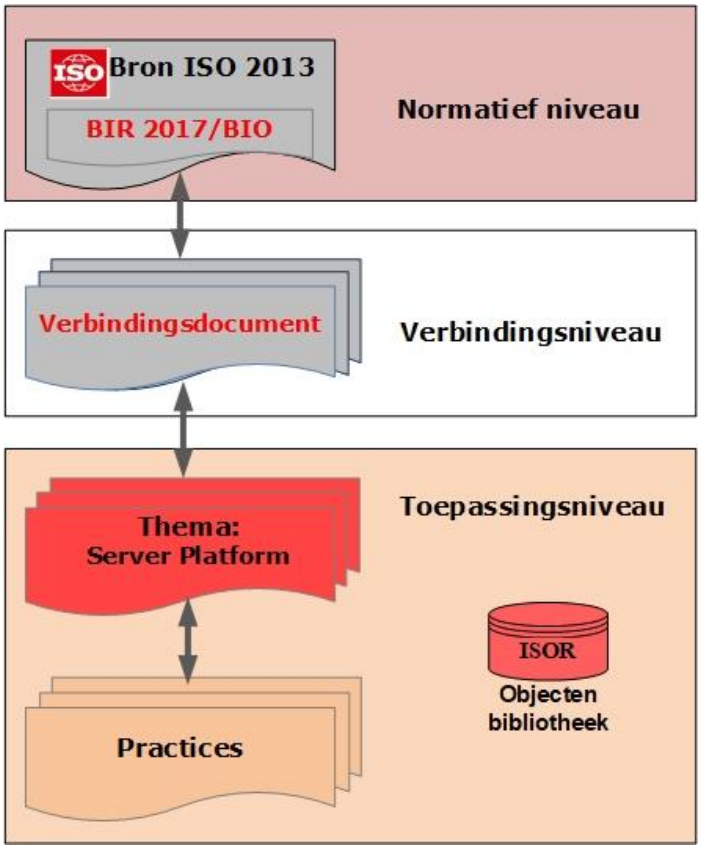
BIO Thema Serverplatform



Inhoud

Colofon		
Onderwerp	:	BIO Thema Applicatieontwikkeling
Datum	:	1-2-2019
Versie	:	Concept *1.0*
Uitgebracht aan	:	Voorzitter Werkgroep BZK: Henk Wesselink Directeur: CIP: Ad Reuijl

Documentbeheer BIO Thema: Serverplatform	
Naam	Organisatie
Jaap van der Veen (JV)	Ministerie van Financiën/Belastingdienst
Jan Breeman (JB)	UWV/CIP
Kees Hintzbergen (KH)	VNG/IBD
Paul Coret (PC)	Hoogheemraadschap Delfland
Peter van Dijk (PD)	VNG/IBD
René Reith (RR)	IPO (Interprovinciaal Overleg)
Ton Voogt	ICT Architects
Wiekram Tewarie (WT)	Doelorganisatie/CIP

Historie en versie

Versie	Datum	Doel	Naam	Status
0.1	11-02-2018	Initieel document	Wiekram Tewarie, Jaap van der Veen	Werkdocument
0.2	26-02-2018	Koppeling ISO	Freek Abels, Hilko Batterink, Farida Chotkan, Nico Noorland, Ton Voogt	Werkdocument
0.2.1	1-3-2018	Aanpassingen	Freek Abels	Werkdocument
0.2.2	8-3-2018	Aanpassingen	Ton Voogt	Werkdocument
0.3	26-3-2018	Aanpassingen	Ton Voogt	Werkdocument
0.3.1	28-3-2018	Aanpassingen	Hilko Batterink, Ton Voogt	Werkdocument
0.3.2	30-3-2018	IFGS toegevoegd	Ton Voogt	Werkdocument
0.3.3	3-4-2018	Aangepast naar SoGP 2016	Wiekram Tewarie, Ton Voogt	Werkdocument
0.4	30-5-2018	Objectnamen en IFGS aangescherpt	Wiekram Tewarie, Ton Voogt	Werkdocument
0.4.1	5-6-2018	Normen aangescherpt	Wiekram Tewarie, Ton Voogt	Werkdocument
0.4.2	15-8-2018	Normen herschreven	Ton Voogt	Werkdocument
0.5	29-8-2018	Objecten aangescherpt	Ton Voogt	Concept
0.8	17-9-2018	Aanpassingen n.a.v. reviews	Ton Voogt	Concept
0.8.1	7-11-2018	Aanpassingen n.a.v. reviews	Wiekram Tewarie, Jaap van Veen, Ton Voogt, Jan Breeman	Concept
0.8.2/ 0.84	7-11-2018	Aanpassingen n.a.v. reviews	Wiekram Tewarie, Jaap van Veen, Ton Voogt, Jan Breeman	Concept

0.9	17-12-2018	Conceptversie	Wiekram Tewarie, Jaap van der Veen, Ton Voogt, Jan Breeman	Concept
1.0	29-1-2019	Bijgewerkt tot conceptversie	Wiekram Tewarie, Jaap van der Veen, Jan Breeman	Concept

1. Inleiding

Dit document bevat een referentiekader voor het thema Serverplatform. Het is geënt op controls uit de BIO (Baseline Informatiebeveiliging Overheid) die gebaseerd is op ISO-27002. Er wordt ook gebruik gemaakt van andere Best Practices als: SoGP en NIST. Dit kader dient evenals andere BIO-thema's, als een toetsinstrument voor interne en externe leveranciers, om inzicht te geven over het beveiligings- en beheersingsniveau van haar ontwikkel- en onderhoudsorganisatie. Dit thema geeft tevens inzicht in de kwaliteitszorg die de leverancier dient toe te passen bij het opleveren van nieuwe infrastructuur.

1.1 Opzet van het thema

Het thema Serverplatform wordt achtereenvolgens uitgewerkt langs twee onderdelen: Structuur en Objecten. De structuur van dit themadocument bestaat uit een indeling op basis van Beleid, Uitvoering en Control (BUC). De objecten vormen de inhoudelijke onderwerpen die in de vorm van control en onderliggende criteria zullen worden behandeld. De objecten en de bijbehorende maatregelen worden gestructureerd door middel van een lagenstructuur.

Dit thema volgt de standaard opzet voor BIO-thema's:

a. scope en begrenzing (§1.2);
b. context en globale structuur van het thema (§1.3);
c. beveiligingsobjecten en uitwerking van deze objecten op de BUC lagen (§2.1);
d. presentatie van de objecten in de BUC/IFGS matrix, inclusief de volledigheidsanalyse van objecten (§2.1);
e. globale relaties van de geïdentificeerd beveiligingsobjecten (§2.2).

1.2 Scope en begrenzing

In dit thema is de scope van het begrip *serverplatform* beperkt tot de basis functionaliteit en algemene onderwerpen die gerelateerd zijn aan serverplatforms. Enkele componenten van dit thema zijn: server-hardware, virtualisatietechnologie en besturingssysteem (OS). Organisaties zullen op basis van deze informatie hun eigen servers in hun omgeving moeten beoordelen en nagaan welke risico's aanvullend gemitigeerd moeten worden.
Het beschrijft niet de kenmerken van specifieke type servers, zoals: bestandserver, applicatieserver, webserver, mailserver of databaseserver.

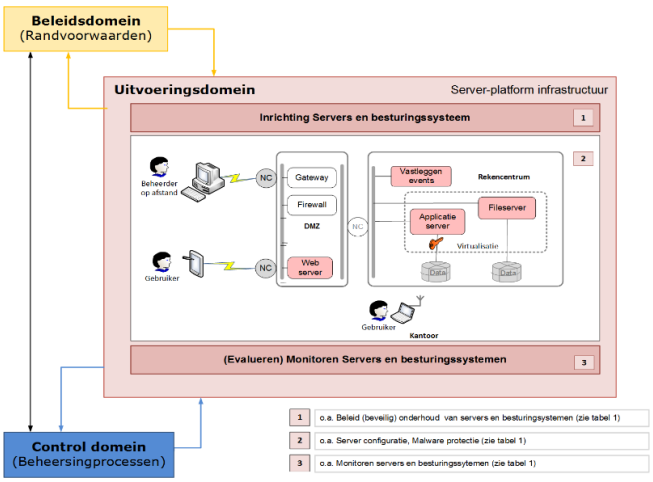
De objecten ten aanzien van serverplatform komen soms direct of indirect uit ISO 27002. De vertaling van objecten uit ISO 27002/BIO wordt geïllustreerd in tabel 1.

ISO/BIO object	Vertaling naar Thema: Serverplatform
Beleid voor beveiligd ontwikkelen (14.2.1)	Beleid voor (beveiligd) onderhouden van serverplatforms
Principes voor engineering van beveiligde systemen	Principes serverplatform beveiliging.

