Applicatieontwikkeling

BIO Thema-uitwerking

Maart 2023 [versie 2.2 definitief]

BIO Thema-uitwerking Applicatieontwikkeling

Titel	BIO Thema-uitwerking Applicatieontwikkeling
Datum	Maart 2023
Versie	2.2 definitief
Opdrachtgever	Directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Wiekram Tewarie (UWV) en Jaap van der Veen (CIP)
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

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.

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

u.01

1	Inleiding	6
1.1	Context applicatieontwikkeling	6
1.2	Doel applicatieontwikkeling	7
1.3	Scope en begrenzing applicatieontwikkeling	7
1.4	Ontwikkelcyclus applicatieontwikkeling	8
1.4.1	Perspectieven	9
1.4.2	Analyseren	10
1.4.3	Specificeren	10
1.4.4	Ontwerpen	10
1.4.5	Ontwikkelen (implementeren)	10
1.4.6	Valideren	11
1.4.7	Gebruiken	11
1.4.8	Onderhouden en beheren	11
1.5	Ontwikkelmethoden	11
1.6	Applicatieobjecten in relatie tot ontwikkelmethode	12
2	Beveiligingsobjecten applicatieontwikkeling	13
2.1	Organisatie van applicatieontwikkelingsobjecten	13
2.2	Observatie bij objectidentificatie	13
2.3	Objecten geprojecteerd op domein en gesorteerd naar invalshoek	14
3	Beleidsdomein	15
3.1	Doelstelling	15
3.2	Risico’s	15
3.3	Objecten, controls en maatregelen	15
3.3.1	B.01 Beleid voor (beveiligd) ontwikkelen	16
3.3.2	B.02 Systeem-ontwikkelmethode	17
3.3.3	B.03 Classificatie van informatie	18
3.3.4	B.04 Engineeringsprincipe voor beveiligde systemen	19
3.3.5	B.05 Business Impact Analyse (BIA)	20
3.3.6	B.06 Privacy en bescherming persoonsgegevens	21
3.3.7	B.07 Kwaliteitsmanagementsysteem	22
3.3.8	B.08 Toegangsbeveiliging op programmacode	23

3.3.9	B.09 Projectorganisatie	24
4	Uitvoeringsdomein	26
4.1	Doelstelling	26
4.2	Risico’s	26
4.3	Objecten, controls en maatregelen	26
4.3.1	U.01 Wijzigingsbeheerprocedure voor applicaties en systemen	27
4.3.2	U.02 Beperking software-installatie	28
4.3.3	U.03 Richtlijn programmacode	29
4.3.4	U.04 Analyse en specificatie informatiesysteem	30
4.3.5	U.05 Analyse en specificatie informatiebeveiligingseisen	32
4.3.6	U.06 Applicatie-ontwerp	32
4.3.7	U.07 Applicatiefunctionaliteit	33
4.3.8	U.08 Applicatiebouw	34
4.3.9	U.09 Testen systeembeveiliging	35
4.3.10	U.10 Systeemacceptatietest	36
4.3.11	U.11 Beschermen testgegevens	38
4.3.12	U.12 Beveiligde ontwikkelomgeving	38
4.3.13	U.13 Applicatiekoppeling	40
4.3.14	U.14 Logging en monitoring	41
4.3.15	U.15 Applicatie-architectuur	41
4.3.16	U.16 Tooling ontwikkelmethode	42
5	Control-domein	44
5.1	Doelstelling	44
5.2	Risico’s	44
5.3	Objecten, controls en maatregelen	44
5.3.1	C.01 Richtlijn evaluatie ontwikkelactiviteiten	45
5.3.2	C.02 Versiebeheer	46
5.3.3	C.03 Patchmanagement	47
5.3.4	C.04 (Software)configuratiebeheer	48
5.3.5	C.05 Quality assurance	49
5.3.6	C.06 Compliance-management	50
5.3.7	C.07 Technische beoordeling informatiesystemen	51
5.3.8	C.08 Beheersorganisatie applicatieontwikkeling	52

Bijlage 1: Objecten ingedeeld naar invalshoeken 53

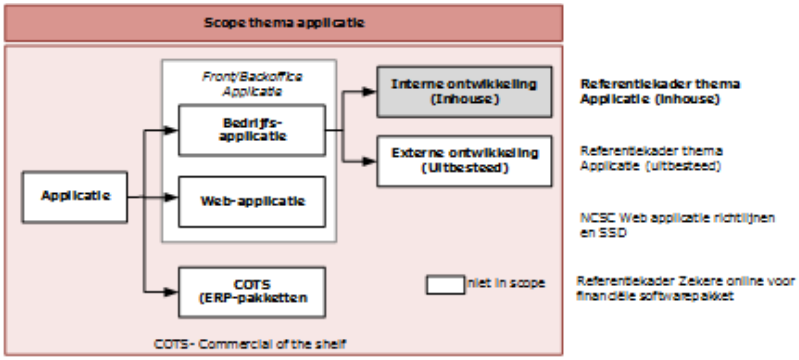
Bijlage 2: Invalshoeken gekoppeld aan het V-model 54

1 Inleiding

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, gevoeligheid van de gegevens, belang van de applicatie voor de organisatie bepalen of en welke normen van toepassing zijn.

1.1 Context applicatieontwikkeling

Dit document bevat de uitwerking van de BIO Thema-uitwerking Applicatieontwikkeling. 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 fa 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.

In deze BIO Thema-uitwerking zullen de beveiligingseisen voor applicatieontwikkeling worden samengesteld. Het uitgangspunt hierbij is de noodzakelijke beveiligingseisen, in de vorm van controls en onderliggende maatregelen uit de BIO en NEN-EN-ISO/IEC 27002:2017 (hierna genoemd ISO 27002), in een samenhangende context te plaatsen en waar nodig deze aan te vullen met controls uit andere ISO-standaarden, National Institute of Standards and Technology (NIST), The Standard of Good Practice (SoGP) 2018 e.d.

Eerst wordt een algemene ontwikkelcyclus beschreven om een beter beeld te krijgen over de te hanteren fases voordat de controls die gerelateerd zijn aan objecten worden geïdentificeerd. Deze exercitie is ook zinvol om geïdentificeerde objecten uit de BIO en overige best practices beter contextueel in samenhang te plaatsen. De beschrijving van de fases vindt plaats in paragraaf 1.4 Ontwikkelcyclus van applicatieontwikkeling.

1.2 Doel applicatieontwikkeling

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.

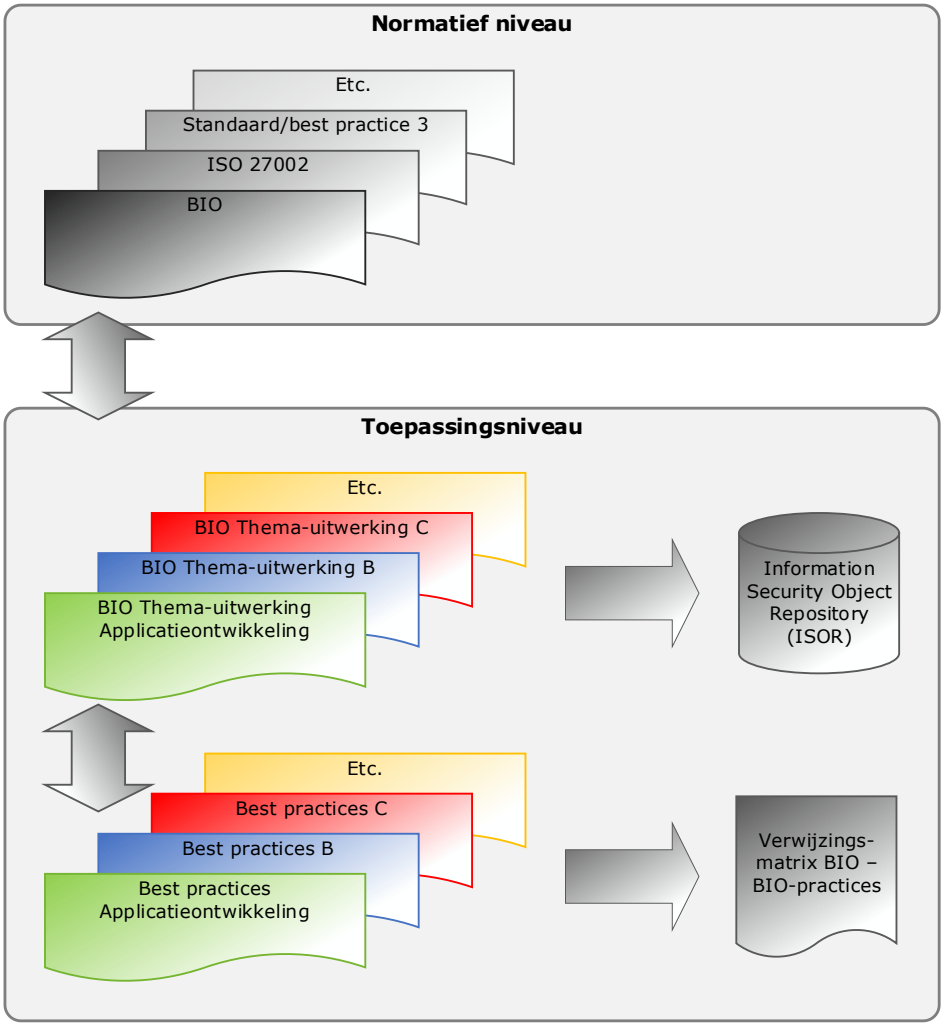
De thema-uitwerking geeft hiermee inzicht in de kwaliteitszorg die de leverancier dient toe te passen en wat de klant kan verwachten bij het opleveren van nieuwe software. Het geeft tegelijkertijd de verplichte activiteiten weer van de klant. Hiernaast kan het als instrument dienen voor het geven van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

1.3 Scope en begrenzing applicatieontwikkeling

In deze BIO Thema-uitwerking wordt voornamelijk gericht op conditionele beveiligings- en beheersingsaspecten die gerelateerd zijn aan het ontwikkelen van applicaties. Geen aandacht wordt besteed aan:

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

De begrenzing van dit document is in afbeelding 2 weergegeven.



