Softwarepakketten

BIO Thema-uitwerking

Maart 2021 [versie 1.1 definitief]

BIO Thema-uitwerking Softwarepakketten

Titel	BIO Thema-uitwerking Softwarepakketten
Datum	Maart 2021
Versie	1.1 definitief
Opdrachtgever	Directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Wiekram Tewarie (UWV/CIP) en Jaap van der Veen (CIP)
Reviewers	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:

1. Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
2. 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.
3. 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.
4. 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

1 Voorwoord en motivatie

Deze BIO Thema-uitwerking is door CIP opgesteld om overheidsorganisaties een beeld te geven van de meest relevante onderwerpen, met name voor de verwerving van standaard software. Daarmee wordt bestaande software bedoeld, die als product op de markt is gebracht om binnen een groot aantal organisaties te kunnen worden gebruikt. Voor algemene informatie over diverse soorten softwarepakketten zie: www.sofwarepakketen.nl[1].

De belangrijkste aanleiding voor het opstellen van dit thema is dat de Baseline Informatiebeveiliging Overheid (BIO) de overheden weinig concrete handvatten biedt voor het verwerven van standaard softwarepakketten. Daarnaast is er de visie dat de complexiteit van de IT verschuift van infrastructuur naar applicaties. Daarom behandelt dit thema in samenhang de beveiligingseisen voor de verwerving van softwarepakketten.

Het kiezen van een softwarepakket blijkt in de praktijk vooral een integratievraagstuk. Hoe past de technologie en het gebruik van een softwarepakket (of dienst) veilig binnen de bestaande bedrijfsvoering? Dit is vooral een taak van de klantorganisatie. De verwervingseisen voor een softwarepakket zijn daarom geënt op zowel de noodzakelijke bedrijfs- en beveiligingsfunctionaliteiten als integratie of koppelingsmogelijkheden.

[1] De website https://www.softwarepakketten.nl biedt een schat aan informatie voor de onderwerpen uit dit thema, bijvoorbeeld Softwarepakket kopen? Dit zijn dé 5 juridische topics in ICT door Mr. Robert Grandia van Advocatenkantoor Legalz ICT en Recht.

2 Inleiding

Dit document bevat een referentiekader voor het thema Softwarepakketten. Het is geënt op controls uit de BIO die gebaseerd is op NEN-ISO/IEC 27002: 2017 (hierna genoemd ISO 27002). Er is bij de samenstelling van dit thema tevens gebruik gemaakt van andere normenkaders en internationale standaarden zoals Application Security Verification Standard (ASVS) van Open Source Foundation for Application Security (OWASP), de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC) en SIG Evaluation Criteria Security: Guidance for producers. Voor het concretiseren van de controls uit de BIO zijn deze eisen tevens gerelateerd aan normen uit de CIP-publicatie Secure Software Development (SSD). Hoewel SSD zich specifiek richt op softwareontwikkeling zijn bepaalde objecten en hieraan gerelateerde controls ook van toepassing op de aanschaf van standaard softwarepakketten.

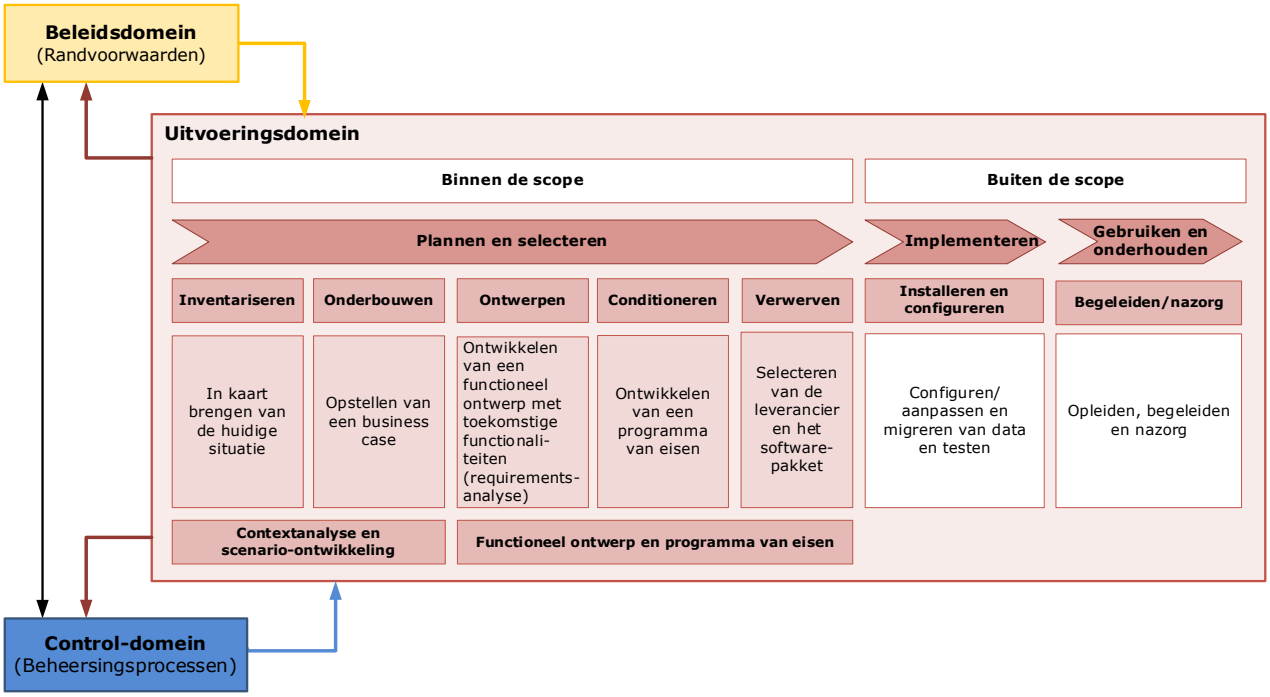
Het landschap van softwarepakketten is zeer divers qua functionaliteit en schaalgrootte. Daarom is het onmogelijk om daarvoor één dekkende lijst van beveiligingseisen op te stellen. Wel is aan te geven welke onderwerpen tijdens het verwervingsproces van belang zijn en waar beveiligingseisen uit afgeleid kunnen worden. Daarom wordt specifiek gericht op objecten die bij het verwerven van belang zijn. Om de juiste objecten te identificeren, wordt uitgegaan van de fases van het verwervingsproces. Hierbij wordt gericht op de fases plannen en selecteren waarin een business case en het stellen van Programma van Eisen (PvE) een onderdeel zijn. Binnen de business case wordt met name aandacht besteed aan objecten gerelateerd aan informatieveiligheid en privacybescherming.

In dit thema wordt een softwarepakket beschouwd als een bestaand softwarepakket dat op de markt is gebracht door een leverancier en kan in verschillende organisaties worden toegepast. Het betreft standaard softwarepakketten die gebaseerd zijn op best practices binnen een bepaalde sector en op een verzameling van op elkaar afgestemde computerprogramma's, die bepaalde bedrijfsfunctionaliteiten bieden. Voorbeelden van softwarepakketten zijn Enterprise Resource Planning (ERP)-pakket en Office-suites.

Softwarepakketten kunnen na verwerving in een eigen rekencentrum geïnstalleerd worden, maar ook afgenomen worden als een standaard clouddienst of als een hybride vorm hiervan, dat wil zeggen: in eigen rekencentrum en in de cloud. Web-gebaseerde toepassingen kunnen ook op een lokale server draaien.

2.1 Levenscyclus van een softwarepakket

De ISO 27034-5 'Protocols and application security controls data structure' uit 2017 beschrijft een referentiemodel, waarin de levenscyclus van software is gedefinieerd, vanaf de voorbereiding via de verwerving tot en met de uitfasering van het product. Onderstaande afbeelding is daarvan afgeleid en wordt gebruikt bij de uitleg van beveiligingseisen.



Afbeelding 1: Levenscyclus van een softwarepakket

2.2 Voorbereiding vanuit de klantorganisatie

Voordat de werving en selectie van een softwarepakket start, worden de onderstaande stappen doorlopen, waarmee belangrijke vraagstukken worden ingevuld. De output van deze stappen maakt onderbouwing van keuzes mogelijk en maakt deze transparant en traceerbaar voor bestuurders en de inhoudelijke functies in zowel de business- als de informatievoorzieningsketen.

2.2.1 Stap 1. Inventariseren

De uitgangssituatie wordt in kaart gebracht, zowel van de organisatie als de techniek. Onderzocht wordt welke functionele behoeften er precies bestaan binnen de klantorganisatie (hierna genoemd klant) en welke afhankelijkheden verwacht worden tussen de al beschikbare bedrijfsfuncties en de beoogde nieuwe functionaliteit.

2.2.2 Stap 2. Onderbouwen

Een business case omschrijft de noodzaak voor een nieuw softwarepakket en de verwachte resultaten en voordelen daarvan. Binnen een business case worden ook de nieuwe IT-functionaliteiten vastgesteld waarin de kosten-baten worden geanalyseerd.

2.2.3 Stap 2a. en 2b. Contextanalyse en scenario-ontwikkeling

Na of tijdens de uitwerking van de business case wordt met een risicoanalyse (zie ISO 27005 'Information security risk management' uit 2018) de in- en externe context vastgesteld. Dus in welke omgeving moet het pakket kunnen functioneren? Vanuit de business case en contextanalyse worden doelscenario's ter besluitvorming uitgewerkt. Enkele vraagstukken daarbij zijn hieronder belicht.

Cloud of on-premise Voor standaard softwarepakketten wordt door leveranciers steeds meer overgegaan naar clouddiensten. Sommige software is zelfs alleen nog als clouddienst af te nemen. Business drivers als kosten/baten, 'time-to-market' en 'wendbaarheid' kunnen functionaliteit, geleverd als clouddienst heel aantrekkelijk maken. Organisaties die zijn overgestapt naar clouddiensten hebben ervaren dat die keuze een grote impact heeft op de bedrijfsvoering zoals men die gewend was met een eigen rekencentrum. Die impact geldt zowel voor de afnemende gebruikersorganisatie als voor de vorm van IT-dienstverlening.