Tabel 1: Voorbeeld vertaling BIO objecten naar Thema 'Serverplatform' objecten

1.3 Context van serverplatform

Servers zijn computers, die via werkstations (clients), één of meerdere diensten aan



Afbeelding 1: Context thema Serverplatform

eindgebruikers of aan andere computersystemen beschikbaar stellen. Voorbeelden van servers zijn: file server, database server, mail server, web server, FTP server. Het kan ook gerelateerd zijn software die deze dienst mogelijk maakt: accepteert verzoeken van gebruikers en verwerkt deze. Aan een server hangt één of meerdere clients. **Fout! Verwijzingsbron niet gevonden.** geeft een globale context van enkele type servers en hoe ze in relatie staan met beleids- en beheersingsaspecten.

Een externe gebruiker logt bijvoorbeeld aan op een webserver vanuit internet. Dit type server geeft de relevante gebruikersgegevens door aan een portal-toegangsserver, die op zijn beurt applicatieve diensten vanuit backoffice-servers beschikbaar stelt. De onderste gebruiker in de afbeelding is een medewerker van een vertrouwde partij en zoekt via een semi-vertrouwd kanaal informatie op een webserver van de partnerorganisatie. De interne gebruiker logt aan op z'n werkstation via het lokale netwerk. In veel gevallen is er tevens sprake van 'middleware', oftewel applicatiecode die bepaalde functies vervult tussen de gebruikersapplicatie en het operating systeem.

2. Beveiligingsobjecten serverplatform

Objecten worden geïdentificeerd aan de hand van onderzoeksvragen en risicogebieden. De objecten zijn afgeleid vanuit de invalshoek van algemene beveiligingseisen: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid (BIVC) die vervolgens zijn ingedeeld in drie domein: Beleid, Uitvoering en Control. De vragen die hierbij een rol hebben gespeeld zijn:

- welke rand voorwaardelijke elementen spelen een rol bij de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
- welke elementen spelen een rol bij de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
- welke elementen spelen een rol bij de beheersing van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?

Afbeelding 3 geeft de positionering weer van servers binnen de lagenstructuur. Die functieblokken bevatten op hun beurt beveiligingsmaatregelen, die we vanuit de normatiek duiden als beveiligingsobjecten.

2.1 Vaststellen van beveiligingsobjecten voor serverplatform

Onderstaande tabel geeft een overzicht van alle relevante beveiligingsobjecten voor het serverplatform, afkomstig uit BIO die gebaseerd is ISO 27002 standaard; de BIO volgt dezelfde hoofdstuk indeling en control-teksten.

Uit de contextuele analyse blijkt dat er enkele onderwerpen bestaan die niet in de ISO/BIO voorkomen. Voor deze onderwerpen, waarvoor de BIO geen control heeft geformuleerd, worden controls uit andere baselines geadopteerd, zoals: Standard of Good Practice (SoGP), NIST en NCSC beveiliging web richtlijnen.

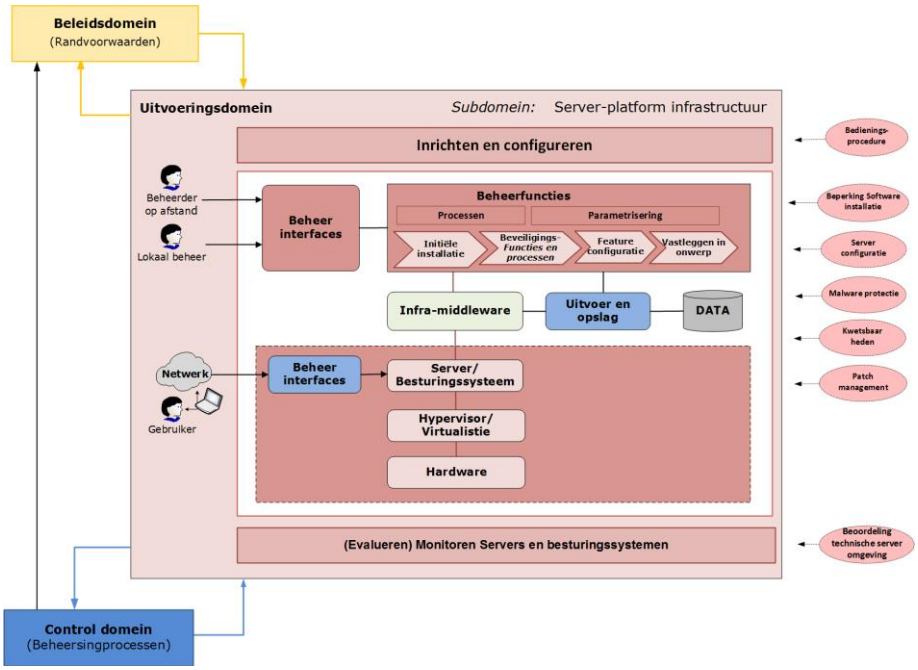
Nr.	Relevante beveiligingsobjecten	Referentie naar standaarden	IFGS
B.01	Beleid voor beveiligde inrichting en onderhoud	BIO/14.2.1	I
B.02	Principes voor inrichten van beveiligde servers	BIO/14.2.5	I
B.03	Serverplatform architectuur	SoGP/SD2.2 (afgeleid uit)	S
U.01	Bedieningsprocedure	BIO/12.1.1	I
U.02	Standaarden voor configuratie van servers	SoGP/SY1.2	I
U.03	Malwareprotectie	BIO/12.2.1	F
U.04	Beheer van serverkwetsbaarheden	BIO/12.6.1	F
U.05	Patch-management	BIO/12.6.1, NCSC/WA	F

U.06	Beheer op afstand	BIO/6.2.2 (Afgeleid)	F
U.07	Onderhoud van servers	BIO/11.2.4	F
U.08	Veilig verwijderen of hergebruiken van serverapparatuur	BIO/11.2.7	F
U.09	Hardenen van servers	SoGP/SYS1.25 en SYS12.8	G
U.10	Serverconfiguratie	SoGP/SY1.2	G
U.11	Virtueel serverplatform	SoGP/SY1.3	G
U.12	Beperking van software- installatie	BIO/12.6.2	G
U.13	Kloksynchronisatie	BIO/12.4.4	G
U.14	Ontwerpdocumentatie	SoGP/12.4.4	S
C.01	Evaluatie van richtlijnen voor servers en serverplatforms	BIO/10.10 2 (versie 2007)	I
C.02	Beoordeling technische serveromgeving	BIO/18.2.3	F
C.03	Logbestanden beheerders	BIO/12.4.3	G
C.04	Registratie van gebeurtenissen	BIO/12.4.1	G
C.05	Monitoren van servers en serverplatforms	NIST/AU-6	G
C.06	Beheerorganisatie servers en serverplatforms	Aanvullend	S

Tabel 2: Overzicht relevante beveiligingsobjecten voor het serverplatform

2.2 Globale relaties tussen de geïdentificeerde beveiligingsobjecten

Het thema Serverplatform omvat het geheel van beleid, richtlijnen, procedures, processen, mensen (actoren), middelen en registraties ten behoeve van het betrouwbaar functioneren van serverplatforms die het fundament vormen voor informatiesystemen. De essentiële objecten voor serverplatforms worden ingedeeld naar de domeinen: Beleidsdomein, Uitvoeringsdomein en Control domein en worden weergegeven in . Deze objecten worden in bijlage 1 verder toegelicht. De objecten per domein worden in hoofdstukken 3, 4 en 5 verder uitgewerkt. Moderne, gevirtualiseerde systeemomgevingen zien er mogelijk qua systeemtopologie geheel anders uit, maar de basiselementen die het fundament vormen voor informatiesystemen zijn niet anders.



Afbeelding 2: Gelaagdheid serverplatform met enkele beveiligingsobjecten (Bron: Nora)

Beleidsdomein

Geeft de randvoorwaarden, conditionele aspecten en contraints waar de inrichting van het serverplatform aan moeten voldoen.

Uitvoeringsdomein
De keuze van objecten uit ISO voor het thema serverplatform vloeit voort uit enkele uitgangspunten die gerelateerd is serverplatform:

- *initiële installatie*
  de initiële installatie wordt uitgevoerd op basis van richtlijnen en procedures, bijvoorbeeld: Bedieningsprocedure (ISO terminologie),
- *beveiligings- en beheerfuncties*
  de beveiligingsfunctie is gerelateerd aan protectie mechanismen die de beveiliging van de server moeten bevorderen, zoals malwareprotectie en hardenen van features. De beheerfuncties is gerelateerd aan enkele processen, zoals: Onderhoud van servers en Beheer van kwetsbaarheden,
- *feature configuratie*
  Servers hebben verschillende features. Deze features moeten adequaat zijn geconfigureerd om beveiligingsniveau te kunnen garanderen.
- *structuur en ontwerp*
  De configuraties van servers en de koppelingen en relatie tussen verschillende servers moet in een ontwerp document worden vastgelegd.

Control domein
Er zijn beoordelingsrichtlijnen vastgesteld voor het evalueren van de vastgestelde randvoorwaarden en de uitvoeringscomponenten.

3. Beleid domein

3.1 Doelstelling

De doelstelling van het beleidsdomein is de conditionele elementen te identificeren die rand voorwaardelijk zijn voor het inrichten, beveiligen en beheersen van de serverplatforms. De hiervoor van belang zijnde beveiligingsobjecten en de daaraan gerelateerde maatregel zijn opgenomen.