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, of te wel een programma van eisen (PvE). Het PvE wordt ontwikkeld in samenwerking met informatieanalisten, softwareontwikkelaars en -gebruikers.

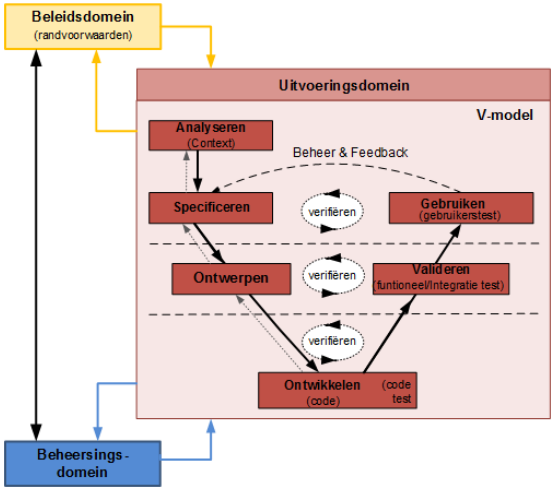
De kwaliteit (succes) van een applicatie wordt onder andere bepaald door:

- hoe goed het PvE de gebruikerseisen en -wensen weerspiegelt;
- hoe goed de gebruikerseisen en -wensen de reële situatie (daadwerkelijke noodzakelijkheden) weerspiegelt;
- hoe goed 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 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

Hiernaast 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 in afbeelding 3 weergegeven.

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 leverancierssperspectief en de linkerkant als het klantperspectief. Hierover maken de klant en leverancier heldere afspraken. De afspraken zijn gericht op:

- 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;

[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 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. Om een goede beheersing te waarborgen, is het vanuit best practices noodzakelijk de verschillende fases 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 de context van 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 over 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 tijdens in de eerdere fase gedetailleerde en vastgestelde uitwerking van informatie en modellen plaats. 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 met 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-features (eisen: 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, zoals:

- 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 (gebruikers)/het ontwerp (security by design) en de AVG).

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

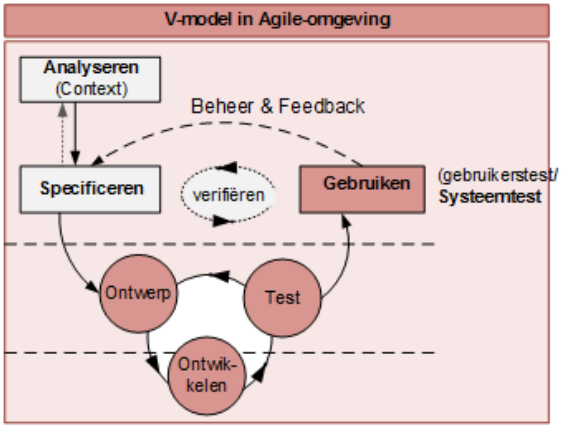
Er zijn verschillende modellen voor het ontwikkelen van applicaties, zoals de:

- Lineaire methode
  Het meest bekende voorbeeld is de Watervalmethode (zie paragraaf 1.4 Ontwikkelcyclus van applicatieontwikkeling). In deze ontwikkelmethode wordt het eindproduct (software-product) in een aantal fases 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 fases 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 productfeatures 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. Na de totstandkoming van dit thema kan met de definitieve versie een versie worden gemaakt die gerelateerd is aan applicatieonderhoud en een versie die gerelateerd is aan de Agile-methode. Dit zullen aparte documenten zijn die overeenkomsten zullen hebben met dit document, maar vanuit de optiek van onderhoud of Agile-aanpak kunnen objecten aangepast en/of toegevoegd worden.

2 Beveiligingsobjecten applicatieontwikkeling

Objecten voor applicatieontwikkeling worden gerelateerd aan de ontwikkelfasen en geïdentificeerd met onderzoeksvragen en risicogebieden. De objecten zijn afgeleid vanuit de optiek van de kwaliteitscriteria: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid (BIVC), die vervolgens zijn ingedeeld in het beleids-, uitvoerings- en control-domein.

De vragen die hierbij een rol spelen, zijn:

1. Welke randvoorwaardelijke elementen spelen vanuit de optiek van BIVC een rol bij applicatieontwikkeling en wat is de consequentie bij afwezigheid hiervan?
2. Welke elementen spelen vanuit de optiek van BIVC een rol bij applicatieontwikkeling en wat is de consequentie bij afwezigheid hiervan?
3. 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 contextuele samenhang gepositioneerd. De betekenis die aan elk domein wordt toegekend, zijn:

1. Beleid
   Binnen dit domein bevinden zich conditionele elementen over de 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 operationele activiteiten over het ontwikkelen 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 en/of het in standhouden van activiteiten die wel naar wens verlopen.

2.2 Observatie bij objectidentificatie

Er is gebleken dat bij het identificeren van objecten uit de BIO en de ISO 27002 weinig controls te vinden zijn die direct gerelateerd zijn aan de ontwikkelfases: analyseren, specificeren, ontwerpen en ontwikkelen. Dit komt doordat binnen deze ISO-standaard niet is uitgegaan van de ontwikkelfasen van systeemontwikkeling en wellicht ook doordat de activiteiten binnen deze fasen gerelateerd zijn aan specifieke methoden en/of programmeertalen. In de ISO 27002 zijn wel beveiligingscontrols en bijbehorende maatregelen aangetroffen 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. Vanuit een baseline-gebaseerde benadering is een lijst gemaakt van relevante objecten uit verschillende baselines. Los van de baselines zijn enkele objecten als relevant voor dit thema aangegeven. Ervan bewust zijnde dat deze zogenaamde baseline-gebaseerde benadering tot selectie van objecten leidt die niet allemaal in de huidig wereld van systeemontwikkelingsaanpak thuishoren. Er is gekozen om een baseline-benadering toe te passen om zo de overgang naar de Agile-benadering beter te kunnen maken.

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.

Opgemerkt wordt dat er verschillende termen gehanteerd worden voor hetzelfde, zoals: informatiesysteem, applicatie, systeem en toepassing. Voor de consistentie is gekozen om de term ‘systeem’ in de betiteling van de betreffende controls (dus de objecten) aan te passen naar applicatieontwikkeling.

