Grip op SSD

Veilige software door marktbrede samenwerking

Ad Kint en Marcel Koers

30 april 2015

Agenda

- “CIP”
- Aanleiding
- Grip op SSD:
  - De methode
  - De normen
- Grip op SSD een open standaard

CIP: Centrum voor Informatiebeveiliging en Privacybescherming

Speerpunt
Compacte overheid

Aanleiding voor de overheid:

- Toenemende afhankelijkheid van het internet, mobile devices,ed.
- Toenemende (organisatiegraad van) cyber crime

De overheid organiseert zich en CIP faciliteert dit door

- Werken aan gezamenlijke afspraken en normatiek
- Aanbieden/toegankelijk maken van kennis en practices
- Het bouwen aan een IB-community in de overheid

Netwerkorganisatie: Overheid

CIP centrum informatiebeveiliging en privacybescherming

Agentschap NL
Ministerie van Economische Zaken, Landbouw en Innovatie

Auditdienst Rijk
Ministerie van Financiën

Basisadministratie Persoonsgegevens en Reisdocumenten
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Immigratie- en Naturalisatiedienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Belastingdienst

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Rijksoverheid

Ministerie van Defensie

Gemeente Groningen

Gemeente Utrecht

KING Kwaliteits Instituut Nederlandse Gemeenten

Gemeente Den Haag

Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid

Centraal Justitieel Incassobureau
Ministerie van Veiligheid en Justitie

Gemeente Amsterdam

provincie groningen

VNG Vereniging van Nederlandse Gemeenten

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

OPENBAAR MINISTERIE

Gemeente Rotterdam

Stichting Inlichtingenbureau

BKWI Bureau Keteninformatisering Werk & Inkomen

ip Interprovinciaal Overleg

College Bescherming Persoonsgegevens

SVB

HetWaterschapshuis

CVZ

ciz

UMC Universitair Medisch Centrum Utrecht

ccMO

Platform voor Cybersecurity CPNI.NL

uwv

CAK

RDW

kadaster

vts Politie Nederland

Netwerkorganisatie: Bedrijfsleven

- Leveranciers vragen op een UWV om heldere specificaties

Aanleiding: Ons streven

- De overheid als professionele opdrachtgever
  - De overheid maakt zijn verwachtingen duidelijk ten aanzien van software
  - Leveranciers kunnen hun verantwoording nemen
  - Heldere eisen voor een heldere governance (ook intern)
- Dat overheidsbreed:
  - Geen zwakke schakels
  - Eén overheid

Aanleiding: Oorzaken onveilige software

- Beveiligingseisen zijn onduidelijk en niet op maat
  - Opdrachtgever verwacht deskundigheid
  - Leverancier verwacht precieze specificaties
- Er wordt niet of laat getoetst
- Opdrachtgever heeft te weinig risico-overzicht
- Bestaande standaarden bieden te weinig houvast
  - Lange lijsten met technische en organisatorische maatregelen
  - Vooral toegesneden op het *hoe*, niet het *wat*