3.2 Risico's

Als de juiste beleidsaspecten voor de inrichting en onderhoud van het serverplatform ontbreken, bestaat het risico dat onvoldoende sturing wordt gegeven aan een veilige inrichting en exploitatie van deze systemen. Daardoor komt de informatievoorziening van de organisatie als geheel in gevaar en bestaat er een grote kans dat er datalekken optreden.

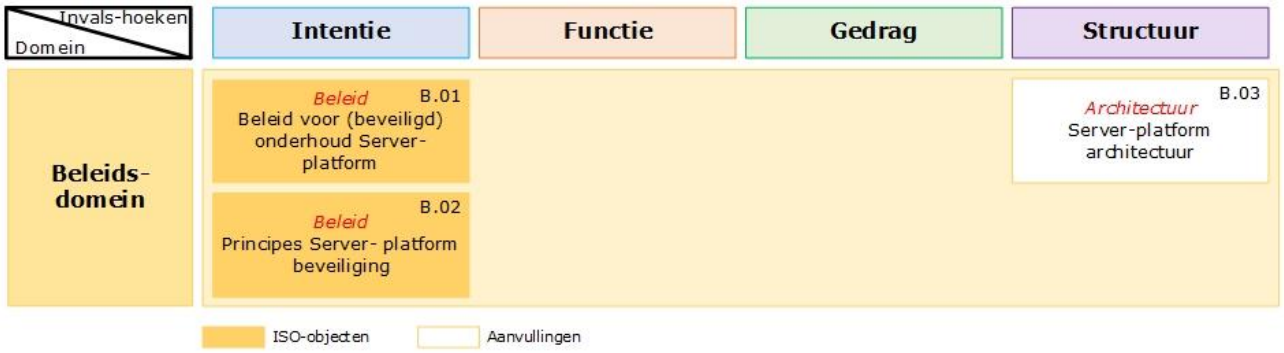
3.3 Specifieke beleidsobjecten

De onderwerpen die specifiek voor het serverplatform een rol spelen, zijn in Tabel 3 en Afbeelding 3 vermeld. Binnen de kolom functies behoren objecten te worden opgenomen die ten aanzien van het serverplatform gerelateerd zijn aan beveiligingsfuncties en beheerprocessen. Deze objecten hebben, in dit geval, echter meer een operationele karakter. Daarom zijn functie gerelateerde objecten in het Uitvoeringsdomein opgenomen. De noodzakelijke beveiligingseisen t.a.v. functies op dit niveau zijn vermeld in het beleid voor 'Serverplatform' (B.01).

Binnen de gedrag kolom zouden we een beleid ten aanzien van configuratie, parametrisering en toegangsbeleid tot serverplatform kunnen opnemen. Echter, dit soort beleidselementen komen, in dit geval, ook voor in het beleid voor 'Serverplatform' (B.01). Vandaar dat ook in deze kolom geen objecten zijn vermeld.

Nr.	Relevante beveiligingsobjecten	Referentie naar standaarden	IFGS
B.01	Beleid voor beveiligde inrichting en onderhoud	BIO: 14.2.1	I
B.02	Principes voor inrichten van beveiligde servers	BIO: 14.2.5	I
B.03	Serverplatform architectuur	SoGP: SD2.2 (afgeleid uit)	S

Tabel 3: Beleidsobjecten uitgewerkt in het beleidsdomein



Afbeelding 3: Beleidsobjecten naar invalshoek

B.01 Beleid voor beveiligde inrichting en onderhoud

De ISO-baseline (ISO, pg. 74) formuleert 'beveiligd ontwikkelen' als een eis voor het opbouwen van beveiligde dienstverlening, software, systemen en architectuur.

In dit thema wordt bij het object 'beleid voor (beveiligd) gericht op 'inrichtings- en onderhoudsaspecten' van serverplatform benadrukt. In het beleid worden onder andere standaarden en procedures beschreven voor het beveiligd inrichten en onderhouden van servers.

B.01		**Beleid voor beveiligde inrichting en onderhoud**	ISO27002: 14.2.1
Control		Voor het beveiligd inrichten en onderhouden van het serverplatform behoren *regels* te worden vastgesteld en binnen de organisatie te worden toegepast.	
Conformiteitsindicatoren en Maatregelen			
regels	*1.*	De gangbare principes rondom Security by design zijn uitgangspunt voor het onderhouden van servers.	BIO: 14.2.1.1
	2.	In het beleid voor beveiligd inrichten en onderhouden zijn de volgende aspecten in overweging genomen: a. het toepassen van richtlijnen/standaarden voor configuratie van servers en operating systemen; b. het gebruik van hardening richtlijnen; c. het toepassen van standaard images; d. het beperken van toegang tot krachtige faciliteiten en host parameter settings; e. het beschermen tegen ongeautoriseerde toegang.	SoGP: SY1.2.1

B.02 Principes voor inrichten van beveiligde servers

Bij het inrichten van een beveiligde server behoren beveiligingsprincipes in acht te worden genomen. In ISO zijn twee principes expliciet genoemd: "Security by design" en "Defense in depth". In andere baselines (zoals SoGP) zijn nog verschillende andere van belang zijnde inrichtingsprincipes te vinden.

B.02		**Principes voor inrichten van beveiligde servers**	ISO27002: 14.2.5
Control		De *principes* voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.	
Conformiteitsindicatoren en Maatregelen			
principes	*1.*	De gangbare principes rondom Security by design zijn uitgangspunt voor het inrichten van servers.	BIO: 14.2.1.1
	2.	Voor het beveiligd inrichten van serverszijn de volgende beveiligingsprincipes van belang: • defense in depth (beveiliging op verschillende lagen); • secure by default; • least privilege (minimale toegangsniveau); • fail secure, waarbij informatie in geval van een systeemfout niet toegankelijk is voor onbevoegde personen en niet kan worden gemanipuleerd of gewijzigd; • eenduidige naamgevingsconventie; • minimalisatie van Single points of failure.	SoGP: SY1

B.03 Serverplatform architectuur

De architectuur van een serverplatform geeft overzicht en inzicht in de wijze waarop de gebieden en objecten behoren te worden beveiligd. Architectuur geeft ook inzicht in de samenhang en samenwerking van beveiligingsmaatregelen. In de architectuur zijn gemaakte ontwerp en inrichtingskeuzen gedocumenteerd, verantwoord en zijn de gemaakte keuzen onderbouwd.

Documentatie speelt ook een belangrijke rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpfouten. Documentatie moet dan ook na elke wijziging worden bijgewerkt en oude documentatie moet worden gearchiveerd.

B.03		**Serverplatform architectuur**	SoGP: SD2.2
Control		De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een ***architectuurdocument*** vastgelegd.	
Conformiteitsindicatoren en Maatregelen			
architec-tuur-document	*1.*	Van het in te richten serverplatform is een actueel architectuurdocument 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; • wordt actief onderhouden.	SoGP: SD2.2
	2.	In het architectuurdocument is vastgelegd welke uitgangspunten, principes, beveiligingsvoorschriften, eisen en overwegingen gelden voor het inrichten van servers platformen.	SoGP: SD2.2

4. Uitvoering domein

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein voor inrichting en exploitatie van het serverplatform is het waarborgen dat de werkzaamheden plaatsvinden overeenkomstig specifieke beleidsuitgangspunten en dat de werking voldoet aan de eisen die door de klant (doelorganisatie) zijn gesteld.

4.2 Risico's

Wanneer adequate protectiefuncties voor het serverplatform ontbreken, ontstaan er risico's op het gebied van virus- en malwarebesmetting, dataverlies of datalekkage.

Wanneer meer functionaliteit is ingeschakeld dan nodig is voor de bedrijfsvoering, dan nemen risico's van diefstal of inbreuk toe.

Wanneer er onvoldoende zoneringsfuncties zijn geactiveerd, kunnen invloeden van buitenaf de dienstverlening via computers of netwerken onmogelijk maken.