Inpasbaarheid Er bestaat vrijwel altijd een bestaande IT-omgeving waarin het softwarepakket moet passen. Dat geldt tot op zekere hoogte ook voor clouddiensten. Dit zijn technische integratievraagstukken. Daarom is het van belang om voldoende IT-deskundigheid in te zetten bij een context- en risicoanalyse en bij het opstellen van een globaal ontwerp, Programma van Eisen (PvE) en de vaststelling van de technische randvoorwaarden. Raadpleeg daarbij de actuele vakliteratuur voor de te nemen technische maatregelen.

Risico's De uit te voeren risicoanalyses zijn onder andere gericht op de vereiste bedrijfscontinuïteit, informatieveiligheid en privacyaspecten van de voorgenomen nieuwe bedrijfsfunctionaliteit. Daarvoor wordt onder andere een Business Impact Assessment (BIA), een risicoanalyse en indien nodig een Data Protection Impact Assessment (DPIA) uitgevoerd. Mede met de uitkomsten van deze analyses kan het meest geschikte implementatiescenario worden gekozen.

Continuïteit Continuïteitsvraagstukken zijn: wat is de maximaal toelaatbare uitvalduur van het softwarepakket en wat is het maximaal toelaatbare dataverlies? Beide factoren kunnen cruciaal zijn voor het voortbestaan van een bedrijf en maken onderdeel uit van Bedrijfscontinuïteitsmanagement (BCM).

Classificatie De classificatie van de data die door het pakket verwerkt zal worden, vormt eveneens een belangrijke input, zowel voor de BIA als voor de DPIA, maar ook voor beveiligingseisen gericht op de transport en opslag van gegevens.

2.2.4 Stap 3. en 4. Ontwerpen en conditioneren

Als de scenariokeuze is gemaakt, wordt een functioneel ontwerp opgesteld. Hierin worden de bedrijfsfuncties uitgewerkt tot een PvE. Dit PvE dient als basis voor de selectie van IT-diensten zoals een softwarepakket.

Bij het vaststellen van een PvE wordt aandacht besteed aan zowel bedrijfsfuncties als aan informatieveiligheid en privacybescherming, waarvoor een set van functionele en non-functionele eisen wordt opgesteld.

In deze BIO Thema-uitwerking zijn de objecten geïdentificeerd en de hieraan gerelateerde BIO-controls gedefinieerd die voor het ontwerp van bedrijfsfuncties en vanuit de verwervingsoptiek noodzakelijk kunnen zijn. Het gaat hier zowel om de organisatie als de techniek.

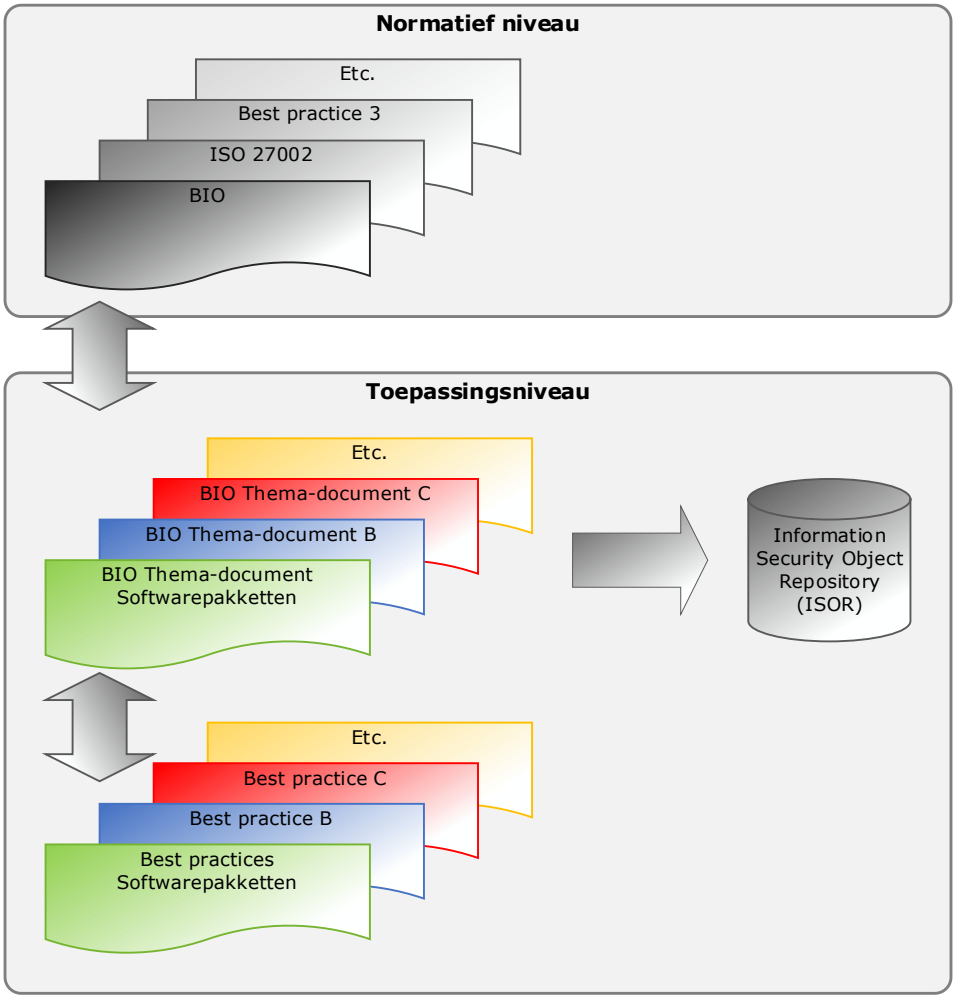
De objecten zijn conform de standaard opzet van BIO Thema-uitwerkingen uitgewerkt in twee onderdelen: structuur en objecten. De structuur van elk thema is een indeling van objecten op basis van het beleids-, uitvoerings- en control-domein. De objecten representeren de inhoudelijke informatiebeveiligingsonderwerpen, die bij voorkeur uit de BIO-/ISO 27002-controls en -maatregelen zijn geadopteerd. Zoals in hoofdstuk 2 Inleiding is aangegeven, zijn sommige controls voor concretisering gerelateerd aan andere baselines zoals SSD-controls en -maatregelen.

2.3 Scope en begrenzing

Dit thema is voornamelijk gericht op conditionele, beveiligings- en beheersingsaspecten en generieke beveiligingseisen die gerelateerd zijn aan de verwerving van softwarepakketten. Buiten scope van dit thema vallen:

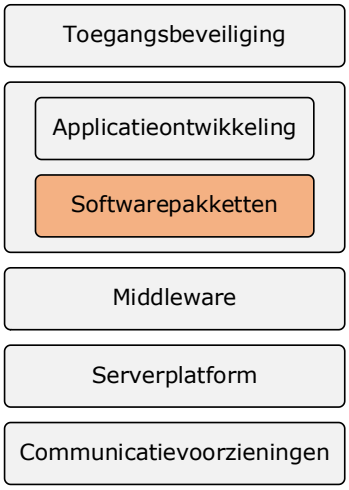
1. operationele implementatie en configuratie van het verworven softwarepakket;
2. activiteiten die specifiek gaan over de infrastructuur van externe hosting en generieke clouddiensten; zie daarvoor de BIO Thema-uitwerkingen Clouddiensten, Serverplatform en Communicatievoorzieningen.
3. specifieke gebruikers- en businesseisen omdat deze eisen organisatieafhankelijk zijn.
4. applicatieontwikkelingseisen, zie daarvoor de BIO Thema-uitwerking Applicatieontwikkeling.

De begrenzing van dit document is in onderstaande afbeelding weergegeven.



Afbeelding 2: Relatie BIO Thema-uitwerking met aanpalende documenten

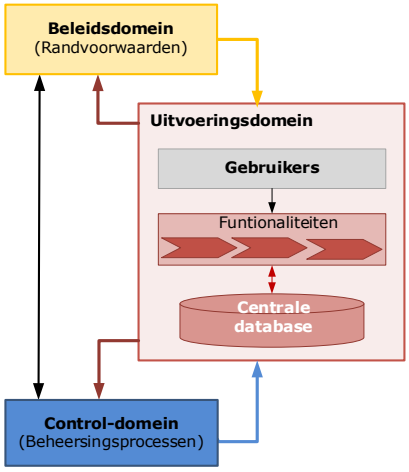
De relatie tussen de verschillende BIO Thema-uitwerkingen is in afbeelding 3 weergegeven.



Afbeelding 3: Positionering thema Softwarepakketten in relatie tot andere thema's

2.4 Relaties tussen beveiligingsobjecten

Het thema Softwarepakketten omvat het geheel van beleid, richtlijnen, procedures, processen, mensen (actoren), middelen en registraties voor het betrouwbaar functioneren van softwarepakketten. De essentiële objecten voor softwarepakketten worden ingedeeld in het beleids-, uitvoerings- en control-domein. Deze objecten worden in de volgende drie hoofdstukken uitgewerkt.



Afbeelding 4: Softwarepakketten in het beleids-, uitvoerings- en control-domein

2.4.1 Beleidsdomein

Dit zijn de randvoorwaarden, conditionele aspecten en contraints die bij de verwerving van softwarepakketten in acht moeten worden genomen.

2.4.2 Uitvoeringsdomein

De control-keuze uit de BIO voor dit thema vloeit voort uit enkele uitgangspunten die gerelateerd zijn aan software:

- Beveiligings- en beheerfuncties
  Het softwarepakket beschikt over beveiligingsfuncties en beschermingsmechanismen die de beveiliging van softwarepakketten moeten bevorderen, zoals virusprotectie en mogelijkheden om tekortkomingen in de beveiliging achteraf te kunnen corrigeren, zoals patchmanagement.
- Configuratie van features
  Het softwarepakket beschikt over features om een adequaat niveau van beveiliging te kunnen bereiken.
- Structuur en ontwerp
  De samenhang tussen de modules binnen het softwarepakket, de geboden koppelingsmogelijkheden met een externe applicatie en de faciliteiten voor import en export zijn inzichtelijk gemaakt met een softwarearchitectuur.

