schade hoog is, worden zo spoedig mogelijk doorgevoerd.	CIP-netwerk

5.3.4 *C.04 (Software)configuratiebeheer*

Objectdefinitie

Instandhoudingsproces voor het vastleggen en actueel houden van gegevens van configuratie-items van een computersysteem.

Objecttoelichting

Configuratiebeheer is het beheerproces dat onder andere verantwoordelijk is voor het registreren van de softwareconfiguratie-items (SCI's) en hun specifieke kenmerken, zodat de SCI's altijd uniek te identificeren zijn en de volledigheid en de juistheid van de in de Configuration Management Database (CMDB) opgenomen items gewaarborgd is. Configuratiemanagement geeft inzicht in de status van de verschillende SCI's die binnen het ontwikkeltraject worden gebruikt en geeft de relaties weer tussen deze SCI's. Hierdoor wordt duidelijk welke gevolgen aanpassingen van het ene SCI heeft voor andere SCI's.

Doelstelling	Het zorgen dat de vastgelegde gegevens van de softwareconfiguratie-items in de configuratie-administratie (CMDB) juist en volledig zijn en blijven.		
Risico	Als softwareconfiguratie-items niet volledig, actueel en juist worden vastgelegd en beheerd in de configuratie-administratie, bestaat het risico dat geen betrouwbaar inzicht bestaat in de gebruikte configuraties en onderlinge afhankelijkheden, waardoor wijzigingen onjuist worden doorgevoerd en de stabiliteit, beheersbaarheid en beveiliging van systemen worden aangetast.		
Control	De inrichting van het configuratiebeheer behoort waarborgen te bieden dat de vastgelegde gegevens van softwareconfiguratie-items in de **configuratie-administratie (CMDB)** juist en volledig zijn en blijven.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Configuratie-administratie (CMDB)	1.	Softwareconfiguratie-items worden volgens procedures en met hulpmiddelen vastgelegd.	CIP-netwerk
	2.	De configuratie-administratie is alleen toegankelijk voor hiertoe geautoriseerd personeel.	CIP-netwerk
	3.	Wijzigingen in softwareconfiguratie-items worden volgens een gestandaardiseerd proces vastgelegd in de CMDB.	CIP-netwerk

5.3.5 *C.05 Quality assurance*

Objectdefinitie

Proces dat zich richt op het beheersen en verbeteren van voortbrengingsprocessen.

Objecttoelichting

Om zekerheid te geven dat de juiste producten worden ontwikkeld en opgeleverd, is het van belang dat het voortbrengingsproces wordt onderworpen aan een kwaliteitscontrole (quality assurance). Quality assurance betreft alle activiteiten gericht op de ontwikkeling van software en richt zich onder andere op het toetsen van deelproducten en van de aanwezige risico's voor het verwerken van de juiste business

requirements en beveiligingseisen in de applicaties. Ook wordt nagegaan in hoeverre in de functionele en technische ontwerpen de beleidseisen en eisen uit wet- en regelgeving zijn meegenomen. Het is daarom van belang dat op bepaalde vastgestelde momenten quality assurance op de ontwikkelde software-producten wordt uitgevoerd.

Doelstelling	Het kunnen vaststellen van de betrouwbare werking van het ontwikkel- en onderhoudsproces voor de applicatieontwikkeling.		
Risico	Als quality-assurance-activiteiten binnen het ontwikkel- en onderhoudsproces niet structureel en aantoonbaar worden uitgevoerd, bestaat het risico dat onvoldoende zekerheid bestaat over de betrouwbaarheid van het proces en dat applicaties worden opgeleverd die niet voldoen aan afgesproken business-, beveiligings- en wettelijke eisen.		
Control	De projectorganisatie behoort een **quality assurance-proces** te hebben ingericht, waarmee zij de betrouwbare werking van het ontwikkel- en onderhoudsproces voor de applicatieontwikkeling kan vaststellen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Quality assurance-proces	1.	De projectorganisatie beschikt over een quality assurance-methodiek voor de ontwikkelde softwareproducten en ziet toe op de naleving van deze methodiek.	CIP-netwerk
	2.	Volgens de quality assurance-methodiek is een quality assurance-proces ingericht, voor het uitvoeren van quality assurance-activiteiten gedurende alle fasen van de ontwikkelcyclus en waarbij aandacht wordt besteed aan: • het evalueren van de requirementsanalyse, het ontwerp, de bouw, het testen en het opleveren van software; • het evalueren of de beveiligingscontrols (beleid, methoden en geprogrammeerde mechanismen voor de betrouwbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid) zoals overeengekomen tijdens het risico-assessment zijn ontwikkeld en adequaat functioneren; • het vaststellen of de ontwikkelmethodologie is opgevolgd.	CIP-netwerk
	3.	De resultaten uit de quality assurance-onderzoeken worden geapporteerd aan de verantwoordelijken die verbetermaatregelen initiëren.	CIP-netwerk
	4.	Toetsingsafspraken en -resultaten zijn beknopt en Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden (SMART) vastgelegd.	CIP-netwerk