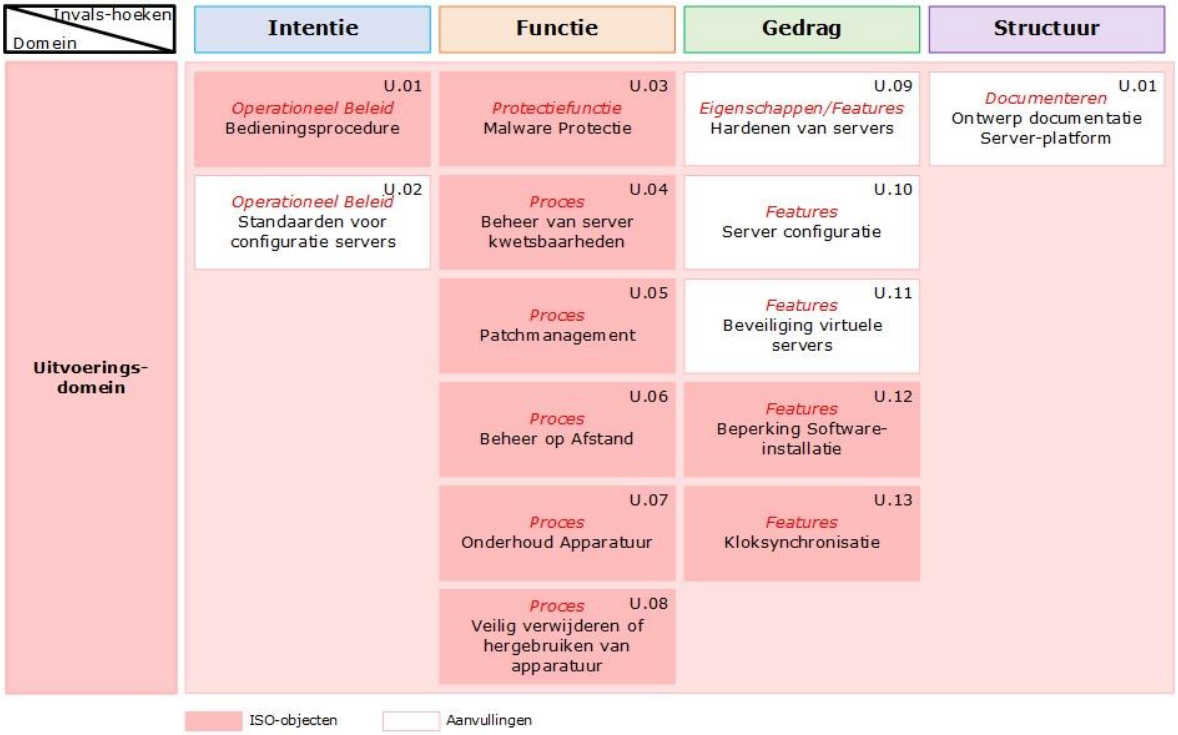
Hiaten in de systeemketens zoals Single points of Failure (SpoF), veroorzaken continuïteitsproblemen en maken 7x24 uur beschikbaarheidsgaranties praktisch onmogelijk.

4.3 Specifieke uitvoeringsobjecten

De onderwerpen die specifiek voor het serverplatform een rol spelen, zijn in Tabel 4 en Afbeelding 4 vermeld.

Nr	Generieke uitvoeringsobjecten serverplatform	Referenties	IFGS
U.01	Bedieningsprocedure	BIO: 12.1.1	I
U.02	Standaarden voor configuratie van servers	SoGP: SY1.2	I
U.03	Malwareprotectie	BIO: 12.2.1	F
U.04	Beheer van serverkwetsbaarheden	BIO: 12.6.1	F
U.05	Patch-management	BIO: 12.6.1, NCSC: WA	F
U.06	Beheer op afstand	BIO: 6.2.2 (Afgeleid)	F
U.07	Onderhoud van servers	BIO: 11.2.4	F
U.08	Veilig verwijderen of hergebruiken van serverapparatuur	BIO: 11.2.7	F
U.09	Hardenen van servers	SoGP: SYS1.25 en SYS12.8	G
U.10	Serverconfiguratie	SoGP: SY1.2	G
U.11	Virtueel serverplatform	SoGP: SY1	G
U.12	Beperking software installatie	BIO: 12.6.2	G
U.13	Kloksynchronisatie	BIO: 12.4.4	G
U.14	Ontwerpdocumentatie	SoGP: 12.4.4	S

Tabel 4: Uitvoeringsobjecten uitgewerkt in het uitvoeringsdomein



Afbeelding 4: Uitvoeringsobjecten naar invalshoek

U.01 Bedieningsprocedures

Bedieningsprocedures zijn een reeks verbonden taken of activiteiten die noodzakelijk zijn voor het beheren van serverplatforms. De activiteiten kunnen gerelateerd zijn aan het starten en afsluiten van de computer, back-up en onderhoud van servers.

U.01		**Bedieningsprocedures**	ISO27002: 12.1.1
Control		*Bedieningsprocedures* behoren te worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	
Conformiteitsindicatoren en Maatregelen			
bedienings-procedures	*1.*	Voor bedieningsactiviteiten die samenhangen met informatieverwerking en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, zijn gedocumenteerde procedures opgesteld.	BIO: 12.1.1
	2.	Wijzigingen aan bedieningsprocedures voor systeemactiviteiten worden formeel door hoger management goedgekeurd.	ISO27002: 12.1.1

	3.	In de bedieningsprocedures zijn de bedieningsvoorschriften opgenomen, onder andere voor: a. de installatie en configuratie van systemen; b. de verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig; c. de back-up; d. de eisen ten aanzien van de planning, met inbegrip van onderlinge verbondenheid met andere systemen; e. de voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen ten aanzien van het gebruik van systeemhulpmiddelen; f. de ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden; g. het beheer van audit- en systeemlogbestandinformatie; h. de procedures voor het monitoren van activiteiten.	ISO27002: 12.1.1

U.02 Standaarden voor configuratie van servers

Standaarden voor configuratie van servers representeren documenten waarin afspraken zijn vastgelegd ten aanzien van configuraties en parametrisering van serverinstellingen.

U.02		**Standaarden voor configuratie van servers**	SoGP: SY1.2
Control		Het serverplatform is geconfigureerd in overeenstemming met gedocumenteerde *standaarden*.	
Conformiteitsindicatoren en Maatregelen			
standaarden	*1.*	De documentatie conform de standaarden omvat: a. het bieden van gestandaardiseerde firmware-configuraties; b. het gebruik van gestandaardiseerde en vooraf bepaalde serverimages voor het bouwen/configureren van servers; c. het wijzigen van de standaardwaarden van leverancier- en andere beveiligingsparameters; d. het uitschakelen of beperken van onnodige functies en services; e. het beperken van de toegang tot krachtige beheerhulpmiddelen en host-parameter instellingen (bijvoorbeeld Windows 'Register-editor'); f. het beschermen tegen ongeoorloofde toegang; *g.* het uitvoeren van standaard beveiligingsbeheerpraktijken.	SoGP: SY1.2.1

U.03 Malwareprotectie

De organisatie maakt gebruik van malwareprotectie bij ingangs- en uitgangspunten van kritieke informatiesystemen (zoals Firewalls, e-mailservers, webservers, proxyservers, servers met externe toegang) en op werkstations, servers of mobiele computerapparatuur op het netwerk.
De organisatie gebruikt deze beschermingsmechanismen om haar servers te beschermen tegen schadelijke code en om schadelijke code te detecteren en te neutraliseren.

U.03		**Malwareprotectie**	ISO27002: 12.2.1
Control		Ter bescherming tegen malware behoren beheersmaatregelen voor *preventie, detectie* en *herstel* te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.	
Conformiteitsindicatoren en Maatregelen			
preventie	*1.*	Een formeel beleid wordt toegepast waarin het gebruik van ongeautoriseerde gebruik van software is verboden.	*ISO27002: 12.2.1*

	5.	Procedures zijn beschreven en verantwoordelijkheden benoemd voor de bescherming tegen malware.	*ISO27002: 12.2.1*
	4.	Severs zijn voorzien van (up-to-date) software die malware opspoort en daartegen beschermt.	*ISO27002: 12.2.1*
	2.	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	*BIO: 12.2.1*
	3.	Het downloaden van bestanden is beheerst en beperkt op basis van een risicoanalyse en van het principe "need-of-use".	*BIO: 12.2.1*
detectie	*6.*	Servers en hiervoor gebruikte media worden als voorzorgsmaatregel routinematig gescand op malware. De uitgevoerde scan omvat alle bestanden die op de server moeten worden opgeslagen.	*BIO: 12.2.1*
	7.	De malware scan wordt op alle omgevingen uitgevoerd.	*BIO: 12.2.1*
herstel	8.	Software die malware opspoort en bijbehorende herstelsoftware zijn geïnstalleerd en worden regelmatig geüpdate.	BIO: 12.2.1

U.04 Beheer van serverkwetsbaarheden

Kwaadwillenden maken gebruik van kwetsbaarheden en zwakheden in software die op de servers zijn geïnstalleerd. Kwetsbaarhedenbeheer is een proactieve benadering van beveiliging door de kans te verminderen dat gebreken in software de beveiliging van een server in gevaar brengt.

Zonder inzicht in de huidige stand van zaken, tast de beheerder in het duister en kan hij niet goed anticiperen op nieuwe ontwikkelingen. Vragen die hierbij een rol spelen:
- Hoe is de serveromgeving opgebouwd en geconfigureerd?
- Wat zijn bekende kwetsbaarheden en zwakheden?

Gerelateerd aan 'Kwetsbaarheden beheer' is het proces 'Patch-management'. Het ISO-onderwerp 'Beheer van technische kwetsbaarheden (12.6.1)' behandelt wat betreft de maatregelen twee onderwerpen:
- kwetsbaarheden beheer (vulnerability management) (zie: U.04);
- patchmanagement (zie: U.05).

In dit thema 'Serverplatform' worden deze twee onderwerpen apart beschreven.