2.4.3 Control-domein

Voor het evalueren van de effectiviteit van de genomen controls en maatregelen uit het beleids- en uitvoeringsdomein zijn in dit domein de daarvoor benodigde objecten, controls en maatregelen bepaald.

3 Beleidsdomein

3.1 Doelstelling

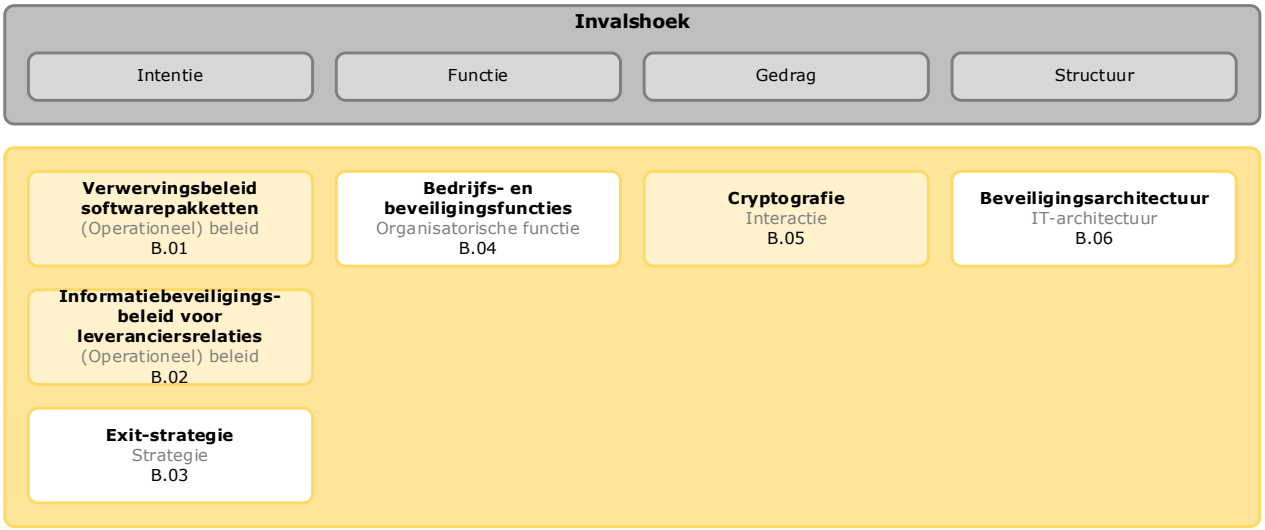
Het doel van het beleidsdomein is om de conditionele- of beleidselementen die van belang zijn bij het selecteren en verwerven van softwarepakketten te identificeren. Het zijn elementen die vooraf bekend moeten zijn en die uitgevaardigd en gecommuniceerd worden door het hogere management.

3.2 Risico's

Als toereikend beleid ontbreekt, dan bestaat het risico dat er geen systematische analyse van de noodzakelijke requirements plaatsvindt waardoor het verworven softwarepakket niet voorziet in de gewenste (non)functionaliteiten.

3.3 Objecten, controls en maatregelen

Afbeelding 5 geeft de ordening van objecten in het beleidsdomein weer met invalshoeken voor dit thema. Elk objectblok bevat de objectnaam, het basiselement en het objectnummer. Geelgekleurde objecten zijn afgeleid van de BIO. De witte objecten zijn afgeleid van overige best practices.



Afbeelding 5: Overzicht softwarepakkettenobjecten in het beleidsdomein

De objecten zijn in de volgende paragrafen uitgewerkt. Echter niet elk object is van toepassing voor elke softwarepakketselectie. Dit hangt af van verschillende factoren zoals: schaalgrootte, hostingslocatie, soort en integreerbaarheid met de bestaande IT. In tegenstelling tot andere thema's zijn aan de uitwerking toegevoegd:

1. Schaalgrootte
   De schaalgrootte geeft een globale indicatie (klein, middel of groot) in hoeverre de schaalgrootte van softwarepakketten van invloed kan zijn op de relevantie van een object. Met klein wordt bedoeld getalsmatig en/of bedrijfsmatige impactbeperkte toepassing. Middel is voor middelgrote bedrijfstoepassingen, zoals boekhouding- en officetoepassingen. De waarde groot is

voor grootschalig gebruik, enerzijds in aantallen, anderzijds in omvang van het softwarepakket zoals ERP en Enterprise Data Warehouses (EDW).

2. Voor wie de control van toepassing is
   Het gaat om de klant en/of de leverancier. In veel gevallen is samenwerking tussen de klant en leverancier nodig om risico's tijdens het gebruik van de softwarepakketten afdoende te beperken.

3.3.1 B.01 Verwervingsbeleid softwarepakketten

Toelichting

Een randvoorwaarde voor een succesvolle implementatie van informatievoorzieningen is inzicht hebben in de businessrisico's en het regelmatig beoordelen van businessrisico's gerelateerd aan applicatiesoftware zoals een softwarepakket. De business case onderzoekt de kosten en de baten.

De context- en risicoanalyse[2] onderzoekt informatieveiligheid, bedrijfscontinuïteit en privacybescherming. Beveiligingsrisico's hebben zowel betrekking op de kennis van medewerkers als op de match van de software of IT-diensten met de bestaande bedrijfsprocessen en voldoende kennis van de techniek. Beleid is nodig om deze risico's in kaart te brengen en mee te nemen in de besluitvorming voor de wijze van uitvoering.

Doelstelling	Het beheersen van het verwerven van softwarepakketten.		
Risico	Onvoldoende mogelijkheid om sturing te geven aan het verwerven van softwarepakketten.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Klant.		
Control	Voor het verwerven van software behoren **regels** te worden vastgesteld en op verwervingsactiviteiten binnen de organisatie te worden toegepast.		BIO 2019: 14.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	In het verwervingsbeleid voor softwarepakketten zijn regels vastgesteld die bij de verwerving van softwarepakketten in acht dienen te worden genomen. De regels kunnen onder andere betrekking hebben op: • analyse van de context waarin het softwarepakket moet functioneren; • mobiliseren van kennis die bij het verwerven van belang is; • vaststelling van de eigenaarschap van data; • tijdige scholing van de betrokken medewerkers; • naleven van contractuele verplichtingen.	CIP

[2] Onderzoek Beoordelen veiligheid (web)applicaties (en IT-organisaties) door Gerard Bottemanne van Onderzoeksbureau GBNED, versie 2020, onder andere te vinden op: https://www.softwarepakketten.nl.

	2.	De verwerving van een softwarepakket vindt plaats met een business case, waarbij verschillende toepassingsscenario's worden overwogen: • bedrijfsfuncties vanuit een softwarepakket in een eigen rekencentrum; • bedrijfsfuncties als Software as a Service (SaaS) aangeboden; • hybridevorm van IT-dienstverlening, waarbij SaaS-dienstverlening wordt aangevuld door diensten vanuit het eigen rekencentrum.	CIP
	3.	Verwerving van een softwarepakket vindt plaats met een functioneel ontwerp, waarin de beoogde functionele en niet-functionele requirements zijn uitgewerkt in een op te stellen softwarepakket van eisen en wensen.	CIP
	4.	Leveranciers zijn ISO 27001-gecertificeerd.	CIP

3.3.2 B.02 Informatiebeveiligingsbeleid voor leveranciersrelaties

Toelichting

De kwaliteit die een klant als geheel ervaart van een softwarepakket wordt in belangrijke mate bepaald door de ondersteuning die de leverancier biedt gedurende de levenscyclus van een product in zowel goede als slechte tijden. Hiervoor is het nodig dat een passende leverancier wordt gekozen. Dit maakt onderdeel uit van het selectieproces. Randvoorwaardelijk is het maken van goede contractuele afspraken.

Doelstelling	Het beheersen van de leveranciersrelatie specifiek gericht op informatiebeveiliging.	
Risico	Onvoldoende mogelijkheid om sturing te geven aan leveranciersrelaties specifiek voor informatiebeveiliging.	
Schaalgrootte	Elke schaalgrootte.	
Voor wie	Klant.	
Control	Met de leverancier behoren de **informatiebeveiligingseisen** en een periodieke actualisering daarvan te worden overeengekomen.	BIO 2019: 15.1.1
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Informatiebe-veiligingseisen	1.	De overeenkomsten en documentatie omvatten afspraken over: • procedures voor levenscyclusmanagement, actualisaties en patches; • beveiligingseisen voor fysieke toegang, monitoring en beheer op afstand; • verplichtingen voor leveranciers om vertrouwelijke informatie van de klant te beschermen; • het bepalen van aanvullende beveiligingseisen zoals het recht op een audit; • de bewaking van informatiebeveiligingsprestaties met overeengekomen beveiligingsafspraken voor externe leveranciers; • het vaststellen van een methode voor het afsluiten, beëindigen, verlengen en heronderhandelen van contracten met externe leveranciers (exit-strategie); • de wijze van rapportage over de dienstverlening.	SoGP 2018: SC1.1.1b, j en k

3.3.3 B.03 Exit-strategie

Toelichting

Aan het einde van de levenscyclus van een softwarepakket (met name software in de cloud) moeten er mogelijkheden bestaan om bestaande contracten te ontbinden en een nieuwe leverancier te kiezen. Vendor lock-in moet worden voorkomen. Voor de transitiefase en een probleemloze overdracht van bedrijfsgegevens moeten vooraf bindende afspraken worden gemaakt tussen de klant en de leverancier.