3 Beleidsdomein

3.1 Doelstelling

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

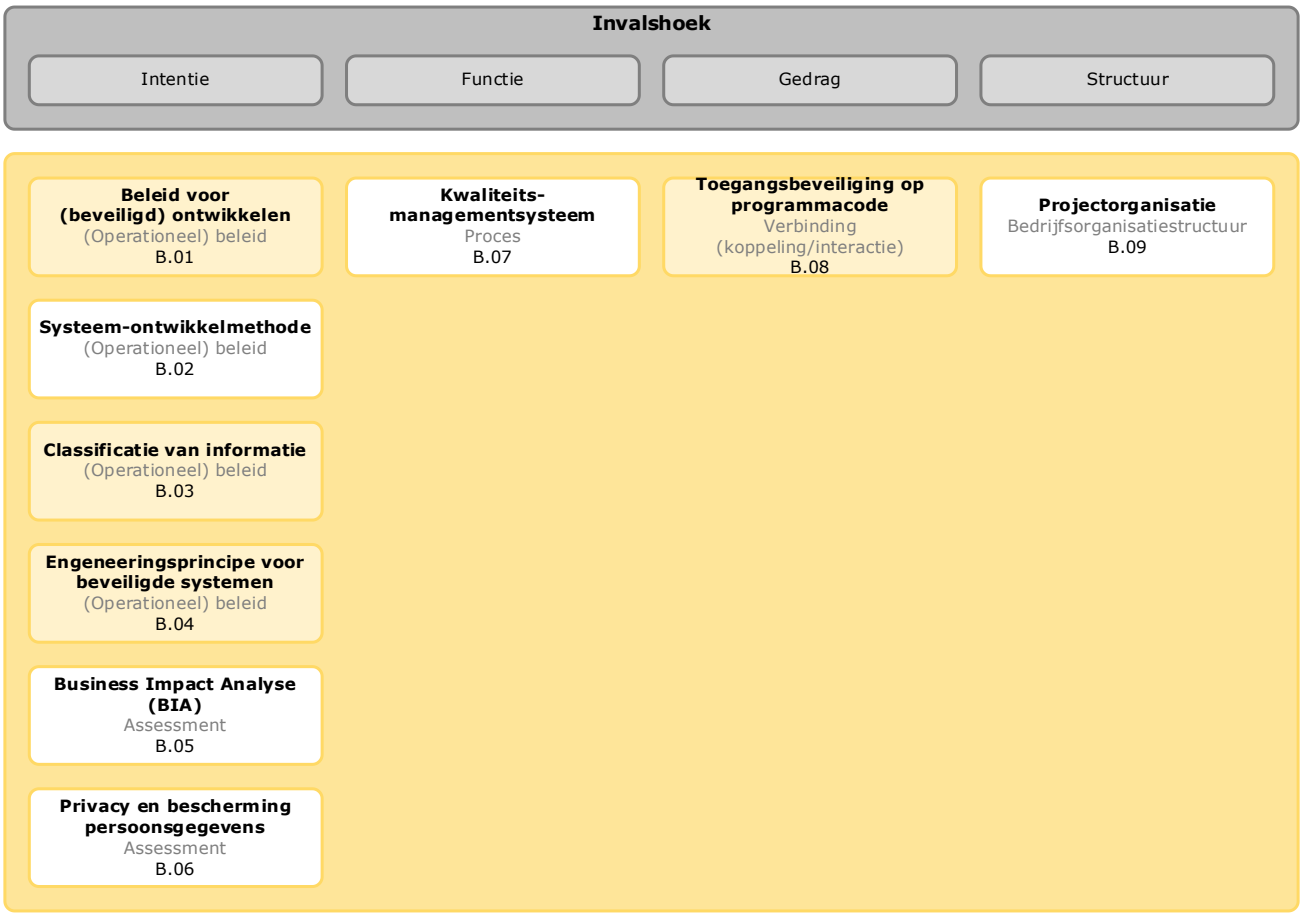
In dit domein worden objecten en daaraan gerelateerde normen opgenomen die het mogelijk maken de applicaties op een veilige manier te ontwikkelen.

3.2 Risico's

Wanneer de juiste beleidsaspecten voor het ontwikkelen van applicaties ontbreken, bestaat 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

Afbeelding 5 toont de objecten die specifiek voor dit domein een rol spelen. Het geeft een overzicht en de ordening van objecten. De geel gemarkeerde objecten komen voor in de BIO. 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 grijs gemarkeerde tekst). Ze zijn ingedeeld naar de invalshoek: Intentie, Functie, Gedrag of Structuur.



Afbeelding 5: Overzicht objecten voor applicatieontwikkeling in het beleidsdomein

3.3.1 B.01 Beleid voor (beveiligd) ontwikkelen

Objectdefinitie

Betreft het resultaat van een besluitvorming over welke regels en protocollen gehanteerd moeten worden om op een veilige wijze beveiligde applicaties te ontwikkelen.

Objecttoelichting

De ISO 27002 2017, artikel 14.2.1 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	Het beheersen van het (beveiligd) ontwikkelen van applicaties.

Risico	Onvoldoende mogelijkheid om sturing te geven aan de inrichting van het (beveiligd) ontwikkelen van applicaties.		
Control	Voor het ontwikkelen van software en systemen behoren **regels** te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.		BIO 2019: 14.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	BIO 2019: 14.2.1.1
	2.	De handreiking: Grip op Secure Software Development (SSD) is uitgangspunt voor de ontwikkeling van software en systemen.	BIO 2019: 14.2.1.1

	3.	In het beleid voor beveiligd ontwikkelen zijn de volgende aspecten in overweging genomen:
		• beveiliging van de ontwikkelomgeving;
		• richtlijnen over de beveiliging in de levenscyclus van softwareontwikkeling:
		  • beveiliging in de software-ontwikkelmethodologie;
		  • beveiligde coderingsrichtlijnen voor elke gebruikte programmeertaal;
		• beveiligingseisen in de ontwikkelfase;
		• beveiligingscontrolepunten binnen de mijlpalen van het project;
		• beveiliging van de versiecontrole;
		• vereiste kennis over toepassingsbeveiliging;
		• het vermogen van de ontwikkelaar om kwetsbaarheden te vermijden, te vinden en te repareren.
			ISO 27002 2017: 14.2.1a t/m g

	4.	Technieken voor beveiligd programmeren worden gebruikt voor nieuwe ontwikkelingen en hergebruik van code uit andere bronnen.	ISO 27002 2017: 14.2.1

3.3.2 B.02 Systeem-ontwikkelmethode

Objectdefinitie

Betreft een 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	De in gebruik genomen applicatie voldoet niet aan de eisen en wensen van de business, vereiste uit wet- en regelgeving, beveiligingsvereisten etc.		
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, zoals Structured System Analyses and Design Method (SSADM) of Scrum (Agile-ontwikkeling).	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

Betreft het systematisch indelen in categorieën van de waarde van informatie, om te kunnen bepalen welk niveau van bescherming de te ontwikkelen van applicaties nodig heeft.

Objecttoelichting

In ISO 27002 2017 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. Binnen dit thema moet de projectverantwoordelijke dit classificatieschema als input beschikbaar hebben om binnen deze context van de applicatie omgeving te kunnen toepassen. Het classificatieschema beidt specifieke richtlijnen voor het ontwikkeltraject.

Doelstelling	Het inzichtelijk maken welke mate van bescherming de informatie nodig heeft.		
Risico	Informatie wordt over of onder beveiligd.		
Control	**Informatie** behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.		BIO 2019: 8.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Informatie	1.	De handreiking: BIO-Dataclassificatie is het uitgangspunt voor de ontwikkeling van software en systemen.	BIO 2019: 8.2.1
	2.	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	BIO 2019: 8.2.1.1
	3.	Bij het ontwikkelen van applicaties is informatie beschermd conform de vereisten uit het classificatieschema.	ISO 27002 2017: 8.2.3
	4.	In het classificatieschema wordt rekening gehouden met de verplichtingen uit wet- en regelgevingen (onder andere privacy), organisatorische en technische requirements.	ISO 27002 2017: 8.2.1

3.3.4 B.04 Engineeringsprincipe voor beveiligde systemen

Objectdefinitie

Betreft een regel, norm of beginsel voor 'goed gedrag', specifiek voor het ontwikkelen van applicaties die beveiligd moeten worden.

Objecttoelichting

Bij het ontwikkelen van applicaties 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	Het continue hebben van een toegepaste beveiligingsbasis voor alle verrichtingen voor het implementeren van informatiesystemen.

Risico	Informatiebeveiligingsmaatregelen voor het implementeren van informatiesystemen zijn niet/minder effectief.		
Control	**Principes** voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.		BIO 2019: 14.2.1, 14.2.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Principes	1.	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	BIO 2019: 14.2.1.1
	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 Business Impact Analyse (BIA)

Objectdefinitie

Betreft een methode om de mogelijke bedrijfsimpact te bepalen die een organisatie zou kunnen ervaren door een incident, die de functionaliteit van of de informatie in een applicatie in gevaar brengt.

Objecttoelichting

Eén van de specifieke activiteiten bij applicatieontwikkeling is het uitvoeren van een BIA. Hierbij wordt vanuit verschillende optieken de doelomgeving geanalyseerd, om op deze manier de juiste requirements voor de te ontwikkelen applicatie te kunnen identificeren en traceren.

Doelstelling	Het vaststellen van een mogelijke bedrijfsimpact die de verantwoordelijke wil accepteren, in het geval de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie wordt aangetast.	
Risico	De gekozen beveiligingsmaatregelen sluiten niet aan bij de bedrijfsimpact door een beveiligingsincident.	
Control	De BIA behoort te worden uitgevoerd vanuit verschillende **perspectieven**, zich te richten op verschillende **scenario's** en vast te stellen welke impact de **aspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid** hebben op de organisatie.	SoGP 2018: IR2.2, BIO 2019 14.2.7.1
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Perspectieven	1.	Bij de business impact analyse worden onder andere de volgende perspectieven in beschouwing genomen: • de relevante stakeholders (business owners, business- en IT-specialisten); • de scope van de risico-assessment; • het profiel van de 'doelomgeving'; • de aanvaardbaarheid van risico's in de doelomgeving.	SoGP 2018: IR2.2.1 SoGP 2018: IR2.2.3e
Scenario's	2.	De business impact analyse richt zich op verschillende scenario's met aandacht voor: • de hoeveelheid mensen die nadelig beïnvloed worden; • de hoeveelheid systemen die out-of-running kan raken; • een realistische analyse en een analyse van worst-case situaties.	SoGP 2018: IR2.2.4
Aspecten beschikbaar-heid, integriteit, vertrouwelijk en controleer-baarheid	3.	Met de business impact analyse wordt vastgesteld op welke wijze een eventuele inbreuk op de aspecten beschikbaarheid, integriteit, vertrouwelijkheid- en controleerbaarheid invloed hebben op de financiën van de organisatie in termen van: • Verlies orders, contracten en klanten • Verlies tastbare assets • Onvoorziene kosten • Verlies managementcontrol • Concurrentie • Late leveringen • Verlies productiviteit • Compliance • Reputatie	SoGP 2018: IR2.2.5

3.3.6 B.06 Privacy en bescherming persoonsgegevens

Objectdefinitie

Privacy betreft de persoonlijke vrijheid, het recht om alleen gelaten te worden. Bescherming persoonsgegevens betreft het proces van de bescherming van deze gegevens.