5.3.6 *C.06 Compliance-management*

Objectdefinitie

Besturingsproces dat de toepassing van geldende wet- en regelgeving, organisatiebeleid en contracten bij softwareontwikkeling zeker stelt.

Objecttoelichting

Compliance-management richt zich op het naleven van de verplichtingen die voortkomen uit wet- en regelgeving en door de organisatie overeengekomen beleid, richtlijnen, standaarden en architectuur. Vanuit de optiek van de functionele en technische beveiligingseisen voor software is het van belang om met een compliance-managementproces vast te stellen in welke mate de gerealiseerde software voldoet aan de verplichtingen die voorvloeien uit wet- en regelgeving en uit vooraf overeengekomen beleid, architectuur, standaarden en contracten.

Doelstelling	Het reduceren van risico's en het vermijden van (im)materiële schade die kan voortvloeien uit het niet nakomen van wet- en regelgeving, overeenkomsten, beleid en andere verplichtingen.		
Risico	Als compliance-management binnen softwareontwikkeling onvoldoende is ingericht of toegepast, bestaat het risico dat wet- en regelgeving, contractuele verplichtingen en interne beleidskaders niet structureel worden nageleefd, waardoor de organisatie wordt blootgesteld aan juridische, financiële en reputatieschade en tekortkomingen in informatiebeveiliging niet tijdig worden onderkend.		
Control	De projectorganisatie behoort een **compliance-managementproces** ingericht te hebben, waarmee zij de implicaties uit wet- en regelgeving en verplichtingen voortvloeiend uit overeenkomsten en beleid kan vaststellen.		SoGP 2018: SI2.3.1 SoGP 2018: SI2.3.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Compliance management-proces	1.	Het compliance-managementproces, bestaande uit de sub-processen planning, evaluatie, rapportering en correctie/implementatie is gedocumenteerd en vastgesteld door het management.	CIP-netwerk
	2.	Voor het compliance-proces hebben de desbetreffende stakeholders de noodzakelijke eisen uit de verschillende bronnen samengevat en vastgelegd. Hierbij is aandacht geschonken aan: • wet- en regelgeving (AVG, wet Computercriminaliteit, Encryptie e.d.) die invloed hebben op het ontwikkelen van applicaties; • het vertalen van de wet- en regelgeving en het overeengekomen informatiebeveiligingsbeleid, de architectuur en de standaarden tot concrete maatregelen binnen het ontwikkelproces; • het rapporteren van de evaluatie van compliance-checks op wet- en regelgeving en overeengekomen beleid, architectuur en standaarden die beschikbaar zijn gesteld aan het management; • het vastleggen van de verplichtingen voor security-compliance in een autorisatiematrix.	CIP-netwerk

5.3.7 *C.07 Beheersorganisatie applicatieontwikkeling*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen die verantwoordelijk zijn voor de beheersing van softwareontwikkeling.