Doelstelling	Het voorkomen van discontinuïteit en het kunnen overgaan tot exit bij vooraf bepaalde condities.	
Risico	Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.	
Schaalgrootte	Middel of groot.	
Voor wie	Klant.	
Control	In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal **bepalingen** over exit zijn opgenomen, als een aantal **condities** die aanleiding kunnen geven tot een exit.	CIP
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Bepalingen	1.	De klant legt in de overeenkomst bepalingen over exit vast dat: • De exit-bepaling geldt zowel bij het einde van de overeenkomst als om valide redenen aangedragen door de klant (zie condities). • De overeenkomst (en eventuele verwerkersovereenkomst) duurt voort totdat de exit-regeling helemaal is uitgevoerd. • De opzegtermijn voldoende tijd geeft om te kunnen migreren. • Data en configuratiegegevens (indien relevant) pas na succesvolle migratie verwijderd mogen worden. • Door een onafhankelijke partij wordt gecontroleerd en vastgesteld dat alle data is gemigreerd. • De exit-regeling wordt aangepast/anders ingevuld als de software die gebruikt wordt voor de clouddienst is gewijzigd.	BSI C5 2020: PI-02

Condities	2.	De klant kan, buiten het verstrijken van de contractperiode, besluiten over te gaan tot exit wanneer sprake is van aspecten die gerelateerd zijn aan:
		• Contracten:
		  • niet beschikbaar zijn van de afgesproken prestatie;
		  • eenzijdige wijziging door de leverancier van het SLA;
		  • prijsverhoging.
		• Geleverde prestatie/ondersteuning:
		  • onvoldoende compensatie voor storingen;
		  • niet leveren van de afgesproken beschikbaarheid of prestatie;
		  • gebrekkige ondersteuning.
		• Clouddienst(en):
		  • nieuwe eigenaar of nieuwe strategie;
		  • einde van de levensduur van clouddiensten als softwarepakket;
		  • achterwege blijvende features.
			CIP

3.3.4 B.04 Bedrijfs- en beveiligingsfuncties

Toelichting

De eigenschappen van het softwarepakket voldoen aan de businessbehoefte van de klant en ondersteunt daarmee op een veilige manier het bedrijfsproces. Het softwarepakket bevat goed-gedefinieerde mogelijkheden en interfaces.

Integratie en mogelijke koppelingen spelen daarbij een belangrijke rol. Het is zinvol na te gaan welke (open) standaarden een softwarepakket ondersteunt en in hoeverre deze in de toekomst actueel gehouden worden. Denk daarbij aan een standaard als Pan-European Public Procurement OnLine (PEPPOL) voor E-factureren.

Het softwarepakket dient de klant naast businessfuncties ook voldoende ‘digitale behendigheid’ te leveren, waardoor de organisatie componenten kan veranderen, naar behoefte kan uitbreiden en het softwarepakket aan het einde van de levenscyclus kan vervangen onafhankelijk van de belendende systemen.

Doelstelling	Het voldoen aan de businesseisen van de organisatie en de beoogde, veilige ondersteuning van het bedrijfsproces.		
Risico	Datalekken en de continuïteit niet kunnen waarborgen.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Klant.		
Control	De noodzakelijke **bedrijfs- en beveiligingsfuncties** binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.		CIP
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Bedrijfs- en beveiligings-functies	1.	Bij de afleiding van de bedrijfsfuncties worden stakeholders uit het veranderingsgebied betrokken.	CIP
	2.	Voor het afleiden van bedrijfs- en beveiligingsfuncties worden formele methoden voor een gegevensimpactanalyse toegepast, zoals een BIA en DPIA en wordt rekening gehouden met het informatieclassificatie-beleid.	CIP
	3.	Het softwarepakket dekt de eisen van de organisatie zodanig dat geen maatwerk noodzakelijk is. Wanneer de functionaliteit door een SaaS-leverancier wordt aangeboden via een app-centre, dan wordt het volgende onderzocht en overeengekomen: • Wie zijn de leveranciers of contractpartners van apps? • Wie is verantwoordelijk voor het goed functioneren van de app en de continuïteit?	CIP
	4.	Het softwarepakket biedt de noodzakelijke veilige interne en externe communicatie-, koppelings- (interfaces) en protectiefuncties, bij voorkeur gerelateerd aan open standaarden.	CIP
	5.	De documentatie van het softwarepakket beschrijft alle componenten voor de beveiligingsfuncties die ze bevatten.	CIP

3.3.5 B.05 Cryptografie

Toelichting

Cryptografie is een techniek om informatie te beschermen vanuit het oogpunt van vertrouwelijkheid, authenticiteit, onweerlegbaarheid en authenticatie. Een solide cryptografiebeleid is daarbij een randvoorwaarde om de vertrouwelijkheid van informatie te kunnen garanderen. Met dit beleid geeft de organisatie aan op welke wijze het omgaat met voorzieningen, procedures en certificaten voor versleuteling van gegevens.

Doelstelling	Het beheersen van cryptografie binnen softwarepakketten om de vertrouwelijkheid van informatie te kunnen garanderen.

Risico	Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen softwarepakketten.		
Schaalgrootte	Groot.		
Voor wie	Klant.		
Control	Ter bescherming van de **communicatie en opslag** van informatie behoort een beleid voor het gebruik van **cryptografische beheersmaatregelen** te worden ontwikkeld en geïmplementeerd.		BIO 2019: 10.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Communicatie en opslag	1.	Communicatie en opslag van informatie door softwarepakketten is passend bij de classificatie van de gegevens, al dan niet beschermd door versleuteling.	CIP
Cryptografische beheersmaatregelen	2.	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: • Wie verantwoordelijkheid is voor de implementatie en het sleutelbeheer. • Het bewaren van geheime authenticatie-informatie tijdens verwerking, transport en opslag. • De wijze waarop de normen van het Forum Standaardisatie worden toegepast.	BIO 2019: 10.1.1.1

3.3.6 B.06 Beveiligingsarchitectuur

Toelichting

Op het hoogste niveau beschrijft een zogenaamde enterprise-architectuur de context van de organisatie en op hoofdlijnen het geheel aan organisatorische en functionele activiteiten en tot welke bedrijfsoutput dit resulteert.

De beveiligingsarchitectuur beschrijft met het beveiligingsbeleid in samenhang welke organisatorische en technische beveiligingsmaatregelen de beoogde bedrijfsfunctionaliteit en dienstverlening ondersteunen voor eindgebruikers en klanten.

Doelstelling	Het effectief sturen en beheersen van veranderingen in het applicatielandschap.	
Risico	Onvoldoende mogelijkheid om sturing te geven op de beveiligingsmaatregelen van softwarepakketten die in de architectuur zijn opgenomen.	
Schaalgrootte	Middel en groot.	
Voor wie	Klant.	
Control	De klant behoort het **architectuurlandschap** in kaart te hebben gebracht waarin het softwarepakket geïntegreerd moet worden en **beveiligingsprincipes** te hebben ontwikkeld.	CIP

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Architectuur-landschap	1.	De beveiligingsarchitectuur ondersteunt een bedrijfsbreed proces voor het implementeren van samenhangende beveiligingsmechanismen en tot stand brengen van gemeenschappelijke gebruikersinterfaces en Application Programming Interfaces (API's), als onderdeel van softwarepakketten.	SoGP 2018: TS1.1.7
Beveiligings-principes	2.	Er zijn beveiligingsprincipes voorgeschreven waaraan een te verwerven softwarepakket getoetst moet worden, zoals: • Security by default Standaard instellingen van beveiligingsparameters. • Fail secure In geval van systeemstoringen in het softwarepakket is informatie daarover niet toegankelijk voor onbevoegde personen. • Defence in depth Gelaagde, diepgaande bescherming, die niet afhankelijk is van één beveiligingsmethode). • Default deny Het voorkomen van ongeautoriseerde toegang.	SoGP 2018: TS1.1.6

4 Uitvoeringsdomein

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein is te waarborgen dat de operationele functionele en non-functionele eisen die deel uitmaken van het PvE voor het verwerven van softwarepakketten gebaseerd zijn op organisatorische- en technische uitgangspunten van de organisaties.

4.2 Risico's

Als adequate normen en maatregelen voor de inzet en veilig gebruik van softwarepakketten ontbreken, dan ontstaan enerzijds risico's voor het verkrijgen van onjuiste functionaliteiten en anderzijds risico's voor het verkrijgen van een softwarepakket met onvoldoende beschermende eigenschappen binnen het softwarepakket.

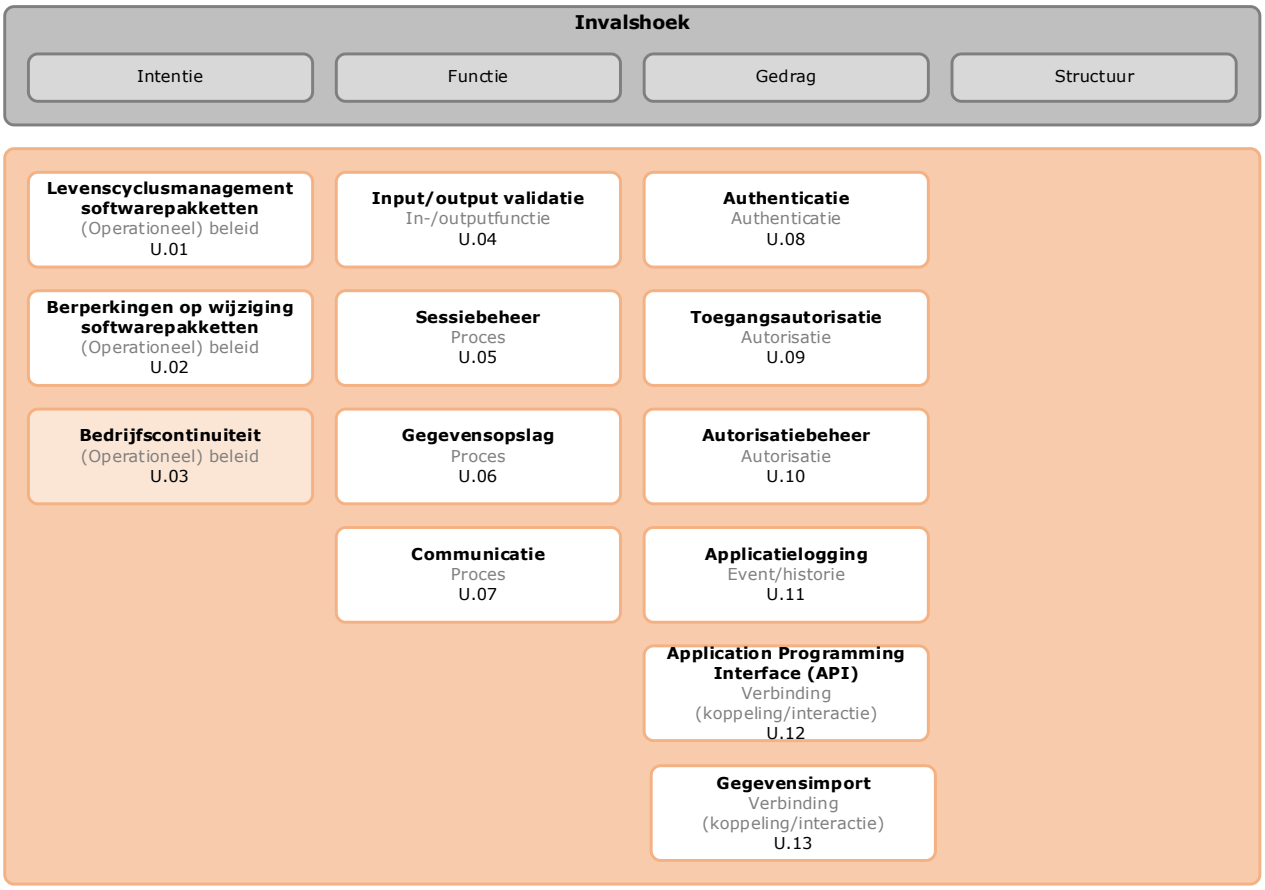
Cyberaanvallen maken meestal misbruik van kwetsbaarheden in standaard software, zoals softwarepakketten. Kwetsbaarheden kunnen om vele redenen aanwezig zijn, zoals codeerfouten, logische fouten, door onvolledige vereisten vanuit opdrachtgevers en het niet testen op ongebruikelijke of onverwachte omstandigheden. Veel voorkomende specifieke fouten (en daarmee kwetsbaarheden) in software zijn:

- Het niet controleren van de omvang van gebruikersinvoer (Structured Query Language (SQL)-injection).
- Het niet filteren op potentieel kwaadaardige tekenreeksen van invoerstromen.
- Het niet initialiseren en wissen van variabelen.
- Slecht geheugenbeheer waardoor overflows optreden en softwarefouten kunnen worden beïnvloed.

Per object is aangegeven welke risico's de bedrijfsvoering van organisaties lopen, wanneer beveiligingsmaatregelen niet of in onvoldoende mate worden geïmplementeerd.

4.3 Objecten, controls en maatregelen

Afbeelding 6 geeft de ordening van objecten in het uitvoeringsdomein weer met invalshoeken voor dit thema. Elk objectblok bevat de objectnaam, het basiselement en het objectnummer. Oranjegekleurde objecten zijn afgeleid van de BIO. De witte objecten zijn afgeleid van overige best practices.



Afbeelding 6: Overzicht softwarepakkettenobjecten in het uitvoeringsdomein

De objecten zijn in de volgende paragrafen uitgewerkt. Echter niet elk object is van toepassing voor elke softwarepakketselectie. Dit hangt af van verschillende factoren zoals: schaalgrootte, hostingslocatie, soort en integreerbaarheid met de bestaande IT. In tegenstelling tot andere thema's zijn aan de uitwerking toegevoegd:

- Schaalgrootte
  De schaalgrootte geeft een globale indicatie (klein, middel of groot) in hoeverre de schaalgrootte van softwarepakketten van invloed kan zijn op de relevantie van een object. Met klein wordt bedoeld getalsmatig en/of bedrijfsmatige impactbeperkte toepassing. Middel is voor middelgrote bedrijfstoepassingen, zoals boekhouding- en officetoepassingen. De waarde groot is voor grootschalig gebruik, enerzijds in aantallen, anderzijds in omvang van het softwarepakket zoals ERP en EDW.

- Voor wie de control van toepassing is
  Het gaat om de klant (de eisensteller) en/of de leverancier (levert het softwarepakket of diensten). In veel gevallen is samenwerking tussen de klant en leverancier nodig om risico's tijdens het gebruik van de softwarepakketten afdoende te beperken.

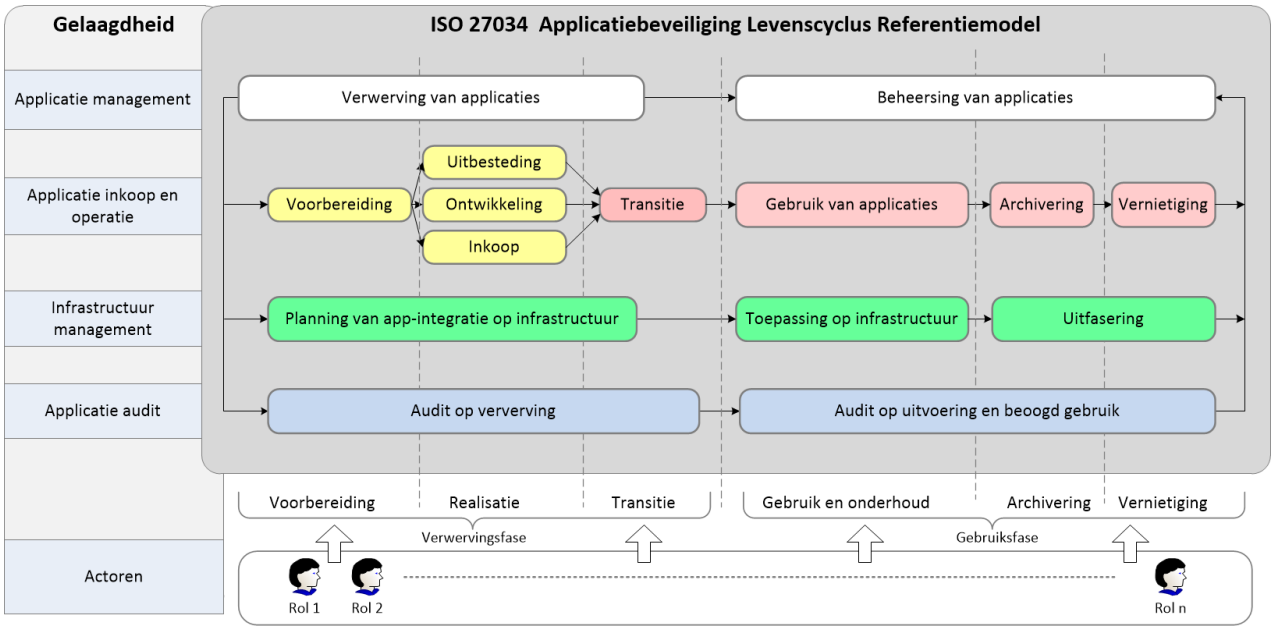
4.3.1 U.01 Levenscyclusmanagement softwarepakketten

Toelichting

Verwerving van software is geen enkelvoudige gebeurtenis. Na het verwerven van een softwarepakket blijft de klant tijdens de levenscyclus afhankelijk van de leverancier en heeft verschillende contactmomenten. Interactie met de leverancier blijft nodig tijdens de levensduur van het product, voor ingebruikname, actualisaties, innovaties en het uitfaseren.

De klant dient inzicht en overzicht te verschaffen aan de leverancier over de technische omgeving, de technische stack en de gewenste interoperabiliteit tussen de diverse softwarecomponenten behorende tot het softwarepakket. Het doel daarvan is de continuïteit van de beschikbaarheid van de bedrijfsfuncties zeker te stellen. Cruciaal daarbij is het tijdig upgraden van de software tijdens de levensduur van het product. Wanneer het softwarepakket niet langer door de leverancier wordt ondersteund, kan dit beveiligingsrisico's voor de klant opleveren.

De ISO 27034-5 'Protocols and application security controls data structure' uit 2017 beschrijft onderstaand referentiemodel, waarin de levenscyclus van software is gedefinieerd, vanaf de voorbereiding van de verwerving tot en met de uitfasering van het product. Het is een model dat verschillende aspecten in beeld brengt. In dit thema ligt de focus op het verwervingsproces en de fase van een software die equivalent is aan het verwerven van een softwarepakket.



Afbeelding 7: Referentiemodel levenscyclus softwarebeveiliging

Doelstelling	Het zorgen dat informatiebeveiliging deel uitmaakt van de levenscyclus van software.
Risico	De continuïteit van de bedrijfsprocessen kan niet gewaarborgd worden.
Schaalgrootte	Middel en groot.

Voor wie	Klant en leverancier.		
Control	De leverancier behoort de klant te **adviseren** met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over **strategische ontwikkeling** en **innovatieve** keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.		CIP
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Adviseren	1.	Tussen de leverancier en klant is een procedure afgesproken voor het tijdig actualiseren/opwaarderen van verouderde softwarepakketten uit de technische stack.	CIP
Strategische ontwikkeling	2.	De leverancier onderhoudt een registratie van de gebruikte softwarestack. Hierin is de vermelding van de uiterste datum dat ondersteuning plaatsvindt opgenomen, waardoor inzicht bestaat in de door de leverancier ondersteunde versies van de software.	CIP
Innovatieve	3.	Technologische innovaties van softwarepakketten worden aan de klant gecommuniceerd en de toepassing daarvan wordt afgestemd met de klant voor implementatie.	CIP

4.3.2 U.02 Beperkingen op wijziging softwarepakketten

Toelichting

Bij voorkeur dienen geleverde softwarepakketten ongewijzigd te worden toegepast. Wijzigingen van applicatiecode die niet door de leverancier zijn aangebracht, leveren bij actualisaties van het onderliggende serverplatform en interactie met andere platformen vaak technische problemen op. Ze veroorzaken daarbij mogelijk beveiligingsrisico's. Eventuele wijzigingen dienen onder strikte voorwaarden, met goedkeuring van de leverancier plaats te vinden. Anderzijds worden organisaties die clouddiensten gebruiken soms geconfronteerd met nieuwe versies, die ze nog niet hebben kunnen testen voordat ze in de organisatie worden toegepast.