U.04	**Beheer van serverkwetsbaarheden**	ISO27002: 12.6.1
Control	Informatie over *technische serverkwetsbaarheden*[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden *geëvalueerd* en passende maatregelen moeten worden genomen om risico's die hiermee samenhangen aan te pakken.	
Conformiteitsindicatoren en Maatregelen		
technische server kwetsbaar-heden	*1.* Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	BIO: 12.6.1
	2. Voor een doeltreffende kwetsbaarhedenanalyse van serverplatform en servers is informatie aanwezig over beschikbaarheid van: • (onderlinge)afhankelijkheden; • software t.a.v. versienummers, toepassingsstatus; • verantwoordelijken voor de software.	ISO27002: 12.6.1

1 Zie Handreiking:4.42 Penetratietesten

	3.	*Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen, zijn:* • *de rollen en verantwoordelijkheden in samenhang met beheer van technische kwetsbaarheden vastgesteld;* • *de middelen om technische kwetsbaarheden te bepalen vastgesteld.*	ISO27002: 12.6.1
	4.	*Met betrekking tot de technische kwetsbaarheden zijn voor een doeltreffend beheerproces, de activiteiten afgestemd op het incidentbeheerproces.*	ISO27002: 12.6.1
	5.	*Het proces Kwetsbaarhedenbeheer wordt uitgevoerd ten behoeve van:* • *identificatie van bekende technische kwetsbaarheden;* • *high-level inzicht in de kwetsbaarheden in de technische infrastructuur van de organisatie;* • *relevantie, gericht op de mate waarin het serverplatform en de servers kunnen worden blootgesteld aan bedreigingen;* • *prioriteit geven aan herstel van onderkende kwetsbaarheden.*	SoGP: TM1.1.6
	6.	*Technische kwetsbaarheden worden via de processen 'Patch management en of Wijzigingsbeheer' hersteld.*	SoGP: TM1.1.9
geëvalueerd	*7.*	*Het kwetsbaarheden beheerproces wordt regelmatig gemonitord en geëvalueerd.*	ISO27002: 12.6.1

U.05 Patch management

Patch-management is het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem. Een solide updatemechanisme is essentieel om voldoende beschermd te zijn tegen bekende beveiligingsproblemen in software.
De noodzaak van het patchen staat vaak niet ter discussie, vaak ontstaat echter wel discussie over de urgentie waarmee patches moeten worden uitgevoerd. De ernst van de kwetsbaarheid bepaald de noodzaak om de tijdsduur tussen het uitkomen van een patch en het implementeren van een patch zo kort mogelijk te houden. Daarom is het van belang vast te stellen welke doelstelling en prioriteit met patchmanagement worden nagestreefd. Het kan voorkomen dat systemen die niet meer ondersteund worden, (tijdelijk) operationeel gehouden moeten worden. In dat geval is het van belang om te weten welke systemen dat zijn en welke aanvullende maatregelen getroffen zijn om deze systemen voor het uitbuiten van kwetsbaarheden te behoeden, zodat inzicht bestaat over het al of niet uitvoeren van de patch op deze systemen.

U.05		**Patch-management**	ISO27002: 12.6.1 NCSC
Control		Patch-management is *procesmatig* en *procedureel* opgezet wordt ondersteund door *richtlijnen* zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.	
Conformiteitsindicatoren en Maatregelen			
proces-matig	*1.*	Patch-management proces is beschreven, goedgekeurd door het management en toegekend aan een verantwoordelijke functionaris.	NCSC: WA
	2.	Een technisch mechanisme zorgt voor (semi-) automatische updates.	NCSC: WA
	3.	Configuratiebeheer geeft het inzicht op basis waarvan de servers worden gepatcht.	NCSC: WA

	4.	Het patchbeheerproces bevat methoden om: a. patches te testen en te evalueren voordat ze worden geïnstalleerd; b. patches te implementeren op servers die niet toegankelijk zijn via het bedrijfsnetwerk; c. om te gaan met de mislukte of niet uitgevoerde patches; d. te rapporteren over de status van het implementeren van patches; e. acties te bepalen, ingeval een technische kwetsbaarheid niet met een patch kan worden hersteld, of een beschikbare patch niet kan worden aangebracht.	ISO27002: 12.6.1, SoGP: TM1.1.10
procedu-reel	*5.*	De patch-management procedure is actueel en beschikbaar.	NCSC: WA
	6.	De rollen en verantwoordelijkheden voor patchmanagement zijn vastgesteld.	NCSC: WA
	7.	De volgende aspecten van een patch worden geregistreerd: • de beschikbare patches; • hun relevantie voor de systemen / bestanden; • het besluit tot wel/niet uitvoeren; • de testdatum en het resultaat van de patch-test; • de datum van implementatie; en • het patchresultaat.	NCSC: WA
richtlijnen	*8.*	Ter ondersteuning van de patchactiviteiten is op het juiste (organisatorische) niveau een opgestelde patchrichtlijn vastgesteld en geaccordeerd.	NCSC: WA
	9.	Alleen beschikbare patches van een legitieme (geautoriseerde) bron mogen worden geïmplementeerd.	ISO27002: 12.6.1
	10.	De risico's die verbonden zijn aan het installeren van de patch worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid worden vergeleken met het risico van het installeren van de patch.	ISO 12.6.1
	11.	Wanneer voor een gepubliceerde technische kwetsbaarheid geen patch beschikbaar is, worden andere beheersmaatregelen overwogen, zoals: • het uitschakelen van functionaliteit of diensten; • het aanpassen of toevoegen van toegangsbeveiligingsmaatregelen, bijv. firewalls, rond de grenzen van netwerken; • het vaker monitoren om de werkelijke aanvallen op te sporen; • het kweken van bewustzijn omtrent de kwetsbaarheid.	ISO 12.6.1

U.06 Beheer op afstand

Toegang tot de servers is beperkt tot geautoriseerde personen en informatiesystemen.
Onder bepaalde voorwaarden is het beheerders die "van buiten" de door de organisatie beheerde netwerken, toegestaan servers te benaderen.

U.06		**Beheer op afstand**	ISO27002: 6.2.2
Control		*Richtlijnen* en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.	
Conformiteitsindicatoren en Maatregelen			
richtlijnen	*1.*	Toegang tot kritieke systemen voor beheer op afstand door externe personen wordt beheerd door middel van: a. het definiëren en overeenkomen van de doelstellingen en reikwijdte van de geplande werkzaamheden; b. het autoriseren van individuele sessies; c. het beperken van toegangsrechten (binnen doelstellingen en reikwijdte); d. het loggen van alle ondernomen activiteiten; e. het gebruiken van unieke authenticatiereferenties voor elke implementatie; f. het toewijzen van toegangsreferenties aan individuen in plaats van gedeeld; g. het intrekken van toegangsrechten en het wijzigen van wachtwoorden onmiddellijk nadat het overeengekomen onderhoud is voltooid; h. het uitvoeren van een onafhankelijke beoordeling van onderhoudsactiviteiten op afstand.	SoGP: NC1.6.1
	2.	Het op afstand onderhouden van servers wordt strikt beheerd door middel van: a. het verifiëren van de bron van de verbinding op afstand; b. het bepalen van de toestemming voordat toegang wordt verleend voor de connectiviteit; c. het beperken van het aantal gelijktijdige externe verbindingen; d. het bewaken van activiteiten gedurende de gehele duur van de verbinding; e. het uitschakelen van de verbinding zodra de geautoriseerde activiteit voltooid is.	SoGP: NC1.6.4
	3.	Het serverplatform is zodanig ingericht, dat deze op afstand kan worden geconfigureerd en beheerd en dat automatisch kan worden gecontroleerd of vooraf gedefinieerde parameters en drempelwaarden worden aangetast of overschreden.	SoGP: SY1.1.2
	4.	Handmatige interventie wordt niet toegepast, tenzij geautoriseerd en gedocumenteerd.	SoGP: SY1.1.2
	5.	Alle externe toegang tot servers vindt versleuteld plaats.	SoGP: SY1.1.2

U.07 Onderhoud van servers

In dit thema wordt apparatuur vanuit de ISO opgevat als het infrastructuurcomponent 'server' die periodiek onderhouden dient te worden. Het onderhoud behoort plaats te vinden binnen een tijdsinterval. Servers worden correct onderhouden door bevoegd personeel, om te zorgen dat de beschikbaarheid van de dienstverlening en de integriteit hiervan gegarandeerd is.