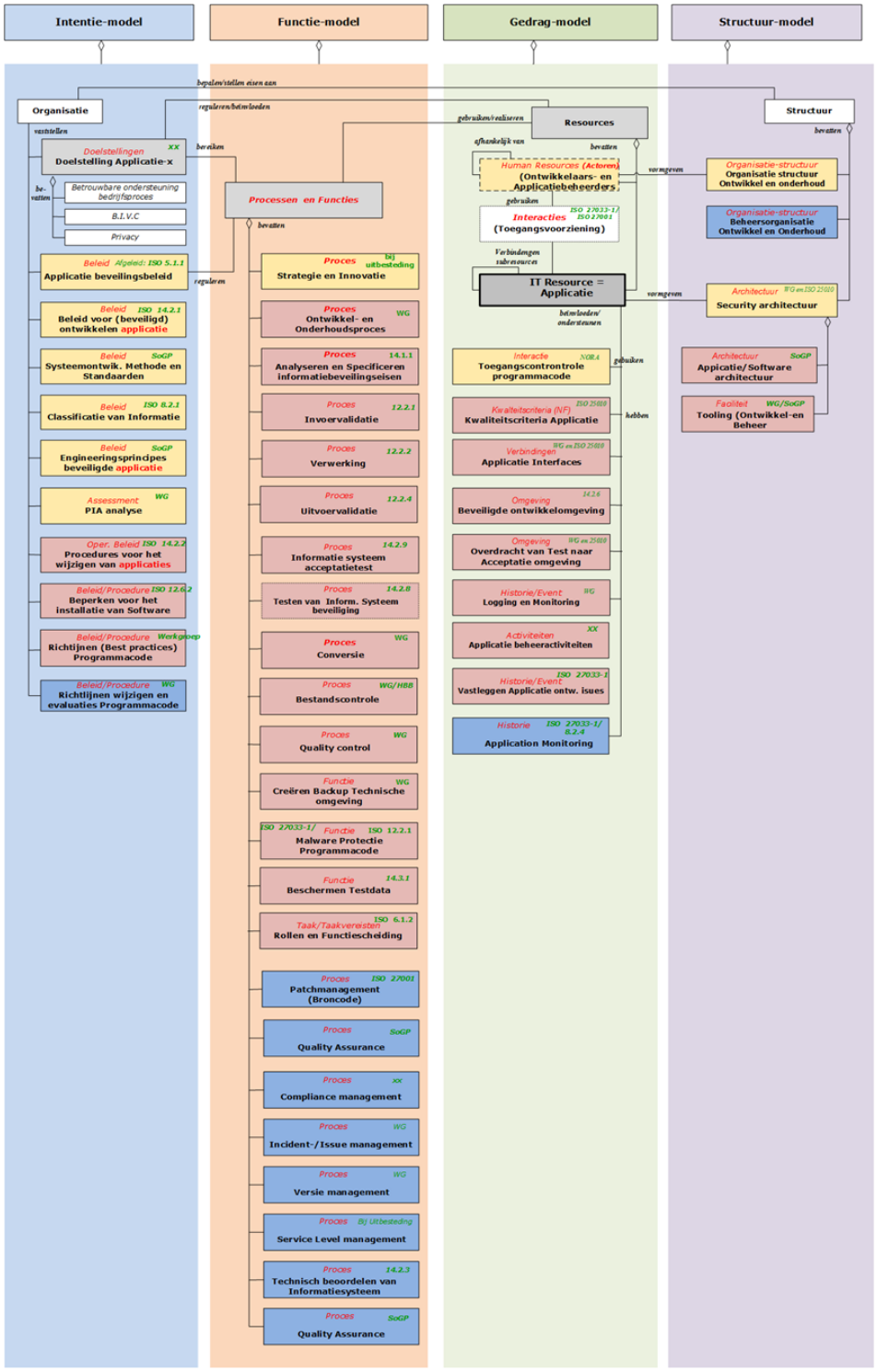
Objecttoelichting

De projectmanager heeft een (beheers)organisatiestructuur ingericht, waarbij de verantwoordelijkheden voor de beheersprocessen met toereikende bevoegdheden zijn uitgedrukt en op het juiste niveau zijn gepositioneerd.