Doelstelling	Wijzigingen aan softwarepakketten gecontroleerd laten verlopen.		
Risico	Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van de data.		
Schaalgrootte	Middel en groot.		
Voor wie	Klant en leverancier.		
Control	**Wijzigingen** aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden **gecontroleerd**.		ISO 27002 2017: 14.2.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Wijzigingen	1.	Bij nieuwe softwarepakketten en bij wijzigingen op bestaande softwarepakketten 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.	Wijzigingen in, door leveranciers geleverde, softwarepakketten worden, voor zover mogelijk en haalbaar, ongewijzigd gebruikt.	ISO 27007 2017: 14.2.4
Gecontroleerd	3.	Indien vereist worden de wijzigingen door een onafhankelijke beoordelingsinstantie getest en gevalideerd (dit geldt waarvoor mogelijk ook voor software in de cloud).	ISO 27002 2017: 14.2.4

4.3.3 U.03 Bedrijfcontinuïteit

Toelichting

Omdat de klant voor de continuïteit van haar bedrijfsvoering in hoge mate afhankelijk kan zijn van de beschikbare functionaliteit van softwarepakketten zijn maatregelen voor calamiteiten van essentieel belang. De beoogde continuïteit kan daarbij bepaald worden door externe factoren, zoals het 'omvallen' van cloud-leveranciers of de hostingproviders.

Bedrijfscontinuïteit omvat een set van maatregelen, die tijdens calamiteiten, zoals natuurrampen, binnen de overeengekomen maximale uitvalsduur (Recovery Time Objective (RTO)), zorgt voor het herstel van data en de kritische dienstverlening, waarbij dataverlies beperkt blijft tot het maximaal toegestane dataverlies. Bekende continuïteitsmaatregelen zijn: redundantie, disaster recovery en het periodiek aantonen dat herstelfuncties werken.

Doelstelling	Het waarborgen van het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie.		
Risico	Onnodig lange uitval van bedrijfsactiviteiten na calamiteiten waardoor bedrijfsdoelstellingen niet worden gehaald.		
Schaalgrootte	Middel en groot.		
Voor wie	Klant en leverancier.		
Control	De leverancier behoort processen, **procedures** en beheersmaatregelen te documenteren, te implementeren en te **handhaven**.		BIO 2019: 17.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procedures	1.	Een adequate risicobeheersing bij de klant impliceert een voorbereiding op het voor korte of lange termijn wegvallen van leveranciersondersteuning: • met disaster recovery procedures voor herstel van de applicatie-functionaliteit en data; • door een contractuele uitwijklocatie; • door de mogelijkheid van dataconversie naar alternatieve IT-systemen.	CIP
Handhaven	2.	De data behorende bij het softwarepakket en de beoogde bedrijfsmatige bewerking van de gegevens kan worden hersteld binnen de overeengekomen maximale uitvalsduur.	CIP

	3.	Periodiek wordt de beoogde werking van de disaster recovery herstelprocedures in de praktijk getest. Met cloud-leveranciers worden continuïteitsgaranties overeengekomen.	CIP

4.3.4 U.04 Input-/output-validatie

Toelichting

Het softwarepakket ontvangt invoer van de gebruiker en van andere applicaties. Deze invoer kan verschillende vormen hebben. Het softwarepakket dient eerst de invoer te normaliseren, voordat een validatie van de invoer kan worden uitgevoerd via mechanismen voor filtering.

Om de integriteit van de informatievoorziening te kunnen waarborgen, zijn inputvalidaties onmisbaar. Dit geldt ook voor elektronische berichten, zoals een E-factuur, loonaangifte etc.

Een bekende kwetsbaarheid van applicaties en dus ook van softwarepakketten is de zogenaamde SQL-injection. Als een applicatie de syntax van gebruikersinput niet of onvoldoende controleert op datgene wat nodig is voor de ontworpen applicatiefuncties, maar naar gebruikers toe bijvoorbeeld ook systeemcommando's reageert, dan is de kans groot dat het softwarepakket gehackt kan worden.

Deze kwetsbaarheden zijn door inputvalidatie relatief eenvoudig te voorkomen. Input-/outputcontroles verdienen extra aandacht bij softwarepakketten die worden gebruikt via openbare netwerken als internet, om zo het lagere beheersingsniveau van die omgeving te compenseren.

Doelstelling	Het beschermen van bedrijfsprocessen door zekerheid te verschaffen over de integriteit van de verwerkte data.		
Risico	Misbruiken van softwarepakketten en ongemerkt toegang krijgen tot gegevens en de beschikbaarheid, integriteit en vertrouwelijkheid van de data schaden.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Leverancier.		
Control	Het softwarepakket behoort mechanismen te bevatten voor **normalisatie** en **validatie** van invoer en voor **schoning** van de uitvoer.		SSD 2020: SSD-19 SSD 2020: SSD-20
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Normalisatie	1.	Het softwarepakket zorgt dat de invoer in een gestandaardiseerde vorm komt, zodat deze herkend en gevalideerd kan worden.	SSD 2020: SSD-19/01.01
Validatie	2.	Foute, ongeldige of verboden invoer wordt geweigerd of onschadelijk gemaakt. Het softwarepakket (of SaaS) voert deze controle van de invoer uit aan de serverzijde en vertrouwt niet op maatregelen aan de cliëntzijde.	SSD 2020: SSD-31/01.02
	3.	Het softwarepakket (of SaaS) valideert alle invoer die de gebruiker aan het softwarepakket verstrekt.	OWASP ASVS 2020: V12

	4.	Binnen het softwarepakket zijn beveiligingsmechanisme ingebouwd om bij import van gegevens, zogenaamde 'ingesloten' aanvallen te detecteren.	OWASP ASVS 2020: V12
Schoning	5.	Alle uitvoer wordt naar een veilig formaat geconverteerd.	SSD 2020: SSD-20/01.01

4.3.5 U.05 Sessiebeheer

Toelichting

Na de authenticatie moet een sessiemanager-component vanuit de server acties van gebruikers op een veilige manier volgen. Hiervoor zijn bewezen raamwerken en bibliotheken beschikbaar. Meestal gebeurt dit met een beveiligde sessietoken. Deze token moet op een veilige manier worden gecreëerd en verlopen. Tokens mogen geen misleidbare of gevoelige informatie bevatten.

Doelstelling	Het voorkomen dat onbevoegden zich via kwetsbaarheden toegang verschaffen tijdens langdurig openstaande sessies.		
Risico	Onbevoegden maken via kwetsbaarheden gebruik van openstaande sessies en krijgen toegang krijgen tot gevoelige data. Het ontstaan van zwakheden als Cross-Site Request Forgery (CSRF) en Clickjacking.		
Schaalgrootte	Groot.		
Voor wie	Leverancier.		
Control	Sessies behoren **authentiek** te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een **time-out** of perioden van inactiviteit.		SSD 2020: SSD-12 SSD 2020: SSD-14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Authentiek	1.	Softwarepakketten hergebruiken nooit sessie-tokens in URL-parameters of foutberichten.	SSD 2020: SSD-14/01.02
	2.	Softwarepakketten genereren alleen nieuwe sessies met een gebruikersauthenticatie.	SSD 2020: SSD-14/01.02
Time-out	3.	Sessies hebben een specifiek einde en worden automatisch ongeldig gemaakt wanneer: • ze niet langer nodig zijn; • gebruikers hun sessie expliciet hebben laten verlopen; • de limiet voor het verlopen van de harde sessies is bereikt.	SSD 2020: SSD-12/02.01

4.3.6 U.06 Gegevensopslag

Toelichting

De door softwarepakketten opgeslagen gegevens worden logisch beschermd tegen ongeoorloofde toegang door deze te versleutelen. Als logische toegang tot de oorspronkelijke gegevens niet vereist is, zoals bij wachtwoorden, dan moet de leesbaarheid onmogelijk worden gemaakt met hashing.

Doelstelling	Toegang tot opgeslagen gegevens door onbevoegden wordt verhinderd.		
Risico	Opgeslagen gegevens worden ongeautoriseerd ingezien, aangepast of verwijderd door ontoereikende versleuteling.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Leverancier.		
Control	**Te beschermen gegevens** worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden **versleuteld**. Opslag vindt alleen plaats als **noodzakelijk**.		SSD 2020: SSD-2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Te beschermen gegevens	1.	De opdrachtgever specificeert de classificatie van gegevens	SSD 2020: SSD-2/01.01
	2.	Indien van een gegeven niet de classificatie van vertrouwelijkheid is vastgesteld, wordt het gegeven per default veilig opgeslagen.	SSD 2020: SSD-2/01.02
Versleuteld	3.	Het softwarepakket voorkomt dat wachtwoorden in leesbare vorm worden opgeslagen door gebruik van hashing in combinatie met salts en minimaal 10.000 rounds of hashing.	SSD 2020: SSD-2/03.01
	4.	Gegevens worden door het softwarepakket deugdelijk versleuteld opgeslagen met passende standaarden voor cryptografie, tenzij door de gegevenseigenaar is gedocumenteerd dat dit niet noodzakelijk is. Cryptografische toepassingen voldoen aan passende standaarden.	SSD 2020: SSD-2/03.02 BIO 2019: 10.1.1.2
Noodzakelijk	5.	Te beschermen gegevens worden door het softwarepakket alleen opgeslagen als dat nodig is voor het doel en voor de kortst mogelijke tijd, zijnde de kortste periode tussen het vervullen van de toepassing en de door wet- of regelgeving verplichte periode.	SSD 2020: SSD-2/04.01

4.3.7 U.07 Communicatie

Toelichting

Om getransporteerde gegevens te beschermen, moeten deze worden beveiligd met een voldoende sterke beveiligingsmethode.