U.07		**Onderhoud van servers**	ISO27002: 11.2.4
Control		Servers behoren correct te worden *onderhouden* om de continue beschikbaarheid en integriteit te waarborgen.	
Conformiteitsindicatoren en Maatregelen			
onderhouden	*1.*	Het onderhoud van servers wordt uitgevoerd op basis van richtlijnen die invulling geven aan de volgende eisen: a. onderhoud wordt uitgevoerd in overeenstemming met de door de leverancier aanbevolen intervallen voor servicebeurten; b. alleen bevoegd onderhoudspersoneel voert reparaties en onderhoudsbeurten uit; c. van alle vermeende en daadwerkelijke fouten en van al het preventieve en correctieve onderhoud wordt registratie bijgehouden; d. voor onderhoud vanuit interne of externe locaties worden passende maatregelen getroffen; *e.* voordat servers na onderhoud weer in bedrijf worden gesteld, vindt een inspectie plaats om te waarborgen dat niet is geknoeid met de server en dat deze nog steeds of weer goed functioneert.	ISO27002: 11.2.4

U.08 Veilig verwijderen of hergebruiken van serverapparatuur

Opslagmedia van apparatuur bevat vaak vertrouwelijke informatie. Wanneer servers buiten gebruik worden gesteld of opnieuw worden ingezet, moet deze informatie veilig verwijderd zijn of worden.

U.08		**Veilig verwijderen of hergebruiken van serverapparatuur**	ISO27002: 11.2.7
Control		Alle onderdelen van servers met *opslagmedia* behoren te worden *geverifieerd*, om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	
Conformiteitsindicatoren en Maatregelen			
opslagmedia	*1.*	Van de server(s): a. wordt informatie welke niet meer benodigd is, vernietigd door middel van het verwijderen of overschrijven gebruikmakend van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen; b. worden opslagmedia die niet meer benodigd zijn en die vertrouwelijke of door auteursrecht beschermde informatie bevatten fysiek vernietigd.	ISO27002: 11.2.7
geverifieerd	*2.*	Voorafgaand aan verwijdering of hergebruik wordt gecontroleerd of de server opslagmedia bevat en of de informatie is vernietigd.	ISO27002: 11.2.7

U.09 Hardenen van servers

De standaardconfiguratie van de meeste besturingssystemen is niet ontworpen met beveiliging als de primaire focus, in plaats daarvan zijn standaardinstellingen meer gericht op bruikbaarheid, communicatie en functionaliteit.

Hardening is het proces van het uitschakelen of verwijderen van overbodige en/of niet gebruikte functies, services en accounts, waarmee de beveiliging wordt verbeterd.

Ook servers behoren te worden gehardend; alle overbodige en niet gebruikte functies, services en

accounts behoren van de server(s) te worden verwijderd of te worden uitgeschakeld.

U.09		**Hardenen van servers**	SoGP: SY1.2.5, SY1.2.8
Control		Voor het beveiligen van servers worden overbodige *functies* en ongeoorloofde *toegang* uitgeschakeld.	
Conformiteitsindicatoren en Maatregelen			
functies	*1.*	Servers zijn zodanig geconfigureerd dat onderstaande functies zijn verwijderd of uitgeschakeld: a. niet-essentiële en overbodige (redundant) services; b. het kunnen uitvoeren van gevoelige transacties en scripts; c. krachtige beheer-hulpmiddelen; d. het "run" commando" en "command-processors"; e. de "auto-run"-functie.	SoGP: SY1.2.5
	2.	Servers zijn zodanig geconfigureerd dat gebruik van onderstaande functies wordt beperkt: a. communicatiediensten die inherent vatbaar zijn voor misbruik; b. communicatieprotocollen die gevoelig zijn voor misbruik.	SoGP: SY1.2.5
toegang	*3.*	Servers worden beschermd tegen ongeoorloofde toegang doordat: a. onnodige of onveilige gebruikersaccounts zijn verwijderd; b. belangrijke beveiliging gerelateerde parameters zijn gewijzigd; c. time-out faciliteiten worden gebruikt, die: – automatisch na een vooraf bepaalde periode van inactiviteit sessies sluiten en een blanco scherm tonen op de beheerschermen; – vereisen dat opnieuw wordt ingelogd voordat een beheerscherm zich herstelt.	SoGP: SY1.2.8

U.10 Serverconfiguratie

Serverplatforms hebben verschillende features en bieden een veelheid van functies om services te kunnen leveren. Om veilig te laten functioneren, behoort elk serverplatform conform bepaalde standaarden en procedures te zijn geconfigureerd.

U.10		**Serverconfiguratie**	SoGP: SY1.2
Control		Serverplatforms behoren zo *geconfigureerd* te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen *ongeautoriseerd* en incorrecte updates.	
Conformiteitsindicatoren en Maatregelen			
geconfigu-reerd	*1.*	De Servers zijn geconfigureerd in overeenstemming met gedocumenteerde standaarden/procedures en welke betrekking hebben op: a. het inrichten van standaard firmware-configuraties; b. het gebruik van gestandaardiseerde vooraf bepaalde serverimages voor het bouwen/configureren van servers; c. het wijzigen van de standaardwaarden en andere beveiligingsparameters van de leverancier(s); d. het verwijderen, uitschakelen en/of beperken van onnodige functies en services; e. het beperken van de toegang tot krachtige beheerhulpmiddelen en host-parameterinstellingen; f. het beschermen tegen ongeoorloofde toegang; g. het uitvoeren van standaard beveiligingsbeheerpraktijken.	SoGP: SY1.2.1

	2.	De servers zijn geconfigureerd in overeenstemming met een gestandaardiseerde en vooraf bepaald serverimage.	SoGP: SY1.2.3
ongeautori-seerd	*3.*	Toegang tot server parameterinstellingen en krachtige beheerinstrumenten is: - beperkt tot een gelimiteerd aantal geautoriseerde personen; - beperkt tot specifiek omschreven situaties; - gekoppeld aan specifieke en gespecificeerde autorisatie.	SoGP: SY1.2.7

U.11 Virtueel serverplatform

Servervirtualisatie stelt een organisatie in staat om één of meer gescheiden 'logische' omgevingen te creëren op één fysieke server. Bij virtualisatie zijn drie soorten componenten betrokken: een fysieke server, een hypervisor en één of meerdere virtuele servers.
De hypervisor alloceert resources van de fysieke server naar elke onderliggende virtuele server, inclusief CPU, geheugen, harddisk of netwerk; hiermee zijn de virtuele servers in staat simultaan of geïsoleerd van elkaar te opereren. Deze drie componenten moeten voldoen aan specifieke eisen.

U.11		**Virtueel serverplatform**	SoGP: SY1.3
Control		Virtuele servers behoren goedgekeurd te zijn en toegepast te worden op robuuste en veilige *fysieke servers* (bestaande uit *hypervisors* en *virtuele servers*) en behoren zodanig te zijn geconfigureerd dat gevoelige informatie in voldoende mate is beveiligd.	
Conformiteitsindicatoren en Maatregelen			
virtuele servers	*1.*	Virtuele servers worden ingezet, geconfigureerd en onderhouden conform standaarden en procedures, die de bescherming omvat van: - fysieke servers, die worden gebruikt voor het hosten van virtuele servers; - hypervisors, die zijn geassocieerd met virtuele servers; - virtuele servers die op een fysieke server worden uitgevoerd	SoGP: SY1.3.1 en SY1.3.2
	2.	Virtuele servers worden beschermd met standaard beveiligingsmechanismen op hypervisors, waaronder: • het toepassen van standaard beveiligingsrichtlijnen ten aanzien van fysieke en logische toegang; • het hardenen van de fysieke en virtuele servers; • wijzigingsbeheer, malwareprotectie; • het toepassen van monitoring en van netwerk gebaseerde beveiliging.	SoGP: SY1.3.6 en SY1.3.7
fysieke servers	*3.*	Fysieke servers worden gebruikt om virtuele servers te hosten en worden beschermd tegen: • onbeheerde en ad hoc inzet van virtuele servers (zonder juiste procedures aanvraag, creëren en schonen); • overbelasting van resources (CPU, geheugen en harde schijf) door het stellen van een limiet voor het aanmaken van het aantal virtuele servers op een fysieke host server.	SoGP: SY1.3.4
hypervisors	*4.*	Hypervisors worden geconfigureerd om: • virtuele servers onderling (logisch) te scheiden op basis van vertrouwelijkheidseisen en om te voorkomen dat informatie wordt uitgewisseld tussen discrete omgevingen; • de communicatie tussen virtuele servers te coderen; • de toegang te beperken tot een beperkt aantal geautoriseerde personen; • de rollen van hypervisor administrators te scheiden.	SoGP: SY1.3.5

U.12 Beperking van software-installatie

Voor het gebruik van software (door een beheerder) op een server zijn regels opgesteld.

U.12		**Beperking van software-installatie**	ISO27002: 12.6.2
Control		Voor het door gebruikers (beheerders) installeren van software behoren *regels* te worden vastgesteld en te worden geïmplementeerd.	
Conformiteitsindicatoren en Maatregelen			
regels	*1.*	Gebruikers (beheerders) kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (white-list).	BIO: 12.6.2
	2.	De organisatie past een strikt beleid toe ten aanzien van het installeren en gebruiken van software.	ISO27002: 12.6.2
	3.	Het principe van least-privilege wordt toegepast.	ISO27002: 12.6.2
	4.	De rechten van beheerders worden verleend op basis van rollen.	ISO27002: 12.6.2

U.13 Kloksynchronisatie

Om gebeurtenissen uit verschillende componenten te correleren, worden de klokken van de verschillende systemen gelijkgericht en waarmee de timestamps van gebeurtenissen zijn gesynchroniseerd. Dit synchroniseren is het effect van de juiste instelling van tijd op betreffende componenten.
Met behulp van het Network Time Protocol (NTP) wordt bereikt dat de tijd op alle servers en andere componenten overeenkomt (zie paragraaf 10.10.6 'Synchronisatie van systeemklokken' in NEN/ISO-IEC 27002 'Code voor informatiebeveiliging').