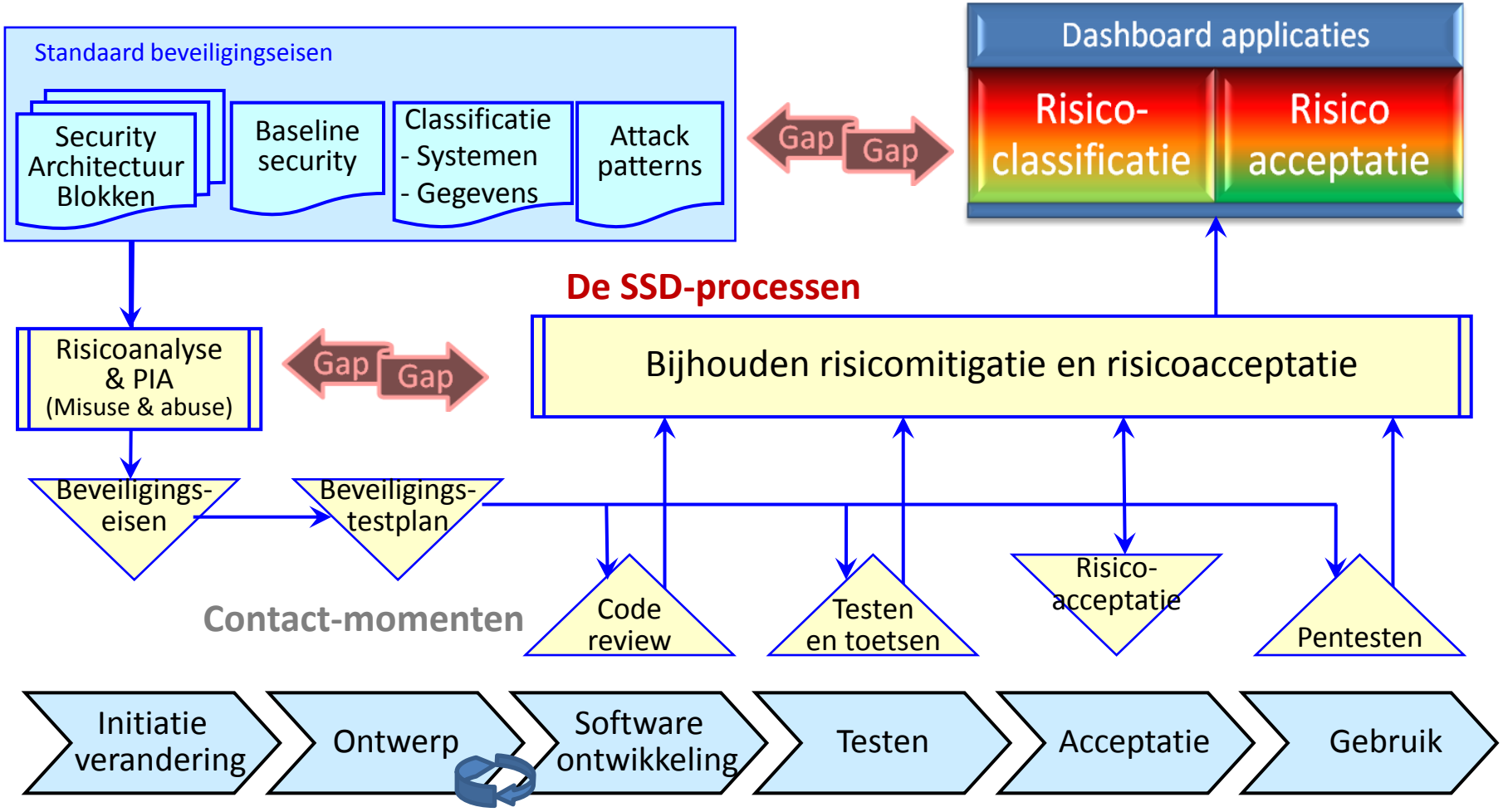
Aanleiding Grip op SSD:

"Een andere wijze van controle en sturing leidt tot een proactieve houding bij opdrachtgever en leverancier."