Doelstelling	Het beschermen van getransporteerde gegevens passend bij het classificatieniveau.	
Risico	Onbevoegden krijgen toegang tot getransporteerde gegevens.	
Schaalgrootte	Elke schaalgrootte.	
Voor wie	Leverancier.	
Control	Het softwarepakket past **versleuteling** toe op de communicatie van gegevens die **passend bij het classificatieniveau** is van de gegevens en **controleert** hierop.	SSD 2020: SSD-4
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Versleuteling	1.	Cryptografische toepassingen voldoen aan passende standaarden.	BIO 2019: 10.1.1.2
	2.	Het platform waarop het softwarepakket draait, zorgt voor de versleuteling van communicatie tussen de applicatieserver en webserver en tussen de applicatie en database. De webserver forceert versleuteling tussen de webserver en cliënt.	SSD 2020: SSD-4/01.02
Passend bij het classificatie-niveau	3.	De opdrachtgever specificeert de classificatie van de gegevens die worden uitgewisseld en waarvoor versleuteling plaatsvindt.	SSD 2020: SSD-4/02.01
Controleert	4.	Het softwarepakket zorgt waar mogelijk voor verificatie dat het certificaat: • is ondertekend door een vertrouwde Certificate Authority (CA); • een valide geldigheidsduur heeft; • nog geldig is en niet is ingetrokken.	SSD 2020: SSD-4/03.01 SSD 2020: SSD-4/03.02 SSD 2020: SSD-4/03.03
	5.	De versleutelde communicatie van het softwarepakket kan zodanig worden geconfigureerd, dat er geen terugval naar niet- of onvoldoende versleutelde communicatie ontstaat.	SSD 2020: SSD-4/03.04

4.3.8 U.08 Authenticatie

Toelichting

Toegang tot softwarepakketten door gebruikers wordt gereguleerd door het toegangsmechanisme gebruikersidentificatie (zoals een gebruikersaccount) en authenticatie (zoals een wachtwoord). Het softwarepakket stelt specifieke eisen aan de authenticatie van gebruikers. Het authenticatiemechanisme moet voldoen aan vooraf vastgestelde beveiligingseisen. Voor het verlenen van toegang tot softwarepakketten ontvangen gebruikers authenticatie-informatie. De gebruikers behoren hier vertrouwelijk mee om te gaan.

NB Dit object en de set van maatregelen is voor softwarepakketten relevant als de onderliggende infrastructuur geen toereikende set van maatregelen bevat, waarmee aan de control kan worden voldaan.

Doelstelling	Het vaststellen van de identiteit van een gebruiker van een softwarepakket.	
Risico	Onbevoegde personen krijgen toegang tot de data in het softwarepakket.	
Schaalgrootte	Elke schaalgrootte.	
Voor wie	Leverancier.	
Control	Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een **mechanisme voor identificatie en authenticatie**.	SSD 2020: SSD-5 SIG 3.2.3
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Mechanisme voor identificatie en authenticatie	1.	De authenticiteit wordt bereikt bij het zekerstellen van de volgende twee activiteiten: • Alle gebruikers zijn juist geauthentiseerd voordat ze toegang krijgen tot (modulen van) het softwarepakket. • Gebruikers kunnen veilig worden toegevoegd, verwijderd en/of geüpdatet in functies/functionaliteiten.	SIG 2015: 3.2.3
	2.	De configuratie van de identificatie- en authenticatievoorziening waarborgt dat de geauthentiseerde persoon inderdaad de geïdentificeerde persoon is.	SSD 2020: SSD-5/02.02
	3.	Het inlogmechanisme is robuust tegen herhaaldelijke, geautomatiseerde of verdachte pogingen om wachtwoorden te raden (brute-forcing of password spraying en hergebruik van gelekte wachtwoorden).	SSD 2020: SSD-5/02.04

4.3.9 U.09 Toegangsautorisatie

Toelichting

Na verkregen toegang met de identificatie en authenticatie ontvangen gebruikers (eindgebruikers en beheerders) autorisaties voor het gebruik van bedrijfs- en beheerfunctionaliteiten van softwarepakketten. De autorisatie zorgt ervoor dat gebruikers uitsluitend toegang krijgen tot die functionaliteit waartoe zij vanuit hun takenpakket recht op hebben.

Doelstelling	Toegang tot bedrijfs- en beheerfuncties toe te kennen en te beperken volgens het vereiste gebruikersprofiel.		
Risico	Het toegang krijgen tot gegevens die niet noodzakelijk zijn voor het uitvoeren van de rol/functie.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Klant en leverancier.		
Control	Het softwarepakket behoort een **autorisatiemechanisme** te bieden.		SSD 2020: SSD-8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Autorisatie-mechanisme	1.	Het softwarepakket biedt mechanismen, waarmee gebruikers, overeenkomstig hun verleende rechten en rollen, alleen informatie met specifiek belang kunnen inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	BIO 2019: 9.4.1.2 SSD 2020: SSD-8/01.03
	2.	Beheer(ders)functies van softwarepakketten worden extra beschermd, waarmee misbruik van rechten wordt voorkomen.	CIP

4.3.10 U.10 Autorisatiebeheer

Toelichting

De toegang tot gebruikersfunctionaliteiten worden georganiseerd met autorisatiebeheer en de toewijzing van een gebruikersaccount. Het softwarepakket moet technische invoermogelijkheden bieden

om via gebruikersrechten de toegang tot functionaliteiten te kunnen organiseren. Dit houdt in dat toegangsrechten tot functionaliteiten met gebruikersprofielen vanuit autorisatiebeheer toegekend dan wel ingetrokken kunnen worden.

Doelstelling	Bewerkstelligen dat de juiste mensen op het juiste moment om de juiste redenen toegang krijgen tot het softwarepakket.		
Risico	Misbruik van gegevens in een softwarepakket.		
Schaalgrootte	Groot.		
Voor wie	Klant en leverancier.		
Control	De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat **autorisaties** kunnen worden toegewezen aan organisatorische functies en **scheiding van niet verenigbare autorisaties** mogelijk is.		SSD 2020: SSD-7
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Autorisaties	1.	De rechten voor toegang tot gegevens en functies in het softwarepakket zijn op een beheersbare wijze geordend, gebruik makend van autorisatiegroepen.	SSD 2020: SSD-7/01.01
Scheiding van niet verenigbare autorisaties	2.	Met taken, verantwoordelijkheden en bevoegdheden zijn verenigbare taken en autorisaties geïdentificeerd.	SSD 2020: SSD-7/03.01
	3.	Er bestaat een proces voor het definiëren en onderhouden van de autorisaties.	SSD 2020: SSD-7/03.04

4.3.11 U.11 Applicatielogging

Toelichting

Logging is een proces voor het registreren van activiteiten en gebeurtenissen in systemen om achteraf de rechtmatigheid van de resourcebenadering en vroegtijdige ongeautoriseerde toegangspogingen van systemen en netwerken te kunnen signaleren.

Voorkomen moet worden dat (te) grote hoeveelheden logdata ontstaan. Logdata dient van hoge kwaliteit te zijn met relevante gebeurtenissen. Logdata bevat doorgaans gevoelige, persoonsgebonden en/of financiële gegevens en moet worden beschermd volgens de lokale privacywetgeving of richtlijnen.

Doelstelling	Het bieden van signaleringsfuncties voor registratie en detectie.
Risico	Afwijkingen van normaal gedrag binnen het softwarepakket zijn niet zichtbaar.
Schaalgrootte	Middel en groot.
Voor wie	Klant en leverancier.

Control	Het softwarepakket biedt signaleringsfuncties voor **registratie en detectie** die **beveiligd** zijn ingericht.		SSD 2020: SSD-30
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Registratie en detectie	1.	In de architectuur van het softwarepakket zijn detectiemechanismen actief voor het detecteren van aanvallen.	SSD 2020: SSD-30/01.03
	2.	De te registreren acties worden centraal opgeslagen.	SSD 2020: SSD-30/01.01
	3.	Er is vooraf bepaald wat te doen bij het uitvallen van loggingsmechanismen (alternatieve paden).	SSD 2020: SSD-30/03.01
Beveiligd	4.	De (online of offline) bewaartermijn voor logging is vastgesteld en komt tot uitdrukking in de configuratie-instellingen van binnen het softwarepakket.	SSD 2020: SSD-30/03.02

4.3.12 U.12 Application Programming Interface (API)

Toelichting

Een API is te beschouwen als een soort digitale stekkerdoos, die externe diensten of personen gecontroleerde toegang kan verschaffen tot interne diensten, algoritmes, apparaten en/of informatiebronnen.

De eigenschappen van een API maakt een algoritme, dienst, apparaat of data programmeerbaar en daarmee ook gevoelig voor aanvallen. De maatregelen hieronder zijn beperkt tot generieke eisen. Zie voor specifieke eisen over JavaScript Object Notation (JSON), Extensible Markup Language (XML) of Graph Query Language (GraphQL) en de Application Security Verification Standard (ASVS) van OWASP.

Bij cloud-toepassingen speelt de HyperText Markup Language (HTML)-5 ondersteuning van bepaalde browsers en de versie van die browser een belangrijke rol, onder andere voor de ondersteuning van bepaalde office-versies.

Doelstelling	Het bieden van veilige mechanismen voor onder andere import en export van gegevens.		
Risico	Gegevens kunnen niet uitgewisseld worden.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Leverancier.		
Control	Softwarepakketten behoren **veilige API's** te gebruiken voor import en export van gegevens.		OWASP ASVS 2020: V13
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Veilige API's	1.	Het softwarepakket maakt tijdens verwerking gebruik van veilige API's op basis waarvan additionele gegevens uit externe bronnen kunnen worden ingelezen en verwerkt.	SIG 2015: 3.3.6

	2.	API-URL's geven geen gevoelige informatie, zoals de API-sleutel, sessie-tokens enz. weer.	OWASP ASVS 2020: V13.1.3
	3.	Het softwarepakket maakt gebruik van veilige API's, die (automatisch) gebruikersdata scheiden van applicatiecode, waarmee injectie kwetsbaarheden zoals SQL injection en Cross-Site Scripting (XSS) te voorkomen.	SIG 2015: 3.3.6
	4.	Het softwarepakket gebruikt veilige API's die bufferlengtes controleren, waarmee kwetsbaarheden als Buffer- en Integer overflow worden voorkomen.	SIG 2015: 3.3.6

4.3.13 U.13 Gegevensimport

Toelichting

Softwarepakketten maken vrijwel altijd gebruik van upload- of download-mechanismen voor de import en export van (gebruikers)gegevens. In veel gevallen worden die gegevens verkregen vanuit niet vertrouwde cliënts, al dan niet gepositioneerd in niet vertrouwde[3] zones, waarna de gegevens getransporteerd worden via niet vertrouwde netwerken.