Objecttoelichting

Bij applicatieontwikkeling behoort de verantwoordelijke stakeholder rekening te houden met privacy en de bescherming van persoonsgegevens. Privacybescherming betekent een contextanalyse verrichten van de situatie waarin de desbetreffende applicatie ontwikkeld wordt. Hierbij wordt voorkomen dat eventuele inbreuk ontstaat op de persoonlijke levenssfeer van de personen waarvan persoonsgegevens worden verwerkt. Om inbreuk op de privacy vast te stellen, wordt voorafgaand aan het ontwerp van de applicatie een PIA uitgevoerd voor waarschijnlijk hoog risicoverwerkingen. Deze verplichting komt voort uit de AVG.

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

Risico	Betrokkenen van wie of over wie persoonsgegevens gaan, leiden schade door ongeoorloofde of onbedoelde toegang tot persoonsgegevens, ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens.		
Control	Bij het ontwikkelen van applicaties behoren **privacy en bescherming van persoonsgegevens**, voor zover van toepassing, te worden gewaarborgd volgens relevante **wet- en regelgeving**.		BIO 2019: 18.1.4
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.	Conform 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

Omvat activiteiten waarmee de organisatie haar doelstellingen identificeert en vaststelt welke processen en middelen vereist zijn om gewenste resultaten te behalen (zie NEN-EN-ISO 9000:2015 Kwaliteitsmanagementsysteem - Grondbeginselen en verklarende woordenlijst).

Objecttoelichting

De doelorganisatie 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	Het kwaliteitsniveau van de applicatieontwikkeling en -onderhoud is te laag of te hoog.	
Control	De doelorganisatie behoort conform 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.	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

Betreft de geautoriseerde toegang tot gevalideerde broncode[2] (source code) voor het bouwen van applicaties.

Objecttoelichting

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

Doelstelling	Het zorgen dat alleen die personen die toegang nodig hebben voor het uitvoeren van hun werkzaamheden toegang krijgen tot de programmabroncodebibliotheken en samenhangende elementen.	
Risico	Onbevoegde toegang tot programmabroncodebibliotheken en samenhangende elementen.	
Control	Toegang tot de **programmabroncodebibliotheken** behoren te worden beperkt.	BIO 2019: 9.4.5
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

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

Programma-broncodebibli-otheken	1.	Om de toegang tot broncodebibliotheken te beheersen en zo de kans op het corrupt raken van computerprogramma's te verkleinen, worden de volgende richtlijnen in overweging genomen: • De broncodebibliotheken worden niet in operationele systemen opgeslagen. • De programmacode en de broncodebibliotheek behoren te worden beheerd conform vastgestelde procedures. • Ondersteunend personeel heeft geen onbeperkte toegang tot broncodebibliotheken. • Het updaten van de programmacode en samenhangende items en het verstrekken van de programmacode aan programmeurs vinden alleen plaats na ontvangst van een passend autorisatiebewijs. • Programma-uitdraaien worden in een beveiligde omgeving bewaard. • Van elke toegang tot broncodebibliotheken wordt een registratie bijgehouden in een auditlogbestand. • Onderhoud en het kopiëren van programmacode in bibliotheken zijn aan strikte procedures voor wijzigingsbeheer onderworpen.	ISO 27002 2017: 9.4.5a t/m g
	2.	Als het de bedoeling is dat de programmabroncode wordt gepubliceerd, behoren aanvullende beheersmaatregelen die bijdragen aan het waarborgen van de integriteit ervan (bijvoorbeeld een digitale handtekening) te worden overwogen.	ISO 27002 2017: 9.4.5

3.3.9 B.09 Projectorganisatie

Objectdefinitie

Betreft een doelgerichte bundeling van kennis en vaardigheden tussen personen die verantwoordelijk zijn voor projectmatige softwareontwikkeling.

Objecttoelichting

Binnen de (project-)organisatie is een beveiligingsfunctionaris betrokken die verantwoordelijkheid draagt bij het ondersteunen van applicatieontwikkelingen (projecten). Binnen het project heeft hij de specifieke taak gericht op het vervaardigen van beveiligingsvoorschriften. De expliciete taken, verantwoordelijkheden en bevoegdheden van de beveiligingsfunctionaris zijn vooraf expliciet benoemd en vastgesteld. De beveiligingsfunctionaris ziet toe op het naleven van het informatiebeveiligingsbeleid en architectuurvoorschriften. Ook staat vast hoe de rapporteringslijnen zijn uitgestippeld.

Doelstelling	Het ondersteunen van de (project-)organisatie voor informatiebeveiliging in het applicatie-ontwikkeltraject.	
Risico	Informatiebeveiliging wordt onvoldoende meegenomen in het systeem-ontwikkeltraject.	
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 applicatieontwikkeling in het uitvoeringsdomein is het waarborgen dat de ontwikkel- en onderhoudsactiviteiten plaatsvinden conform specifieke beleidsuitgangspunten en dat de werking daarvan 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.

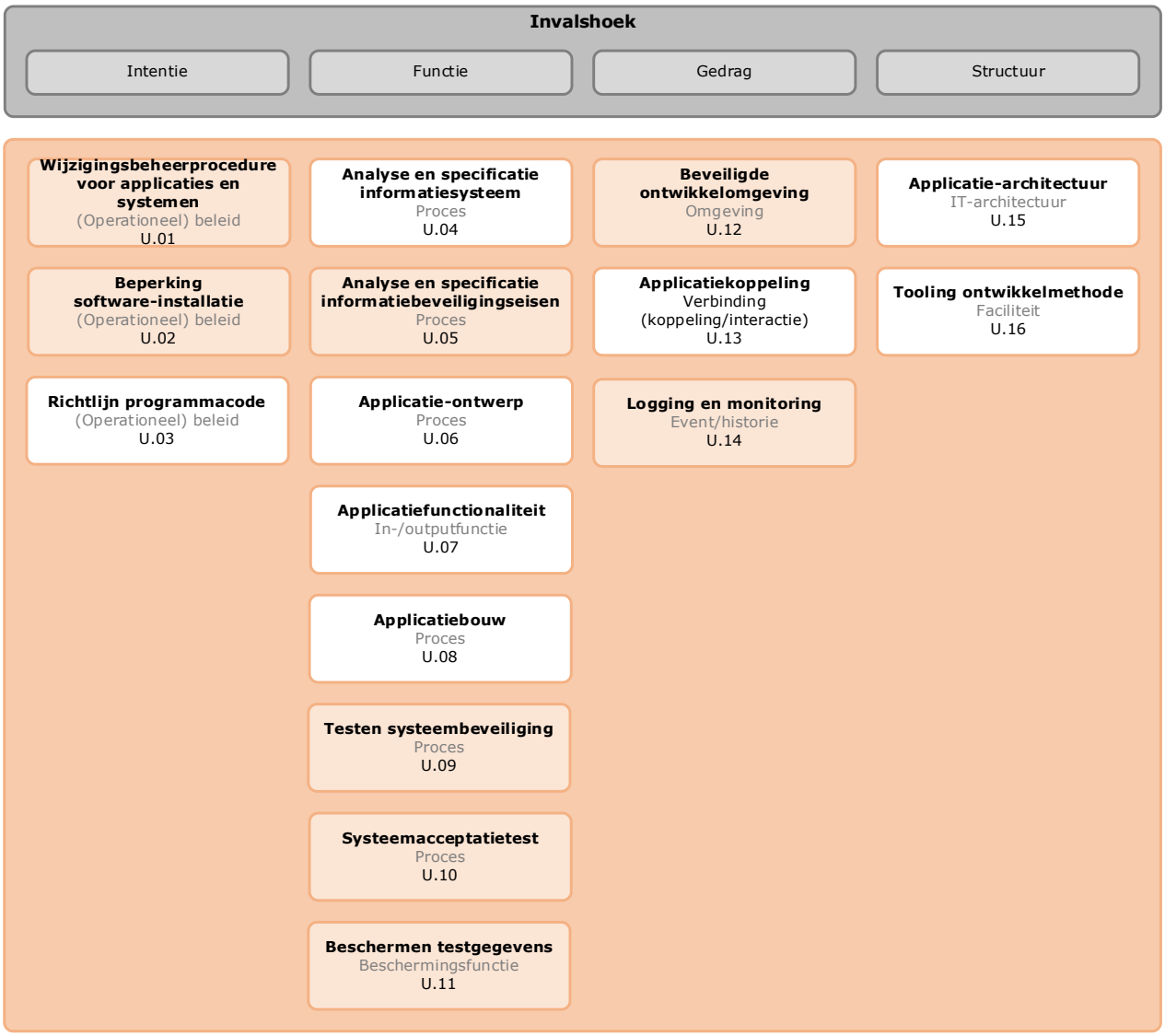
4.2 Risico's

Wanneer adequate normen voor applicatieontwikkeling en onderhoud ontbreken, bestaat het risico dat deze activiteiten plaatsvinden met onjuiste gronden of dat het fundament waarop deze activiteiten steunen niet aan het juiste beveiligingsniveau voldoen.