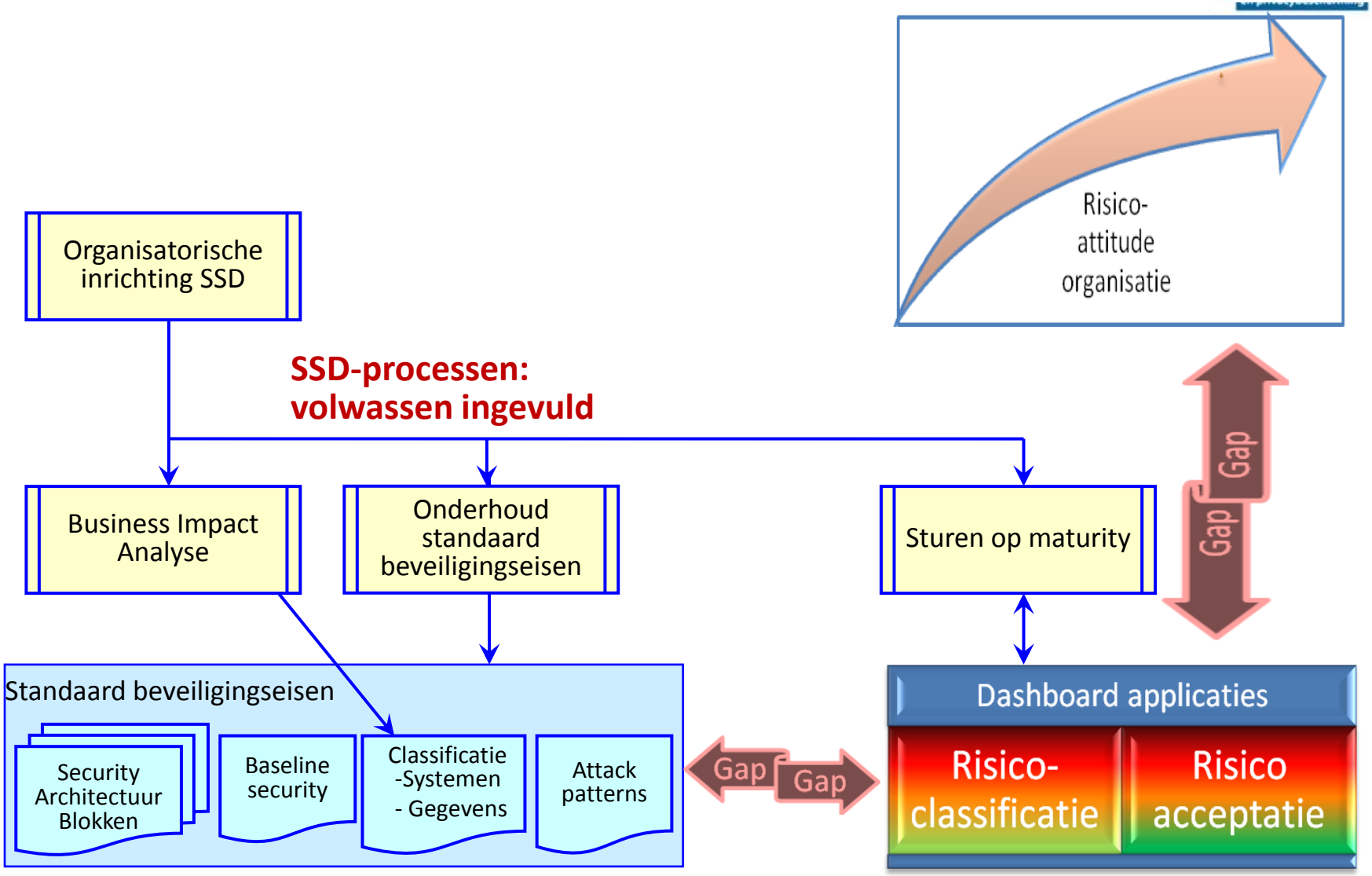
- Geeft de opdrachtgever handvat om te sturen op de veiligheid van software
- Leveranciersonafhankelijk:
  - ✓ Geen eisen die ingrijpen op het HOE bij de leverancier
  - ✓ Inzetbaar bij meerdere verschillende interne of externe leveranciers
- Toepasbaar bij alle ontwikkelmethodieken (waterval, agile) of wel of niet via een scrum aanpak.
- Geschikt voor maatwerk èn standaard pakketten
- Brede acceptatie door softwareleveranciers, ook in de pers

Samen werken aan veiligheid	
Traditionele aanpak	Prestatiegerichte aanpak
Controle op de (beveiligings-) processen.	Controle over de (beveiligings-)kwaliteit van de dienst.
Gebruik van indirecte (proces-) informatie.	Gebruik van geaggregeerde informatie (KPI's) over de (beveiligings-)kwaliteit.
De aanbieder wordt als expert gezien, die door een derde partij op zijn invulling wordt beoordeeld.	Opdrachtgever en leverancier bundelen hun expertise.
Denken vanuit het 'wij en zij', doordat beiden werken vanuit eigen verwachtingen	Denken vanuit het 'samen', doordat beiden uitgaan van dezelfde prestatie-indicatoren, waarbij de leverancier vrij is in hoe de dienst wordt vormgegeven.
Streven naar het verplaatsen van de risicoverantwoordelijkheid.	Daadwerkelijk minimaliseren van risico's.