Om risico's voor de bedrijfsvoering te beperken, behoort hiervoor een samenhangende set van maatregelen te worden toegepast.

Doelstelling	Bewerkstelligen dat niet-vertrouwde omgevingen bestandsgegevens uit niet vertrouwde omgevingen veilig geïmporteerd en veilig opgeslagen worden.		
Risico	De beschikbaarheid, integriteit en vertrouwelijkheid van de data wordt geschaad.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Leverancier.		
Control	Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen **veilig te importeren en veilig op te slaan**.		OWASP ASVS 2020: V12
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Veilig te importeren en op te slaan	1.	Het softwarepakket biedt een flexibel quotummechanisme voor het importeren van gegevens uit externe bronnen.	OWASP ASVS 2020: V12.1
	2.	Binnen het softwarepakket zijn beveiligingsmechanismen ingebouwd om bij import van gegevens, 'ingesloten' aanvallen te detecteren.	OWASP ASVS 2020: V12.3
	3.	Het softwarepakket accepteert geen extreem grote bestanden, die buffers of het werkgeheugen kunnen 'overspoelen' en daarmee een Denial-of-Service (DoS)-aanval kunnen veroorzaken.	OWASP ASVS 2020: V12.1

[3] Zie voor de begrippen vertrouwde en niet-vertrouwde zones de beveiligingspatronen op de NORA online over zonering.

5 Control-domein

5.1 Doelstelling

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

1. de controls voldoende zijn ingericht en functioneren voor het garanderen van de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van softwarepakketten;
2. softwarepakketten functioneel en technisch op het juiste niveau worden gehouden.

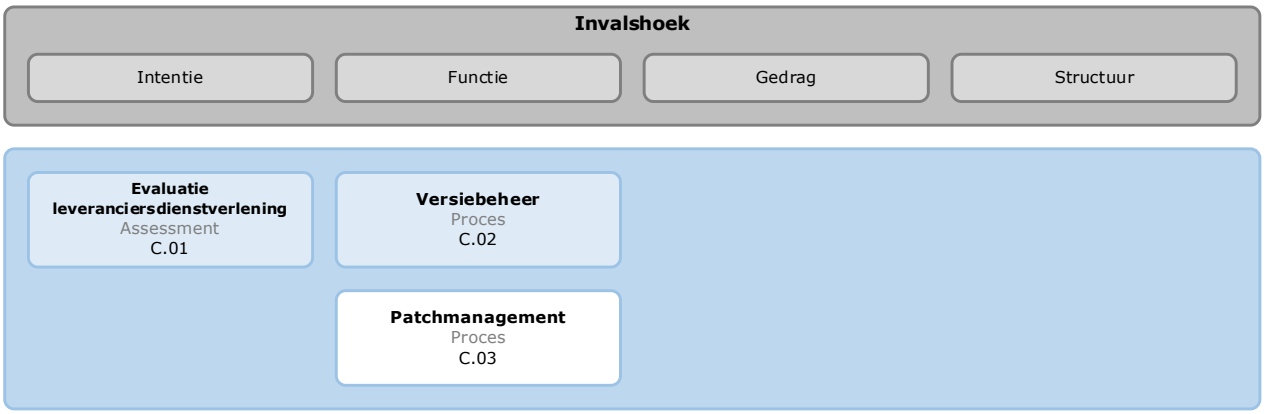
Dit houdt onder meer in dat binnen de organisatie een adequate beheersorganisatie moet zijn ingericht, waarin beheersprocessen zijn vormgegeven.

5.2 Risico's

Als de regie en control op noodzakelijke maatregelen binnen de klant en de leverancier ontbreken, is het niet zeker of de bedrijfs- en technische functies aan de beoogde beveiligingsvoorwaarden voldoen en dat de governance van deze omgeving toereikend is ingericht. Ook kan niet vastgesteld worden of de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Afbeelding 8 geeft de ordening van objecten in het control-domein weer met invalshoeken voor dit thema. Elk objectblok bevat de objectnaam, het basiselement en het objectnummer. Blauwgekleurde objecten zijn afgeleid van de BIO. De witte objecten zijn afgeleid van overige best practices.



Afbeelding 8: Overzicht softwarepakkettenobjecten in het control-domein

De objecten zijn in de volgende paragrafen uitgewerkt. Echter niet elk object is van toepassing voor elke softwarepakketselectie. Dit hangt af van verschillende factoren zoals: schaalgrootte, hostingslocatie, soort en integreerbaarheid met de bestaande IT. In tegenstelling tot andere thema's zijn aan de uitwerking toegevoegd:

1. Schaalgrootte
   De schaalgrootte geeft een globale indicatie (klein, middel of groot) in hoeverre de schaalgrootte van softwarepakketten van invloed kan zijn op de relevantie van een object. Met

klein wordt bedoeld getalsmatig en/of bedrijfsmatige impactbeperkte toepassing. Middel is voor middelgrote bedrijfstoepassingen, zoals boekhouding- en officetoepassingen. De waarde groot is voor grootschalig gebruik, enerzijds in aantallen, anderzijds in omvang van het softwarepakket zoals ERP en EDW.

2. Voor wie de control van toepassing is
   Het gaat om de klant en/of de leverancier. In veel gevallen is samenwerking tussen de klant en leverancier nodig om risico's tijdens het gebruik van de softwarepakketten afdoende te beperken.

5.3.1 C.01 Evaluatie leveranciersdienstverlening

Toelichting

Het overeengekomen niveau van de informatiebeveiliging en dienstverlening met de leverancier dient te worden gehandhaafd. De operationele beheersing daarvan wordt met leveranciersovereenkomsten geregeld via het proces 'Levenscyclusmanagement voor softwarepakketten'. Monitoring en beoordeling van prestaties en auditing is nodig om de naleving van overeenkomsten vast te stellen en om vastgestelde problemen in de operationele lijn op te lossen en te beheren.

Doelstelling	Het bepalen/vaststellen in hoeverre de leveranciersovereenkomst wordt nageleefd.		
Risico	De leverancier levert niet hetgeen is opgenomen in de overeenkomst.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Klant.		
Control	De klant behoort regelmatig de dienstverlening van softwarepakketleveranciers te **monitoren**, te **beoordelen** en te **auditen**.		BIO 2019: 15.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Monitoren	1.	De mate waarin de leveranciersovereenkomsten worden nageleefd, wordt geverifieerd.	ISO 27002 2017: 15.2.1a
Beoordelen	2.	De door leveranciers opgestelde rapporten over dienstverlening worden beoordeeld en zijn de basis voor besprekingen met de leveranciers voor zover dit is opgenomen in de overeenkomst.	ISO 27002 2017: 15.2.1b
Auditen	3.	Leveranciersaudits worden uitgevoerd in samenhang met rapportages over de dienstverlening.	ISO 27002 2017: 15.2.1c
	4.	Er wordt inzicht gegeven in de complete verslaglegging van leveranciersaudits.	ISO 27002 2017: 15.2.1d
	5.	Vastgestelde problemen worden opgelost en beheerd.	ISO 27002 2017: 15.2.1f

5.3.2 C.02 Versiebeheer

Toelichting

Versiebeheer is een beheerproces dat voor softwarepakketten verantwoordelijk is voor het beheren van softwareversies tijdens de levenscyclus van het product. Het vindt zowel bij de klant als bij de leverancier plaats. Dit geldt zowel voor lokale toepassingen als voor clouddiensten. Versiebeheer omvat het beheer van documenten die functionele en technische specificaties bevatten. Bij de leverancier borgt versiebeheer tijdens de levensduur van het softwarepakket de beschikbaarheid van de juiste versies van programmacode voor het onderhoud tijdens de levenscyclus tot en met uitfasering.

Doelstelling	Dat gemachtigden op ieder moment kunnen beschikken over de juiste versie van een softwarepakket.		
Risico	Werken met verouderde versies van een softwarepakket.		
Schaalgrootte	Elke schaalgrootte.		
Voor wie	Klant en leverancier.		
Control	Wijzigingen aan het softwarepakket binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele **procedures** voor wijzigingsbeheer.		BIO 2019: 14.2.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procedures	1.	De leverancier heeft versiebeheer adequaat geregeld en stelt de klant tijdig op de hoogte van de actueel te gebruiken versies.	CIP
	2.	Het versiebeheerproces wordt ondersteund met procedures en werkinstructies.	CIP

5.3.3 C.03 Patchmanagement

Toelichting

Adequaat uitgevoerd patchmanagement draagt voor een heel groot deel bij aan de informatieveiligheid als het gaat om de weerbaarheid tegen aanvallen. Betrouwbare leveranciers monitoren voortdurend of hun producten in exploitatie kwetsbaar zijn en reageren op het bekend worden van geslaagde aanvallen door snel verbeterde code uit te brengen in de vorm van patches of compleet nieuwe releases.

Doelstelling	Zekerstellen dat kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.
Risico	Kwetsbaarheden brengen de stabiliteit en betrouwbaarheid van systemen in gevaar.
Schaalgrootte	Elke schaalgrootte.
Voor wie	Klant en leverancier.

Control	Patchmanagement behoort **procesmatig en procedureel** uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over **technische kwetsbaarheden** van de gebruikte code, zodat **zo snel mogelijk** de laatste (beveiligings-)patches kunnen worden geïnstalleerd.		NCSC 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
Technische kwetsbaar-heden	2.	Het beheer van technische kwetsbaarheden in code omvat minimaal een risicoanalyse van de kwetsbaarheden en eventueel penetratietests en patching.	CIP
Zo snel mogelijk	3.	Actualisaties/patches voor kwetsbaarheden waarvan de kans op misbruik en ontstane schade hoog is, worden zo snel mogelijk geïnstalleerd.	BIO 2019: 12.6.1.1