Zo kan door het ontbreken van richtlijnen en procedures voor activiteiten binnen de verschillende omgevingen software in de productieomgeving geïnstalleerd worden die fouten bevat waardoor productiegegevens ernstig aangetast kunnen worden.

4.3 Objecten, controls en maatregelen

Binnen het uitvoeringsdomein worden specifieke inrichtings- en beveiligingsobjecten voor applicatieontwikkeling beschreven. Per object worden conformiteitsindicatoren en de desbetreffende implementatie-elementen uitgewerkt. De rood gemarkeerde objecten komen voor in de BIO. De wit gemarkeerde objecten zijn betrokken uit andere best practices, zie afbeelding 6. De objecten zijn ingedeeld naar intentie, functie, gedrag en structuur. In bijlage 2 Invalshoeken gekoppeld aan het V-model zijn de invalshoeken gekoppeld aan het V-model.



Afbeelding 6: Overzicht objecten voor applicatieontwikkeling in het uitvoeringsdomein

4.3.1 U.01 Wijzigingsbeheerprocedure voor applicaties en systemen

Objectdefinitie

Omvat een 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	Doorgevoerde wijzigingen aan systemen zijn niet volledig en gecontroleerd.		
Control	Wijzigingen aan systemen binnen de **levenscyclus** van de ontwikkeling behoren te worden beheerst door het gebruik van **formele procedures** voor wijzigingsbeheer.		BIO 2019: 12.1.2, 14.2.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Levenscyclus	1.	Wijzigingsbeheer vindt plaats op basis van algemeen geaccepteerde beheerframeworks, zoals Information Technology Infrastructure Library (ITIL), Application Services Library (ASL), Business Information Services Library (BiSL), Scrum, SIG en SSD.	BIO 2019: 14.2.2.1
	2.	Het wijzigingsproces voor applicaties is zodanig ingericht dat medewerkers (programmeurs) de juiste autorisatie krijgen om hun werkzaamheden te kunnen uitvoeren.	ISO 27002 2017: 14.2.2
Formele procedures	3.	Nieuwe systemen en belangrijke wijzigingen aan bestaande systemen volgen een formeel proces van indienen, prioriteren, besluiten, impactanalyse, vastleggen, specificeren, ontwikkelen, testen, kwaliteitscontrole en implementeren.	ISO 27002 2017: 14.2.2
	4.	Enkele elementen van procedures voor wijzigingsbeheer zijn: • Alle wijzigingsverzoeken/Request for Changes (RFC's) verlopen volgens een formele wijzigingsprocedure (ter voorkoming van ongeautoriseerde wijzigingsaanvragen). • Het generieke wijzigingsproces heeft aansluiting met functioneel beheer. • Wijzigingen worden doorgevoerd door bevoegde medewerkers. • Van elk wijzigingsverzoek wordt de impact op de geboden functionaliteit beoordeeld. • Uitvoering en bewaking van de verantwoordelijkheden/taken zijn juist belegd. • Aanvragers van wijzigingen worden periodiek geïnformeerd over de status van hun wijzigingsverzoek.	ISO 27002 2017: 14.2.2b

4.3.2 U.02 Beperking software-installatie

Objectdefinitie

Betreft 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, om een bepaald type data-analyse in de business-omgeving te kunnen uitvoeren;
2. Softwareontwikkelaars, voor requirementsspecificatie, het creëren van datamodellen en het genereren van de programmacode;
3. Technische beheerders, voor het beheren van servers en netwerkcomponenten.

Deze BIO Thema-uitwerking is gericht op eisen die gerelateerd zijn aan het installeren van software door ontwikkelaars voor het specificeren van gebruikersrequirements. Hierbij kan gedacht worden aan het toekennen van minimale rechten aan ontwikkelaars om additionele hulpsoftware te installeren of het toekennen van rechten die gerelateerd zijn aan de regels: need-to-use, need-to-know, need-to-modify, need-to-delete. Het doel hiervan is om risico's die gerelateerd zijn aan het onbedoeld wijzigen van kritische assets (zoals informatie, software, applicaties en system security controls) te beperken.

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	Het introduceren van kwetsbaarheden in de software.		
Control	Voor het door gebruikers/ontwikkelaars installeren van software behoren **regels** te worden vastgesteld en te worden geïmplementeerd.		BIO 2019: 12.6.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	De organisatie heeft een strikt beleid gedefinieerd voor de software die ontwikkelaars mogen installeren.	ISO 27002 2017: 12.6.2
	2.	Het toekennen van rechten om software te installeren vindt plaats met 'least privilege'.	ISO 27002 2017: 12.6.2
	3.	De rechten worden verleend met de rollen van de typen gebruikers en ontwikkelaars.	ISO 27002 2017: 12.6.2

4.3.3 U.03 Richtlijn programmacode

Objectdefinitie

Betreft systematisch ontwikkelde aanbevelingen voor de broncode van een applicatie.

Objecttoelichting

De programmacode wordt ontwikkeld door bepaalde typen ontwikkelaars. Het ontwikkelen is geen eenmalige activiteit en vindt plaats langs een cyclisch proces van ontwikkelen, testen en verbeteren. Voor een effectieve inrichting van dit cyclische proces nemen ontwikkelaars regels in acht, waarbij zij gebruik maken van afgesproken best practices. Zonder deze regels en afspraken bestaat 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 die effectief onderhoudbaar is.
Risico	Het voortbrengingsproces van de applicatie raakt verstoord.

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

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

Objecttoelichting

Het analyseren en specificeren van requirements is een proces van het traceren en onderkennen van functionele en niet-functionele requirements waar de te ontwikkelen applicatie aan moet voldoen. Ook worden de constraints geïdentificeerd die zullen gelden in de ontwikkel- en de operatiefases.

BIO Thema-uitwerking Applicatieontwikkeling

Het ontwikkelen van informatiesystemen wordt tegenwoordig veelal uitgevoerd conform 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 (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 met lineaire volgens het V-modelaanpak uitgewerkt. Aangezien bij Agile niet op deze wijze wordt gewerkt, verdient dit aspect extra aandacht.

Doelstelling	Een basis leggen voor de volgende fases (de ontwerpfase en verder) met geanalyseerde en gespecificeerde functionele eisen.		
Risico	In het technisch ontwerp en verder zijn niet alle noodzakelijke functionele eisen meegenomen.		
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 Analyse en specificatie informatiebeveiligingseisen

Objectdefinitie

Betreft een systematisch onderzoek naar en het vaststellen van informatiebeveiligingseisen voor een applicatie.

Objecttoelichting

Het object Analyse en specificatie informatiebeveiligingseisen heeft betrekking op niet-functionele eisen, zoals betrouwbaarheid, gebruiksvriendelijkheid, efficiëntie, onderhoudbaarheid, performance en flexibiliteit in overdraagbaarheid.

Doelstelling	Het waarborgen dat de informatiebeveiligingseisen integraal onderdeel uitmaken van de eisen van informatiesystemen (nieuw en uitgebreid).		
Risico	Het ontbreken van informatiebeveiligingseisen voor nieuwe of uit te breiden informatiesystemen.		
Control	De **beveiligingseisen** die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen en voor uitbreidingen van bestaande informatiesystemen.		BIO 2019: 14.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-eisen	1.	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	BIO 2019: 14.1.1.1
	2.	De Handreikingen: Risicoanalysemethode en Risicomanagement ISO 27005 zijn uitgangspunt voor de ontwikkeling van software en systemen.	BIO 2019: 14.1.1.1
	3.	Informatiebeveiligingseisen zijn al in de ontwerpfase afgeleid uit: • beleidsregels en wet- en regelgeving; • context- en kwetsbaarheidsanalyse van de te ondersteunen bedrijfsprocessen; • afspraken met en afhankelijkheden van ketenpartijen.	ISO 27002 2017: 14.1.1
	4.	Voor informatiesystemen worden onder andere de volgende informatiebeveiligingseisen in overweging genomen: • authenticatie eisen van gebruikers; • toegangsbeveiligingseisen; • eisen over beschikbaarheid, integriteit en vertrouwelijkheid; • eisen afgeleid uit bedrijfsprocessen; • eisen gerelateerd aan interfaces voor het registreren en monitoren van systemen.	ISO 27002 2017: 14.1.1a, b, d, e en f

4.3.6 U.06 Applicatie-ontwerp

Objectdefinitie

Betreft specificaties vastgelegd in tekst en beeld van een computerprogramma.

Objecttoelichting

Tijdens de ontwerpfase worden de (niet-)functionele requirements omgezet naar een uitvoerbaar informatiesysteem. 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 toegepaste 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	In het applicatieontwerp ontbreekt vereiste informatie.		
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

Omvat toepassingsfuncties die ondersteuning bieden aan 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 bedrijfsproces optimaal te ondersteunen.		
Risico	Het informatiesysteem ondersteunt het betreffende bedrijfsproces niet maximaal.		
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 conform vastgestelde beveiligingsklasse gevalideerd op plausibiliteit, volledigheid en bedrijfsgevoeligheid.	CIP-netwerk

4.3.8 U.08 Applicatiebouw

Objectdefinitie

Betreft het ontwikkelen van een programmacode.