De methode:
In contact en in control komen



De methode: Governance



SSD Dashboard

ja	Voldoet aan de eis.
nee	Voldoet niet aan de eis.
nvt	De eis is voor de applicatie niet van toepassing
deels	Afspraken gemaakt met applicatie-eigenaar over de afwijking
	Nog geen constatering

Test Line	Applicatie complex	Datum laatste wijziging	SSD versie	Applicatie	SD-4B	SD-5	SD-6	SD-7	SD-8	SD-9	SD-10	SD-11	SD-12A	SD-12B	SD-13	SI 1
		28-jan-14	1.85			nvt	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt	
		17-okt-13	1.85			nvt	ja	ja		nee	ja	ja	ja	ja	nee	
		27-mrt-14	1.85			nvt	ja	ja		nee	ja	nee	nee	nee	nee	
		4-nov-13	1.85			nvt	nee	ja		ja	ja	ja	ja	ja	ja	
		11-nov-13	1.85			nvt	nee	ja		nee	ja	nvt	nee	nee	nee	
		11-nov-13	1.85			nvt	ja	ja		ja	nee	nee	nee	nee	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	nee	ja		nvt	nvt	nvt	ja	ja	ja	
		4-nov-13	1.85			nvt	nee	ja		ja	ja	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	

Groeien naar volwassenheid

Nog niet

		SSD-processen				
5	rd	dezelfde prestatie-indicatoren leveranciers	dezelfde tooling en prestatie-indicatoren leveranciers	dezelfde tooling en prestatie-indicatoren leveranciers	pentest na meldi beveiligings	
4		e aanpak erlinge ijki	hogere voorspelbaarheid met kortcyclische	onderdeel acceptatie		
3		rd v riti me		diek skr ster		
2		fsg		nte skr ystem		
1		kopie baseline beveiligingseisen	op ad-hoc basis	op ad-hoc basis	slechts na beveiligingsincidenten	acceptatie zonder vervolgafspraken met applicatie-eigenaar
CMM-niveau		Beveiligingseisen	Code review	Testen en toetsen	Pentesten	Risicoacceptatie

Security by design

7. Meenemen context:
- BIA en IB risico-analyse
- Security architectuur

5. Feedback leveranciers:
- Eerst als bijlage op versie in de contracten.

- Uitleg methode aan de IM's
- Contract leveranciers

4. Vergroten bewustzijn:
- Campagneleider
- Voorbeeld publiceren

- Uitleg van de methode
- Uitleg van de baseline

8. Rapp ges op de afwijkingen (Rood/Groen)

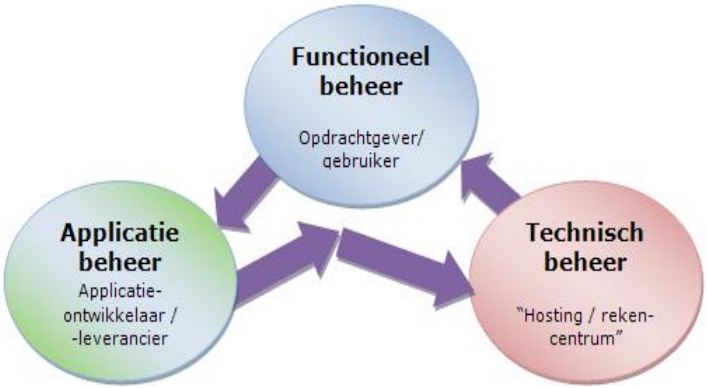
6. Formele acceptatie gedoogsituatie

- Inventarisatie hanteren baseline

SSD: De normen

De veiligheid en de weg ernaar toe zijn inzichtelijk gemaakt

- Gebaseerd op:
  - Risico's voor de bedrijfsvoering
  - NCSC richtlijnen
  - OWASP



- Duidelijkheid over:
  wie moet **wat** doen

- Maakt governance mogelijk:
  - Normen beperkt in omvang
  - Hanteerbaar als auditnorm (SIVA)
  - Ook in het Engels beschikbaar

- Eenvoudig uitbreidbaar: Practitionersgroep

Eisen van de opdrachtgever?

Verify that, if applicable, any personal account numbers are truncated prior to storing on the device.

Verify that any exposed intents, content providers and broadcast receivers perform full data validation on input

Verify that the application makes use of Address Space Layout Randomization (ASLR).

Opzet SSD-normenkader

- SIVAstijl:
  - Concrete, uitvoerbare, en hanteerbare normen;
  - Wie doet wat en waarom en wat is het risico als dit niet gedaan wordt
  - Meenemen van de opdrachtgever in de uitleg

Onderwerp van de norm	
Criterium (wie en wat)	Wat (xxxxxx) <werkwoord> xxxxx trefwoorden xxxxx
Doelstelling (waarom)	De reden waarom de norm gehanteerd wordt.
Risico	Het risico dat de aanleiding vormt om de norm te hanteren.