U.13		**Kloksynchronisatie**	ISO27002: 12.4.4
Control		De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein zijn *gedocumenteerd* en *gesynchroniseerd* op één referentietijdbron.	
Conformiteitsindicatoren en Maatregelen			
gedocumen-teerd	*1.*	De systemen zijn met een standaard referentietijd voor gebruik geconfigureerd, zodanig dat gebruik gemaakt wordt van een consistente en vertrouwde datum- en tijdbron en dat gebeurtenislogboeken nauwkeurige tijdstempels gebruiken.	ISO27002: 12.4.4, SoGP: TM1.2.3
synchroni-satie	*2.*	De interne en externe eisen voor weergave, synchronisatie en nauwkeurigheid van tijd en de aanpak van de organisatie om een referentietijd op basis van externe bron(nen) te verkrijgen en hoe de interne klokken betrouwbaar te synchroniseren zijn gedocumenteerd.	ISO27002: 12.4.4

U.14 Ontwerpdocumentatie

De relatie tussen servers en de instellingen van configuraties moeten zijn vastgelegd in een ontwerpdocument.

U.14		**Ontwerpdocumentatie**	SoGP: SY1.1.1
Control		Het *ontwerp* van een serverplatform behoort te zijn gedocumenteerd.	
Conformiteitsindicatoren en Maatregelen			
ontwerp	*1.*	Het ontwerp van elk serverplatform en elke server is gedocumenteerd, waarbij o.a. beschreven is: - dat in het ontwerp rekening is gehouden met de principes van de beveiligingsarchitectuur en beveiligingsvereisten; - dat in het ontwerp rekening is gehouden met de risico's ten aanzien van voorzienbare ontwikkelingen in het gebruik van IT door de organisatie.	SoGP: SY1.1.1

5. Control domein

5.1 Doelstelling

Doelstelling van het control domein is om vast te stellen of:

- de beoogde controls voldoende zijn ingericht en functioneren voor het garanderen van de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van het serverplatform;
- de infrastructurele 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

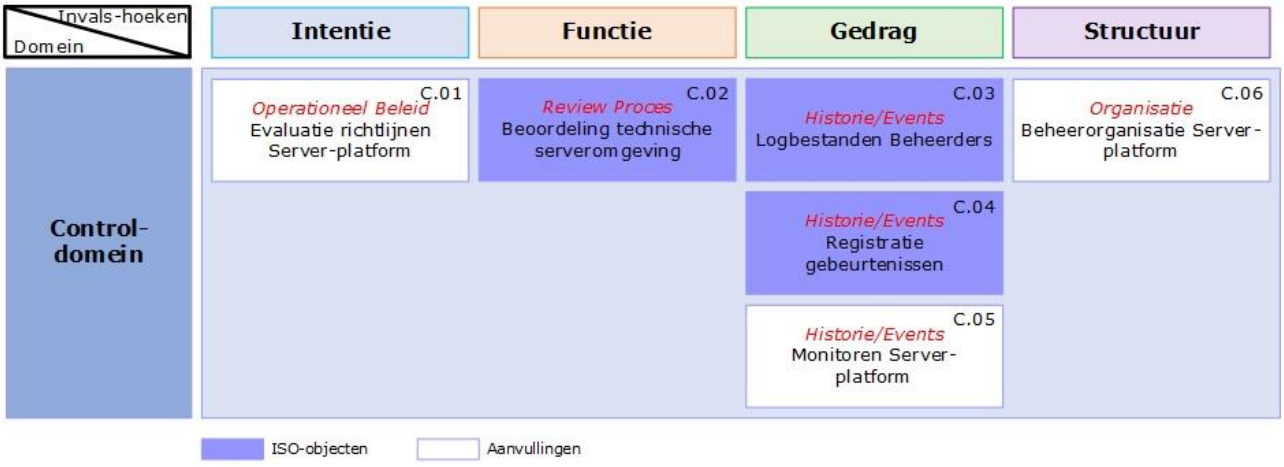
Door het ontbreken van noodzakelijke maatregelen binnen de organisatie van de IT-Leverancier is het niet zeker of de ontwikkel- en onderhoud- administratie aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet en dat de governance van deze omgeving toereikend is ingericht. Tevens kan er niet vastgesteld worden dat de gewenste maatregelen worden nageleefd.

5.3 Specifieke control-objecten

De onderwerpen die specifiek voor het serverplatform een rol spelen, zijn in Tabel 5 en in Afbeelding 5 vermeld.

Nr	Generieke control-objecten voor serverplatform	Referenties	IFGS
C.01	Evaluatie van richtlijnen voor servers en serverplatforms	ISO27002-2007: 10.10 2	I
C.02	Beoordeling technische serveromgeving	ISO27002: 18.2.3	F
C.03	Logbestanden beheerders	ISO27002: 12.4.3	G
C.04	Registratie gebeurtenissen	ISO27002: 12.4.1	G
C.05	Monitoren van servers en serverplatforms	NIST AU-6	G
C.06	Beheerorganisatie servers en serverplatforms	xxx	S

Tabel 5: Control-objecten uitgewerkt in het control domein



Afbeelding 5: Control-objecten naar invalshoek

C.01 Evaluatie richtlijn servers en serverplatforms

Binnen de infrastructuur bevinden zich verschillende servers en besturingssystemen die het fundament vormen voor applicaties. Deze servers en besturingssystemen moeten daarom continu worden onderhouden, gehardend en op een veilige wijze geconfigureerd. Het is van groot belang dat deze servers en besturingssystemen, in het kader van risicomanagement, periodiek geëvalueerd worden. De evaluatie activiteiten dienen ondersteund te worden met evaluatie richtlijnen, procedures en instructies. Anders bestaat het risico dat deze resultaten van de controle activiteiten niet voldoen aan de verwachte eisen. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

C.01		**Evaluatie richtlijnen servers en serverplatforms**	ISO27002: 10.10.2 (versie 2007)
Control		*Richtlijnen* behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.	
Conformiteitsindicatoren en Maatregelen			
richtlijnen	*1.*	De organisatie beschikt over richtlijnen voor het beoordelen van de technische omgeving van servers en besturingssystemen.	ISO27002: 10.10.2 (2007)
	2.	De organisatie beschikt over geautomatiseerde middelen voor effectieve ondersteuning van de controle activiteiten.	ISO27002: 10.10.2 (2007)
	3.	De organisatie beschikt over richtlijnen voor het uitvoeren van registratie, statusmeting, analyse, rapportage en evaluatie.	ISO27002: 10.10.2 (2007)
	4.	De organisatie heeft de taken, verantwoordelijkheden en bevoegdheden (TVB's) van controle functionarissen vastgelegd.	ISO27002: 10.10.2 (2007)

C.02 Beoordeling technische serveromgeving

Het is noodzakelijk om de technische omgeving regelmatig te beoordelen om de beveiliging doeltreffend te kunnen beheersen. Hiertoe dienen periodiek zowel de organisatorische als technische aspecten beoordeeld te worden, zoals: de toepassing van het geformuleerd inrichtingsbeleid voor servers, serverplatform architectuur, taken en verantwoordelijkheden, gebruik van technische middelen, frequentie, controle aanpak en inschakelen van externe specialisten. Als resultaat dient een rapportage van bevindingen aan het management te worden uitgebracht.

C.02		**Beoordeling technische serveromgeving**	ISO27002: 18.2.3
Control		Technische serveromgevingen behoren regelmatig te worden beoordeeld op *naleving* van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.	
Conformiteitsindicatoren en Maatregelen			
naleving	*1.*	Technische naleving wordt bij voorkeur beoordeeld met behulp van geautomatiseerde instrumenten die technische rapporten vervaardigen en geïnterpreteerd door een technisch specialist.	ISO27002: 18.2.3
	2.	Periodiek worden, na verkregen toestemming van het management, penetratietests of kwetsbaarheidsbeoordelingen uitgevoerd.	ISO27002: 18.2.3
	3.	De uitvoering van dergelijke tests worden gepland en gedocumenteerd en zijn herhaalbaar.	ISO27002: 18.2.3

	4.	Beoordeling van technische naleving wordt uitsluitend uitgevoerd door competente, bevoegde personen of onder toezicht van het management.	ISO27002: 18.2.3

C.03 Logbestanden beheerders

Logging is het proces voor het registreren van technische activiteiten en gebeurtenissen. Hiermee kunnen achteraf fouten of onrechtmatigheden in het gebruik van waaronder ongeautoriseerde toegangspogingen tot technische componenten vroegtijdig worden gesignaleerd. Het loggen van activiteiten spitst zich toe tot de bewaking van rechtmatigheid van toegekende rechten en het gebruik hiervan.