Objecttoelichting

Bevat een concrete reeks instructies die een computer kan uitvoeren in een programmeertaal.

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 good practices, methoden/technieken en bepaalde beveiligingsuitgangspunten.

Doelstelling	Het zorgen dat er geen zwakke punten in de veiligheid worden geïntroduceerd en dat applicaties in staat zijn om kwaadaardige aanvallen te weerstaan.		
Risico	De opgeleverde programmuurcode is niet veilig.		
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 die ook het volgende specificeren: • dat een goedgekeurde methode voor applicatiebouw wordt gehanteerd; • dat 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 Testen systeembeveiliging

Objectdefinitie

Betreft het toetsen of een systeem voldoet aan de vooraf gestelde beveiligingseisen.

Objecttoelichting

Bij het object Testen systeembeveiliging gaat het om het testen van het totale informatiesysteem dat ontwikkeld wordt. Tijdens het ontwikkelproces worden in verschillend stadia verschillende tests uitgevoerd. Hierbij worden onder andere onder diverse omstandigheden tests uitgevoerd op input, verwerkingen en verwachte output. Na integratie van het informatiesysteem in de infrastructuur wordt specifiek vanuit beveiligingsoptiek getest.

Doelstelling	Het nagaan of de applicatie met zijn bedrijfs- en beveiligingsfunctionaliteiten werkt conform de eerder vastgelegde eisen.		
Risico	Bedrijfs- en beveiligingsfunctionaliteiten werken niet zoals beoogd.		
Control	Tijdens ontwikkelactiviteiten behoren zowel **bedrijfsfunctionaliteiten** als de **beveiligingsfunctionaliteiten** te worden getest.		BIO 2019: 14.2.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Bedrijfsfunc-tionaliteiten	1.	Vanuit de interne optiek van de organisatie richten bepaalde typen functionarissen zich tijdens de ontwikkelactiviteiten en in relatie tot de beveiligingseisen op het testen van functionele requirements (onder andere business rules).	CIP-netwerk
Beveiligings-functionalitei-ten	2.	De functionaliteiten worden na integratie van de ontwikkelde software (nogmaals) specifiek vanuit beveiligingsoptiek getest in de infrastructuur.	CIP-netwerk

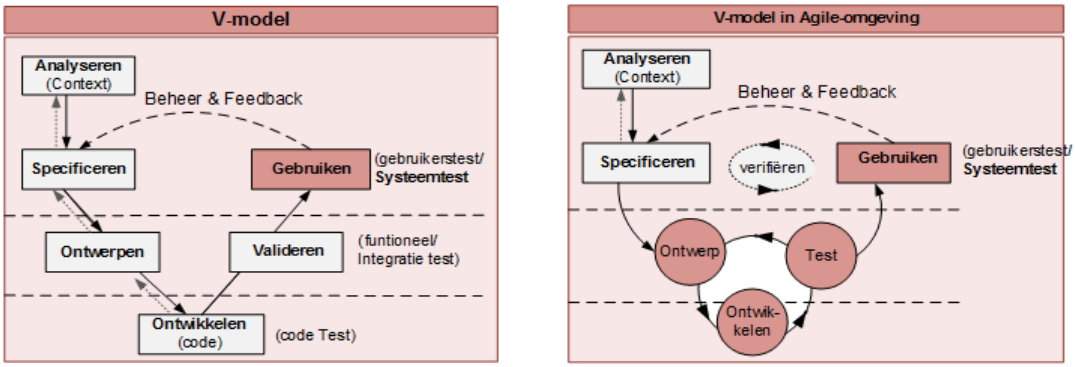
4.3.10 U.10 Systeemacceptatietest

Objectdefinitie

Betreft de eindtoets of een applicatie al dan niet geaccepteerd kan 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 7 geïllustreerd voor beide methoden.



Afbeelding 7: Systeemtest bij de Waterval- en Agile-methode

Doelstelling	Toetsen of de requirements adequaat in het uiteindelijke product, het nieuwe informatiesysteem, zijn verwerkt.		
Risico	Tijdens het gebruik van een informatiesysteem komen onvolkomenheden (afwijkingen op beveiligingseisen, functionele eisen, gebruikerseisen, businesseisen en business rules) voor het eerst aan het licht.		
Control	Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van **acceptatietests** en gerelateerde criteria te worden vastgesteld.		BIO 2019: 14.2.9
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Acceptatie-tests	1.	Voor acceptatietesten van (informatie)systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd worden uitgevoerd.	BIO 2019: 14.2.9.1
	2.	Van de resultaten van de testen wordt een verslag gemaakt.	BIO 2019: 14.2.9.2
	3.	Testresultaten worden formeel geëvalueerd en door de betrokken informatiesysteemeigenaar beoordeeld, waarna - na te zijn goedgekeurd - overgegaan wordt naar de volgende fase.	CIP-netwerk
	4.	Acceptatietesten worden uitgevoerd in een representatieve acceptatie-testomgeving. Deze omgeving is vergelijkbaar met de toekomstige productieomgeving.	ISO 27002 2017: 14.2.9
	5.	Voordat tot acceptatie in de productieomgeving wordt overgegaan, worden acceptatiecriteria vastgesteld en passende testen uitgevoerd.	ISO 27002 2017: 14.2.9
	6.	Tenzij geanonimiseerd worden productiegegevens niet gebruikt als testgegevens.	ISO 27002 2017: 14.3.1

	7.	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

4.3.11 U.11 Beschermen testgegevens

Objectdefinitie

Betreft het beschermen 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 en aangepast. Testgegevens dienen zorgvuldig te worden gekozen, beschermd en gecontroleerd.

Doelstelling	Het vermijden van persoonsgegevens of enige andere vertrouwelijke informatie voor testdoeleinden en de bescherming waarborgen van gegevens die voor het testen van informatiesystemen zijn gebruikt.		
Risico	De beschikbaarheid, integriteit en/of vertrouwelijkheid van testgegevens worden aangetast.		
Control	**Testgegevens** behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.		BIO 2019: 14.3.1
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 gelden voor besturingssystemen gelden ook voor testsystemen; • voor elke keer dat besturingsinformatie naar een testomgeving wordt gekopieerd, wordt een afzonderlijke autorisatie verkregen; • besturingsinformatie wordt onmiddellijk na voltooiing van het testen uit een testomgeving verwijderd; • van het kopiëren en gebruiken van besturingsinformatie wordt verslaglegging bijgehouden om in een audittraject te voorzien.	ISO 27002 2017: 14.3.1a t/m d

4.3.12 U.12 Beveiligde ontwikkelomgeving

Objectdefinitie

Betreft een omgeving die uitsluitend wordt gebruikt om applicaties te creëren of aan te passen.

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	De beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie in een operationele applicatie worden aangetast.		
Control	Organisaties behoren **beveiligde ontwikkelomgevingen** vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie en die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.		BIO 2019: 12.1.4, 14.2.6
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligde ontwikkel-omgevingen	1.	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging. Deze afweging heeft zowel de ontwikkelomgeving als ook het te ontwikkelen systeem in scope.	BIO 2019: 14.2.6.1
	2.	De organisatie heeft logische en/of fysieke scheidingen aangebracht tussen de ontwikkel-, test-, acceptatie- en productie-omgeving, elk met een eigen autorisatiestructuur en werkwijze, zodat sprake is van een beheerst ontwikkel- en onderhoudsproces.	ISO 27002 2017: 12.1.4

	3.	De taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen in de ontwikkel-, test-, acceptatie- en productie-omgevingen worden uitgevoerd conform onderkende rollen.	CIP-netwerk
	4.	Voor remote-werkzaamheden is een werkwijze vastgelegd.	SoGP 2018: PM1.3.1
	5.	Ontwikkelaars hebben geen toegang tot de productieomgeving.	CIP-netwerk
	6.	Voor het kopiëren/verplaatsen van configuratie-items tussen de omgevingen gelden overdrachtsprocedures.	CIP-netwerk
	7.	De overdracht van de ontwikkel- naar de testomgeving vindt gecontroleerd plaats met een implementatieplan.	CIP-netwerk
	8.	De overdracht van de test- naar de acceptatie-omgeving vindt procedureel door daartoe geautoriseerde personen plaats.	CIP-netwerk
	9.	De overdracht naar de productie-omgeving vindt procedureel door daartoe geautoriseerde personen plaats.	CIP-netwerk

4.3.13 U.13 Applicatiekoppeling

Objectdefinitie

Betreft een 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 dienen dit soort koppelingen aan bepaalde eisen te voldoen.

Doelstelling	Het kunnen leveren van de juiste services en de informatiebeveiliging van de betrokken applicaties te kunnen waarborgen.		
Risico	Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van data/informatie van de in ontwikkeling zijnde applicatie en/of de daaraan gekoppelde applicatie.		
Control	De koppelingen tussen applicaties behoren te worden uitgevoerd met geaccordeerde **koppelingsrichtlijnen** om de juiste services te kunnen leveren en de informatiebeveiliging te kunnen waarborgen.		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

4.3.14 U.14 Logging en monitoring

Objectdefinitie

Omvat het vastleggen van informatiebeveiligingsgerelateerde gebeurtenissen en het bewaken en onderkennen van afwijkingen op beleidsregels.