Doelstelling	Het invullen, coördineren en borgen van de beheersing van softwareontwikkeling.		
Risico	Als de beheersorganisatie voor applicatieontwikkeling niet duidelijk is ingericht of onvoldoende effectief functioneert, bestaat het risico dat beheersprocessen, verantwoordelijkheden en bevoegdheden niet goed zijn afgestemd, waardoor de softwareontwikkeling niet consistent wordt aangestuurd en kwaliteits-, beveiligings- en beheersdoelstellingen niet worden gerealiseerd.		
Control	De projectverantwoordelijke behoort voor de software-ontwikkelprojecten een beheersorganisatie te hebben ingericht waarin de **structuur van de beheersprocessen** en van de betrokken **functionarissen** de **taken, verantwoordelijkheden en bevoegdheden** zijn vastgesteld.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Structuur van de beheers-processen	1.	De samenhang van de beheersprocessen wordt met een processtructuur vastgelegd.	CIP-netwerk
Functionaris-sen	2.	De belangrijkste functionarissen (stakeholders) voor de beheerorganisatie zijn benoemd en de onderlinge relaties zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk
Taken, verant-woordelijkhe-den en bevoegdheden	3.	De taken, verantwoordelijkheden en bevoegdheden voor de beheerprocessen zijn aan een specifieke functionaris toegewezen en vastgelegd.	CIP-netwerk
	4.	De projectorganisatie heeft de taken, verantwoordelijkheden en bevoegdheden voor het uitvoeren van de evaluatie- en beheerswerkzaamheden beschreven en de bijbehorende bevoegdheden vastgelegd in een autorisatiematrix.	CIP-netwerk

Bijlage 1: Objecten ingedeeld naar invalshoeken

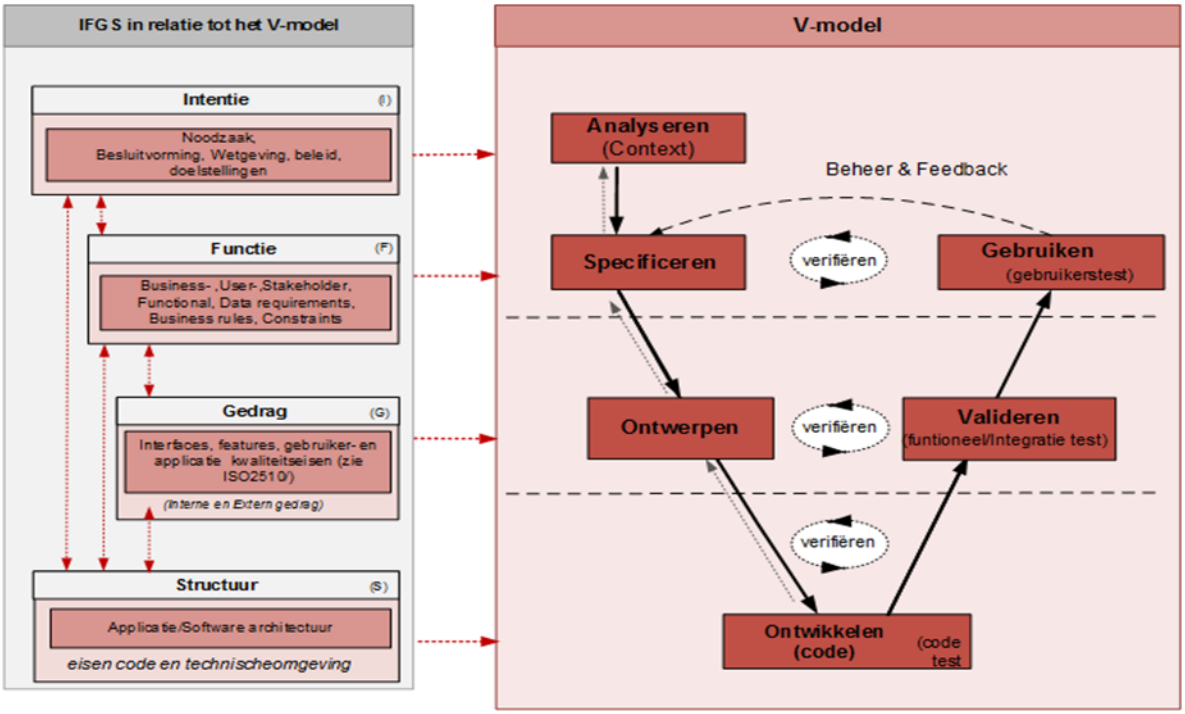
Afbeelding 6 geeft een overzicht van indegeelde objecten naar invalshoeken.



Afbeelding 6: Applicatieontwikkelingsobjecten ingedeeld naar invalshoeken

Bijlage 2: Invalshoeken gekoppeld aan het V-model

In de afbeelding 7 zijn de invalshoeken: intentie, functie, gedrag en structuur gekoppeld aan het V-model.



Afbeelding 7: Invalshoeken gekoppeld aan het V-model