Onderwerp van de norm	
	indicatoren
/01	trefwoord
/01.01	indicator 1.1
/01.01	indicator 1.2
…	…

Toelichting….

Een succesvolle invoering van de methode Grip op SSD

Iedereen weet wat van hem of haar wordt verwacht.

- ✓ Start bij de leveranciers/contracten
- ✓ Begin met een minimum baseline…. en start met het dashboard.

Comply or explain

PIA

WBP

- ✓ Stel de beveiligingsrisicoanalyse verplicht voor alle IV-projecten
- ✓ Baselines en risicoanalyses maken is een vak:
  - ✓ Organiseer kennis

CIP netwerk

- ✓ Zet de methode niet om in een groot implementatieplan

Grip op Beveiliging in inkoopcontracten

Privacy
Informatiebeveiliging

Klassieke aanpak leidt steeds tot onveilige oplossingen en ontevredenheid

Het roer moet om naar een prestatiegericht aanpak !

- Betere sturing
  - Aanspreken op geleverde prestatie
    - Vraagt om afstemming vooraf
    - Delen van informatie en kennis
  - Weerbaarheid van het stelsel vergroot
  - Aandacht voor clouds, SSD, privacyregelgeving, …
- Volgt het bedrijfsbeleid:
  - Opgezet als cafetariamodel
- De prestatiegerichte aanpak zet de beveiligingsorganisatie in positie

SSD Practitionersgroep

Samenwerken
àls dè basis voor
veilige software

Ambitie:

- Betere beveiliging bij overheid en bedrijfsleven door het op grote schaal gebruiken van SSD bij zowel opdrachtgevers als leveranciers

Gemeenschappelijk belang:

- (Overheids-) organisaties delen dezelfde leveranciers
- Gebruik van standaard normen vereenvoudigen het gebruik (SSD-normen)
- Dezelfde wijze van samenwerking (SSD-methode):
  - Optimale en effectieve samenwerking
  - Lagere kosten

Practitionersgroep: Community binnen CIP, met:

- Opdrachtgevers die SSD implementeren of dat van plan zijn
- Leveranciers die SSD opnemen in hun aanbod of dat van plan zijn

Met als doel:

- Het verbeteren van de beveiliging door samenwerking tussen opdrachtgevers en leveranciers
- Het delen van ervaringen, om elkaar te helpen
- De methode en de normen te verbeteren met lessons learned

SSD als norm voor veilige software, dan wel voorschrijft, voor de overheid, omdat:

- SSD is een unieke enabler voor een inhoudelijke professionele samenwerking; intern èn met de leveranciers
- SSD is een uniek toepassingskader:
  - Bewezen praktijk
  - Implementatie is laagdrempelig
  - Aanvulling door SIVA notatie en wie doet wat in de keten.
- Hogere volwassenheidsniveau's haalbaar en meetbaar
- Duurzame doorontwikkeling is geborgd bij het CIP dmv communities, maar ook door aansluiting van partijen met verificatie modellen, zoals OWASP, Enisa, NCSC.
- SSD geeft invulling aan 4 van de slimme "boerenregels" van de commissie Elias
- SSD geeft invulling aan 20 normen van de BIR
- Convergentie naar 1 standaard voor veilige softwareontwikkeling binnen de overheid is mogelijk.
- Door toepassing van SSD als standaard binnen de overheid efficiency voordelen voor auditors, interne en externe leveranciers en aansturende organisaties.

Grip op SSD: Een open community

- Downloads: www.GripOpSSD.org
  - SSD-Methode
  - SSD-normen
  - SSD-training
  - Beveiliging in inkoopcontracten

AVAILABLE FOR FREE

Wij delen de kennis om tot veilige software te komen

...

... en door deze te verrijken zijn we klaar voor cybersecurity

CIP kontakt Ad Kint, ad.kint@uwv.nl

tel. 06-52464200

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Volksgezondheid, Welzijn en Sport

Ministerie van Financiën

Dienst ICT Uitvoering
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Agentschap NL
Ministerie van Economische Zaken, Landbouw en Innovatie

Belastingdienst

SNS REAAL

uwv

IBM

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

DKTP Informatie technologie

SIG Software Improvement Group

ORDINA CONSULTING | ICT | OUTSOURCING

SOGETI

SVB

Justitie

VALORI

CGI