Objecttoelichting

In de te ontwikkelen software moeten faciliteiten voor logging en monitoring zijn ingebouwd die ertoe bijdragen dat bewuste of onbewuste pogingen om informatie in de applicatie te verminken of onterecht te benaderen gedetecteerd en vastgelegd worden.

Doelstelling	Ongeoorloofde en/of onjuiste activiteiten van medewerkers en storingen binnen de applicatie tijdig te detecteren en vast te leggen.		
Risico	Afwijkingen van normaal gedrag binnen de applicatie zijn niet zichtbaar en niet te onderzoeken.		
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

4.3.15 U.15 Applicatie-architectuur

Objectdefinitie

Betreft een modelmatige beschrijving van de samenhang van het applicatielandschap.

Objecttoelichting

De applicatie-architectuur beschrijft de samenhang tussen functionele 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	De werking van de applicatie is onbetrouwbaar.		
Control	De functionele en beveiligingseisen behoren in een **applicatie-architectuur**, conform 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

4.3.16 U.16 Tooling ontwikkelmethode

Objectdefinitie

Betreft hulpmiddelen die bepaalde handelingen tijdens applicatieontwikkeling voor betrokkenen makkelijker maakt of helemaal overneemt.

Objecttoelichting

In de ontwikkelomgeving is sprake van continue veranderingen in de onderkende fasen. Daarom is het noodzakelijk om de omgevingen daadwerkelijk te reguleren. Zodoende 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	De ontwikkelcyclus van een applicatie met de continue veranderingen in de onderkende fasen wordt effectief uitgevoerd.		
Risico	De ontwikkelcyclus wordt minder effectief uitgevoerd.		
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 applicatieontwikkeling in het control-domein is vast te stellen of:

- de applicatie-controls afdoende zijn ingericht voor het garanderen van een beheersbare applicatie omgeving en/of;
- de applicatieve diensten functioneel en technisch op het juiste niveau worden gehouden.

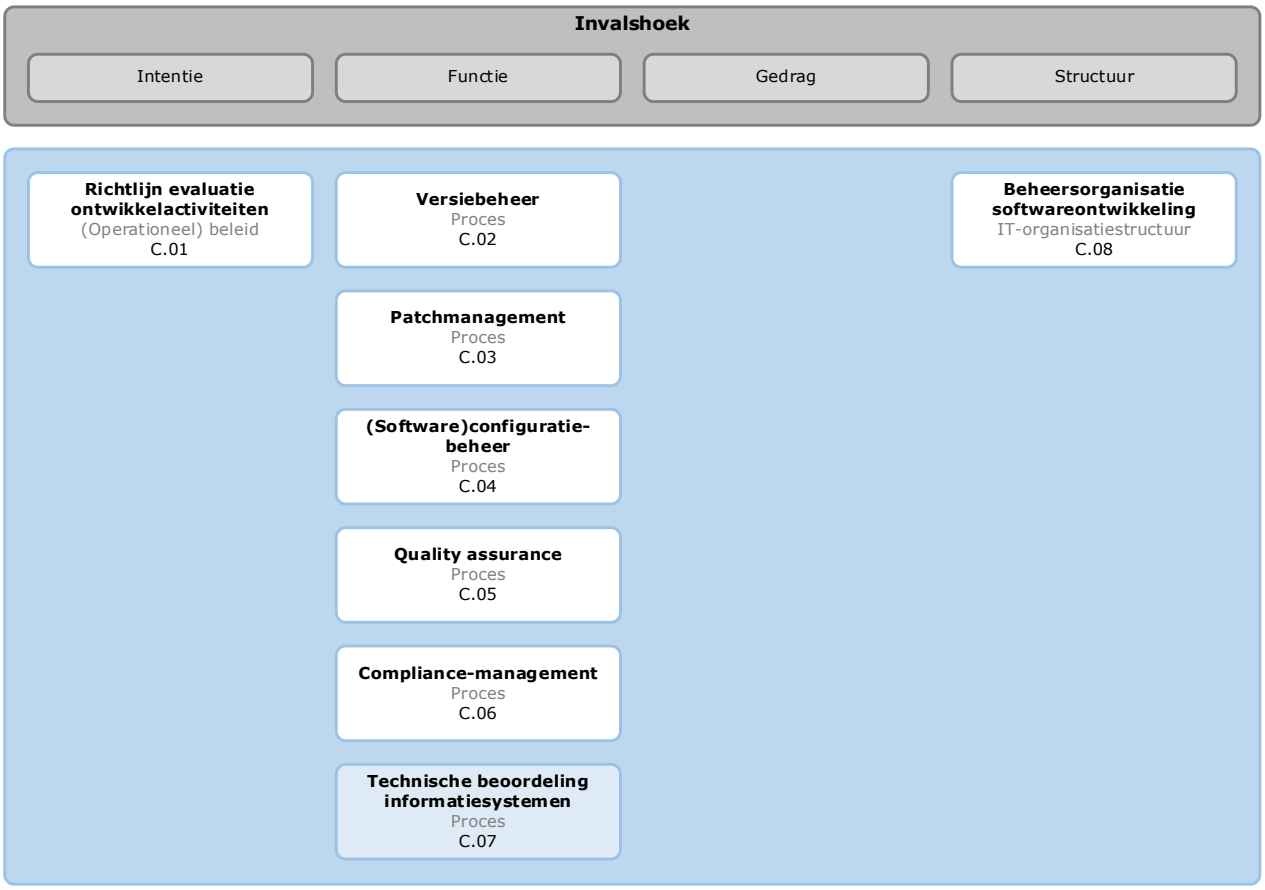
Dit houdt onder meer in dat binnen de organisatie een adequate beheerorganisatie moet zijn ingericht waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

Door het ontbreken van noodzakelijke maatregelen binnen de organisatie van de leverancier is het niet zeker of de ontwikkel- en onderhoudsadministratie aan de beoogde organisatorische en beveiligingsvoorwaarden voldoen en of de governance van deze omgeving toereikend is ingericht. Evenmin kan worden vastgesteld of de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Afbeelding 8 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 invalshoek: Intentie, Functie, Gedrag of Structuur.



Afbeelding 8: Overzicht objecten voor applicatieontwikkeling in het control-domein

5.3.1 C.01 Richtlijn evaluatie ontwikkelactiviteiten

Objectdefinitie

Betreft systematisch ontwikkelde aanbevelingen voor het achteraf beoordelen van ontwikkelactiviteiten.

Objecttoelichting

De ontwikkelorganisatie moet tijdig een softwareproduct realiseren dat aan de gestelde eisen voldoet. Hiervoor verrichten 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 daarvoor beschikken over de nodige controlerichtlijnen.

Doelstelling	Het adequaat controle-activiteiten en rapportages opstellen gericht op ontwikkelactiviteiten.	
Risico	De resultaten van de controle-activiteiten zijn niet dekkend en volledig op ontwikkelactiviteiten.	
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 conform 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 conform de opgestelde richtlijn.	CIP-netwerk

5.3.2 C.02 Versiebeheer

Objectdefinitie

Betreft een instandhoudingsproces voor de registratie van verschillende fases van een document, programma of andere informatie.

Objecttoelichting

Versiebeheer is het beheerproces dat verantwoordelijk is voor het organiseren van versies van applicatie-objecten tijdens het ontwikkel- en onderhoudstraject. Enerzijds heeft versiebeheer te maken met versies van documenten, zoals documenten die functionele eisen en functionele en technische ontwerpen bevatten. Anderzijds heeft versiebeheer te maken met versies van programmacodemanagement in de verschillende fases 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 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	Dat eenieder die in rol heeft in het systeem-ontwikkeltraject op ieder moment kan beschikken over de juiste versie van een document, programma e.d.		
Risico	Het gebruik van een niet actuele versie van een document, programma's e.d. in het systeem-ontwikkeltraject kan leiden tot een incorrecte software specificatie en ontwikkeling.		
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

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

Objecttoelichting

Binnen een projectprogramma wordt bij het ontwikkelen van informatiesystemen programmacode gecreëerd. Soms hebben ontwikkelaars de mogelijkheid om voor bepaalde functionaliteiten code uit een externe bibliotheek te gebruiken. Deze externe code kan fouten in zich dragen. 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	Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.
Risico	Technische en software kwetsbaarheden brengen de stabiliteit en betrouwbaarheid van systemen in gevaar.

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

Betreft een instandhoudingsproces voor het vastleggen en actueel houden van gegevens van configuratie-items van een computerprogramma.

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 waarborgen dat de vastgelegde gegevens van de softwareconfiguratie-items in de configuratie-administratie (CMDB) juist en volledig zijn en blijven.
Risico	De softwareconfiguratie-items zijn onbetrouwbaar (niet juist en niet volledig).

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 conform 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

Betreft het 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 deze producten worden onderworpen aan een kwaliteitscontrole (quality assurance). Quality assurance betreft ook 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	Niet helder is of het ontwikkel- en onderhoudsproces voor de applicatieontwikkeling leiden tot de applicatie zoals deze is afgesproken (voldoet aan de 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.	Conform 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

Betreft een besturingsproces voor het voldoen aan de geldende wet- en regelgeving, beleid, overeenkomsten en andere verplichtingen in de organisatie voor softwareontwikkeling.