C.03		**Logbestanden beheerders**	ISO27002: 12.4.3
Control		Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de *logbestanden* behoren te worden beschermd en regelmatig te worden beoordeeld.	
Conformiteitsindicatoren en Maatregelen			
log-bestanden	*1.*	De logbestanden worden beschermd tegen ongeautoriseerd manipuleren en worden beoordeeld om vast te stellen wie welke activiteit heeft uitgevoerd.	ISO27002: 12.4.3
	2.	Speciale gebruikers geven rekenschap over de door hun uitgevoerde beheer activiteiten.	ISO27002: 12.4.3

C.04 Registratie van gebeurtenissen

Op de servers en besturingssystemen vinden automatische en handmatige activiteiten plaats. Vanuit beveiligingsoptiek is het van belang om deze activiteiten te registreren in logboeken en te controleren.

C.04		**Registratie van gebeurtenissen**	ISO27002: 12.4.1
Control		Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	
Conformiteitsindicatoren en Maatregelen			
log-bestanden	01	Logbestanden van gebeurtenissen bevatten, voor zover relevant: a. gebruikersidentificaties; b. systeemactiviteiten; c. data, tijdstippen en details van belangrijke gebeurtenissen zoals de registratie van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem en tot bronnen van informatie; d. identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie; e. systeemconfiguratieveranderingen; f. gebruik van speciale bevoegdheden; g. alarmen die worden afgegeven door het toegangsbeveiligingssysteem; h. activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen; i. verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.	ISO27002: 12.4.1

C.05 Monitoring van servers en serverplatforms

Onder monitoren wordt verstaan: reviewen, analyseren en rapporteren. Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot servers en serverplatforms tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke

functionaris. Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd en te worden gerapporteerd (alerting). Alerting kan ook geautomatiseerd plaats vinden op basis van vastgestelde overschrijding van drempelwaarden.

C.05		**Monitoren van servers en serverplatforms**	NIST: AU-6
Control		De organisatie *reviewt/analyseert* regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten aan servers en besturingssystemen vast te stellen en bevindingen aan het management te *rapporteren*.	
Conformiteitsindicatoren en Maatregelen			
reviewt/ analyseert	*1.*	De verantwoordelijke functionaris analyseert periodiek: • de gelogde gebruikers-, activiteiten gegevens ten aanzien van servers en serverplatforms; • het optreden van verdachte[2] gebeurtenissen en mogelijke schendingen van de beveiligingseisen; • eventuele ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.	ISO27002: 10.10.1
	2.	De verzamelde log-informatie wordt in samenhang geanalyseerd.	ISO27002: 10.10.1
	3.	Periodiek worden de geanalyseerde en beoordeelde gelogde (gesignaleerde) gegevens aan de systeemeigenaren en/of aan het management gerapporteerd.	ISO27002: 10.10.1
	4.	De rapportages uit de beheerdisciplines compliancy-management, vulnerability-assessment, penetratietest en logging en monitoring worden op aanwezigheid van structurele risico's geanalyseerd en geëvalueerd.	ISO27002: 10.10.1
rapportage	*5.*	De analyse rapportage bevat informatie over kwetsbaarheden, zwakheden en misbruik en wordt gecommuniceerd met verantwoordelijk management.	ISO27002: 10.10.1
	6.	De eindrapportage bevat, op basis van analyses, verbeteringsvoorstellen gedaan.	ISO27002: 10.10.1

C.06 Beheerorganisatie servers en serverplatforms

Voor het adequaat beheersen en beheren van het servers en serverplatforms zou een beheersorganisatiestructuur moeten zijn vastgesteld waarin de verantwoordelijkheden voor de beheersprocessen met toereikende bevoegdheden zijn uitgedrukt en op het juiste niveau zijn gepositioneerd.

C.06	**Beheerorganisatie servers en serverplatforms**	
Control	Binnen de beheerorganisatie is een *beveiligingsfunctionaris* benoemd die de organisatie ondersteunt in de vorm van het bewaken van *beveiligingsbeleid* en die inzicht verschaft in de inrichting van de servers en het serverplatform.	
Conformiteitsindicatoren en Maatregelen		

[2] Verdachte gebeurtenissen zijn afwijkend en opmerkelijk gedrag ten aanzien gangbare patronen en geldende (beleids)regels.

beveiligings-functionaris	*1.*	De beveiligingsfunctionaris zorgt o.a. voor: a. de actualisatie van beveiligingsbeleid ten aanzien servers en besturingssystemen; b. de afstemming van het beveiligingsbeleid in de afgesloten overeenkomsten met o.a. de ketenpartijen; c. de evaluatie van de effectiviteit van de beveiliging van de ontwikkelde systemen; d. de evaluatie van de beveiligingsmaatregelen ten aanzien van de bestaande risico's; e. de bespreking van beveiligingsissues met ketenpartijen; f. het verschaffen van inzicht in de afhankelijkheden tussen servers binnen de infrastructuur.	
beveiligings-beleid	*2.*	Het beveiligingsbeleid geeft o.a. inzicht in: a. de inrichting-, het onderhoud- en het beheervoorschriften (procedureel en technisch); b. specifieke beveiligings- en architectuurvoorschriften; c. afhankelijkheden tussen servers binnen de infrastructuur.	

Bijlage 1: Definiëring/omschrijving van beveiligingsobjecten

Nr.	Relevante beveiligingsobjecten	Omschrijving
1	Beleid voor (beveiligd) onderhouden van serverplatformen	Het resultaat van een besluitvorming ten aanzien van onderhouden van serverplatform die de verantwoordelijke management voor Sever-platformen van een organisatie heeft vastgelegd op welke wijze serverplatforms onderhouden dienen te worden.
2	Principes serverplatform beveiliging	Principiële uitgangspunten voor het inrichten van serverplatforms, zoals: "Security by design" en "Defense in depth'.
3	Serverplatform Architectuur	Raamwerken of blauwdrukken waarmee wordt aangegeven op welke wijze serverplatforms zijn ingericht, samenhangen, beveiligd en beheerst.
U.01	Bedieningsprocedure	Een reeks verbonden taken of activiteiten die noodzakelijk zijn voor het beheren van serverplatforms.
U.02	Standaarden voor configuratie servers	Documenten waarin afspraken zijn vastgelegd ten aanzien van configuraties en parametrisering serverinstellingen.
U.03	Malwareprotectie	Beschermingsmechanismen om servers te beschermen tegen schadelijke code en om schadelijke code te detecteren en te neutraliseren.
U.04	Beheer van serverkwetsbaarheden	Proactieve beveiliging van servers door het verwerven van inzicht in de kwetsbaarheden en zwakheden in de software die op de server zijn geïnstalleerd.
U.05	Patch-management	Het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem.
U.06	Beheer op afstand	Het beheer van server door beheerders vanuit een niet-vertrouwde omgeving.
U.07	Onderhoud apparatuur	Het actualiseren van configuraties van een servers-platform binnen een tijdsinterval.
U.08	Veilig verwijderen of hergebruiken van apparatuur	Het opschonen van apparatuur en het veilig stellen van data op de apparatuur.
U.09	Hardenen van servers	Het proces van het uitschakelen of verwijderen van overbodige en/of niet gebruikte functies, services en accounts, waarmee de beveiliging wordt verbeterd.
U.10	Serverconfiguratie	Het configureren van verschillende features van een serverplatforms
U.11	Virtueel Serverplatform	Het beschikbaar stellen van één of meer gescheiden 'logische' omgevingen op één fysieke server.
U.12	Beperking software installatie	Het stellen regels voor het installeren van serverplatforms.
U.13	Kloksynchronisatie	Het gelijkrichten van klokken op verschillende servers.
U.14	Ontwerp documentatie	Een document waarin de relatie tussen servers en de instellingen van configuraties zijn vastgelegd.
C.01	Evaluatie richtlijnen servers en serverplatforms	Richtlijnen die evaluatie activiteiten van servers ondersteunen.
C.02	Beoordeling technische serveromgeving	Het proces van evalueren van de serveromgeving.
C.03	Logbestanden beheerders	Het vastleggen van activiteiten van beheerders.
C.04	Registratie gebeurtenissen	Het proces van registreren van gebeurtenissen op een server vanuit beveiligingsoptiek.
C.05	Monitoren servers en serverplatforms	Het proces van bewaken, reviewen, analyseren van vastgelegde gebeurtenissen en het rapporteren hierover.
C.06	Beheerorganisatie servers en	Een organisatorische eenheid die verantwoordelijk is voor

	serverplatforms	de beheersing van de serverplatform omgeving en die adequaat is gepositioneerd.

Bijlage 2: Referenties

Nr.	Normenkader	Versie
1.	NORA Beveiliging	2014
2.	ISO/IEC 27001/27002	2013
3.	Baseline Informatiebeveiliging Rijksoverheid	2017
4.	National Institute of Standards and Technology Information Security	2006
5.	NCSC Webapplicaties	2018
6.	The Standard of Good Practice for Information Security	2011
7.	The Standard of Good Practice for Information Security	2016