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	Niet voldoen aan wet- en regelgeving e.d. die van invloed is op de informatiebeveiliging.		
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 Technische beoordeling informatiesystemen

Objectdefinitie

Omvat de evaluatie van de mate waarin informatiesystemen voldoen aan de vooraf gestelde technische eisen.

Objecttoelichting

Tijdens de ontwikkelfase tot kort na ingebruikname kunnen om bepaalde redenen veranderingen in het besturingssysteem plaatsvinden. In deze situaties dient de verantwoordelijke stakeholder de noodzakelijke tests uit te voeren om vast te stellen of de applicatie nog de beoogde functionaliteiten biedt en of de beveiliging van deze applicatie aan de daaraan gestelde eisen voldoet.

Doelstelling	Er ontstaat geen nadelige impact op de activiteiten of de beveiliging van de organisatie.		
Risico	Ongewenste effecten door het wijzigen van besturingsplatforms worden niet zichtbaar.		
Control	Bij **verander**ingen van **besturingsplatforms** behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact ontstaan op de activiteiten of de beveiliging van de organisatie.		BIO 2019: 14.2.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Veranderingen van besturings-platforms	1.	Bij verandering van besturingssystemen wordt onder andere het volgende getest: • de toepassingscontrole procedures; • het vaststellen of de veranderingen aan het besturingssysteem een permanente karakter hebben; • het vaststellen of de veranderingen invloed hebben op de beschikbaarheid van de functionaliteiten van de applicatie en invloed hebben op de beveiliging van de applicatie; • het vaststellen dat de juiste veranderingen plaatsvinden aan de bedrijfscontinuïteitsplannen.	ISO 27002 2017: 14.2.3a en d

5.3.8 C.08 Beheersorganisatie applicatieontwikkeling

Objectdefinitie

Betreft een doelgerichte bundeling van kennis en vaardigheden tussen personen die verantwoordelijk zijn voor de beheersing van softwareontwikkeling.

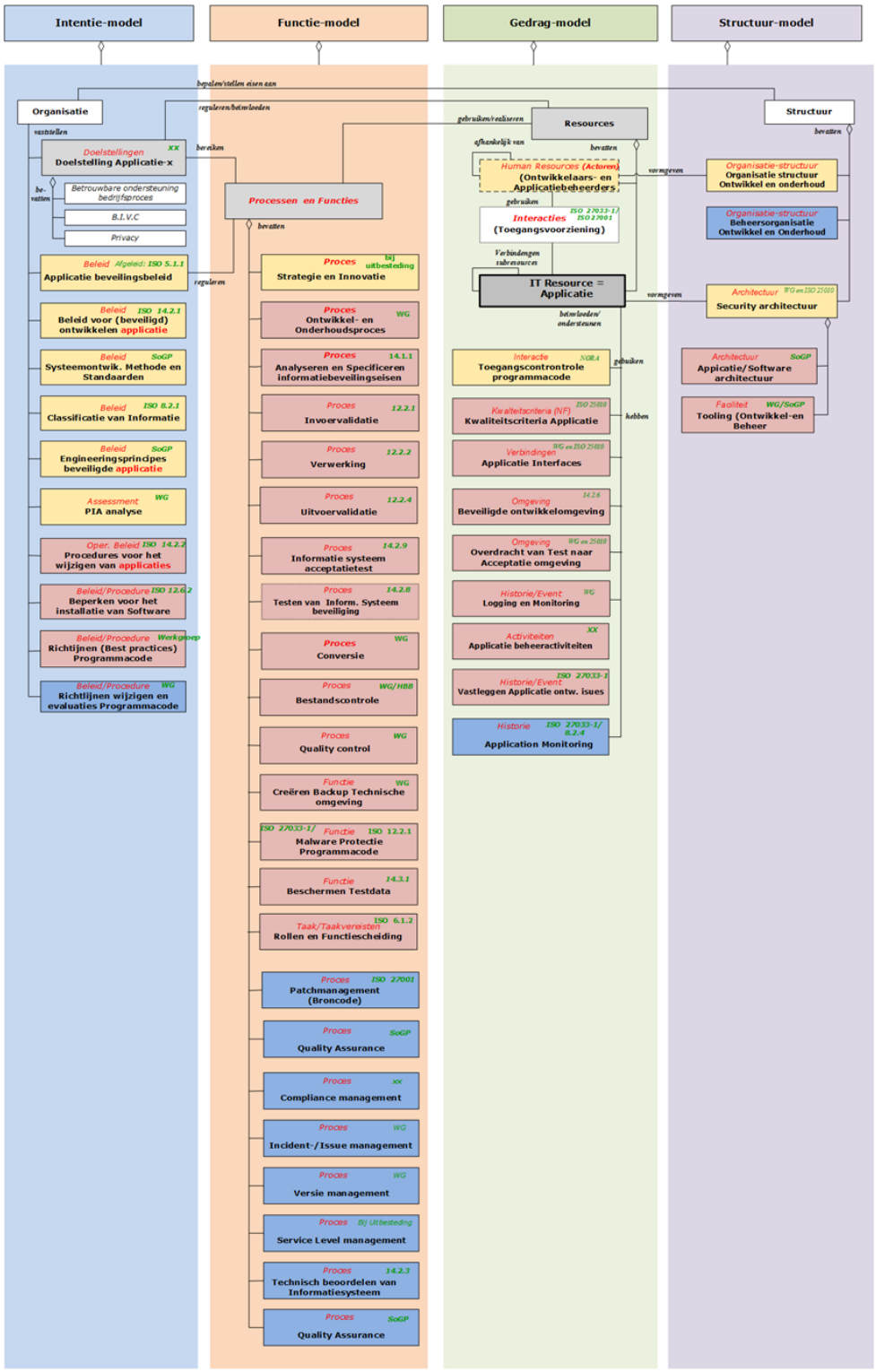
Objecttoelichting

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	De beheersorganisatie is niet effectief ingericht waardoor de softwareontwikkeling niet optimaal verloopt.		
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

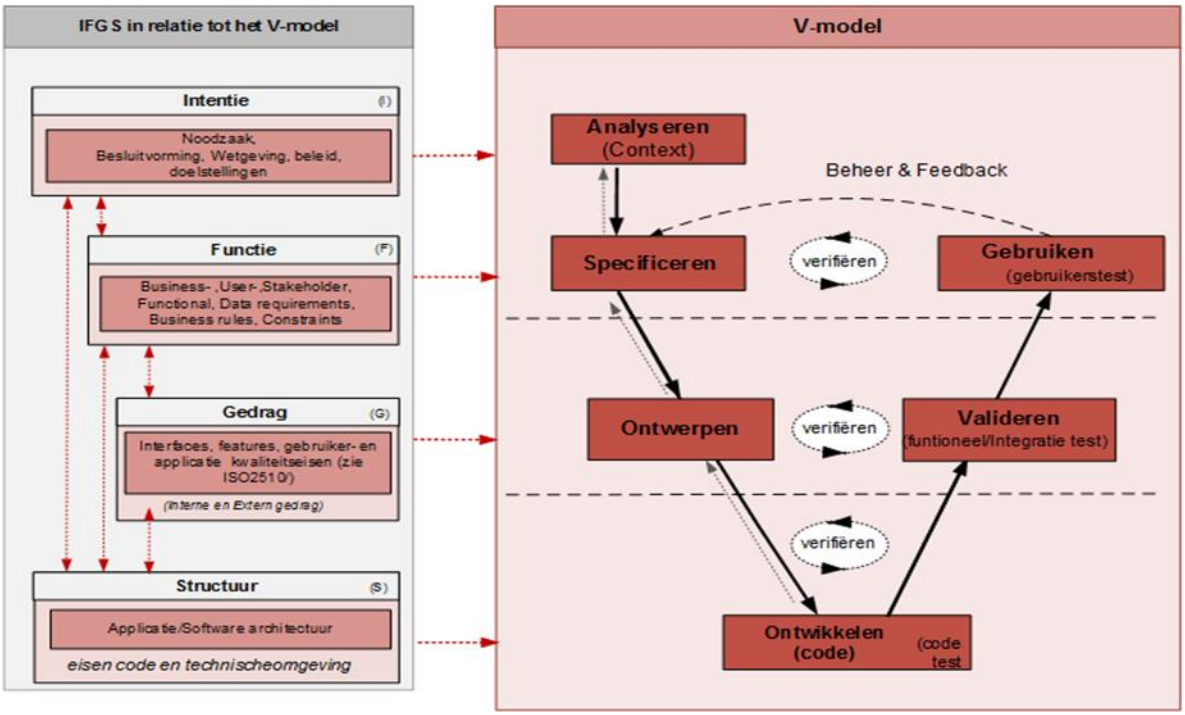
Afbeelding 9 geeft een overzicht van indegeelde objecten naar invalshoeken.



Afbeelding 9: Applicatieontwikkelingsobjecten ingedeeld naar invalshoeken

Bijlage 2: Invalshoeken gekoppeld aan het V-model

In de afbeelding 10 zijn de invalshoeken: intentie, functie, gedrag en structuur gekoppeld aan het V-model.



Afbeelding 10: Invalshoeken gekoppeld aan het V-model