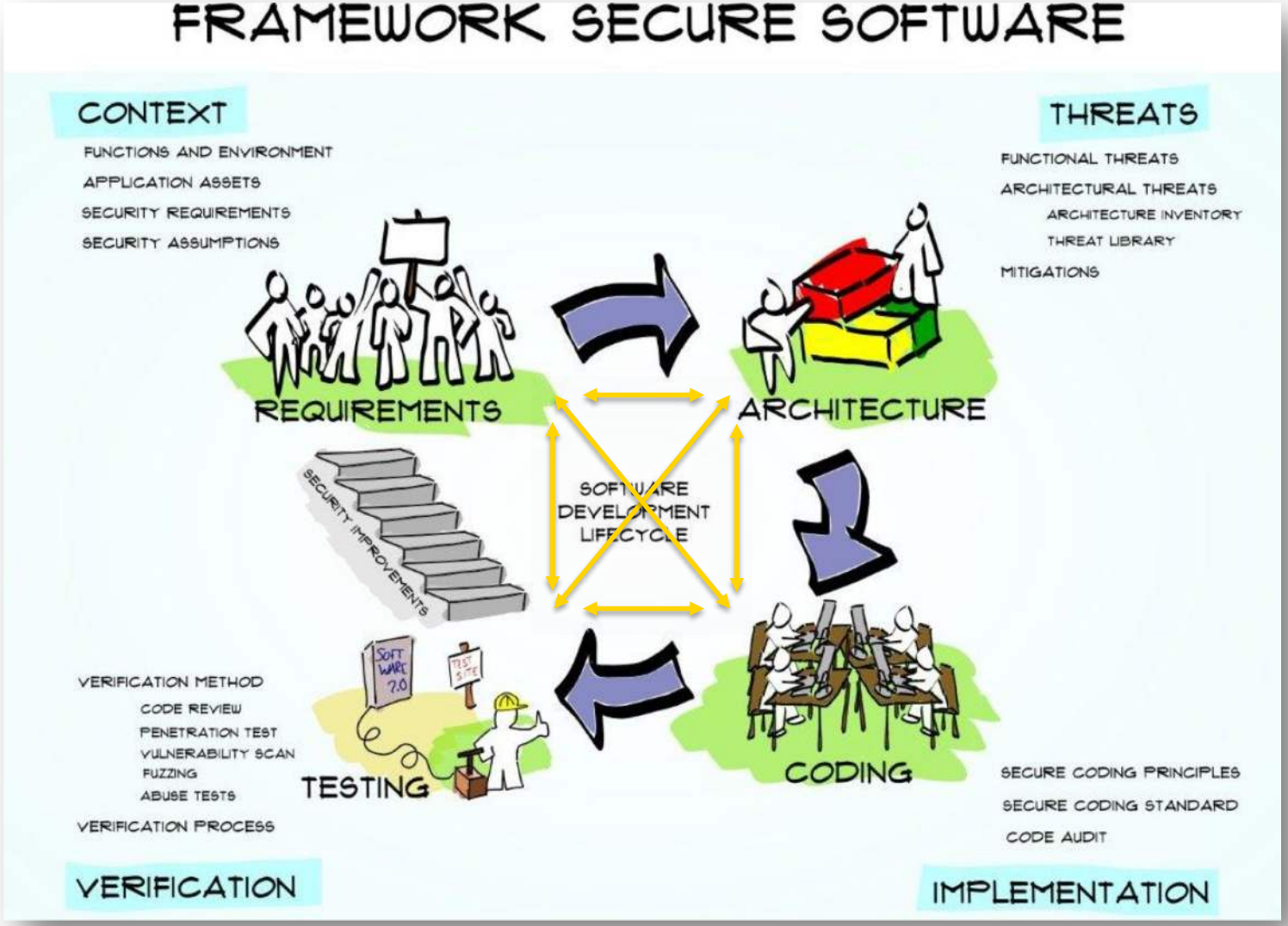
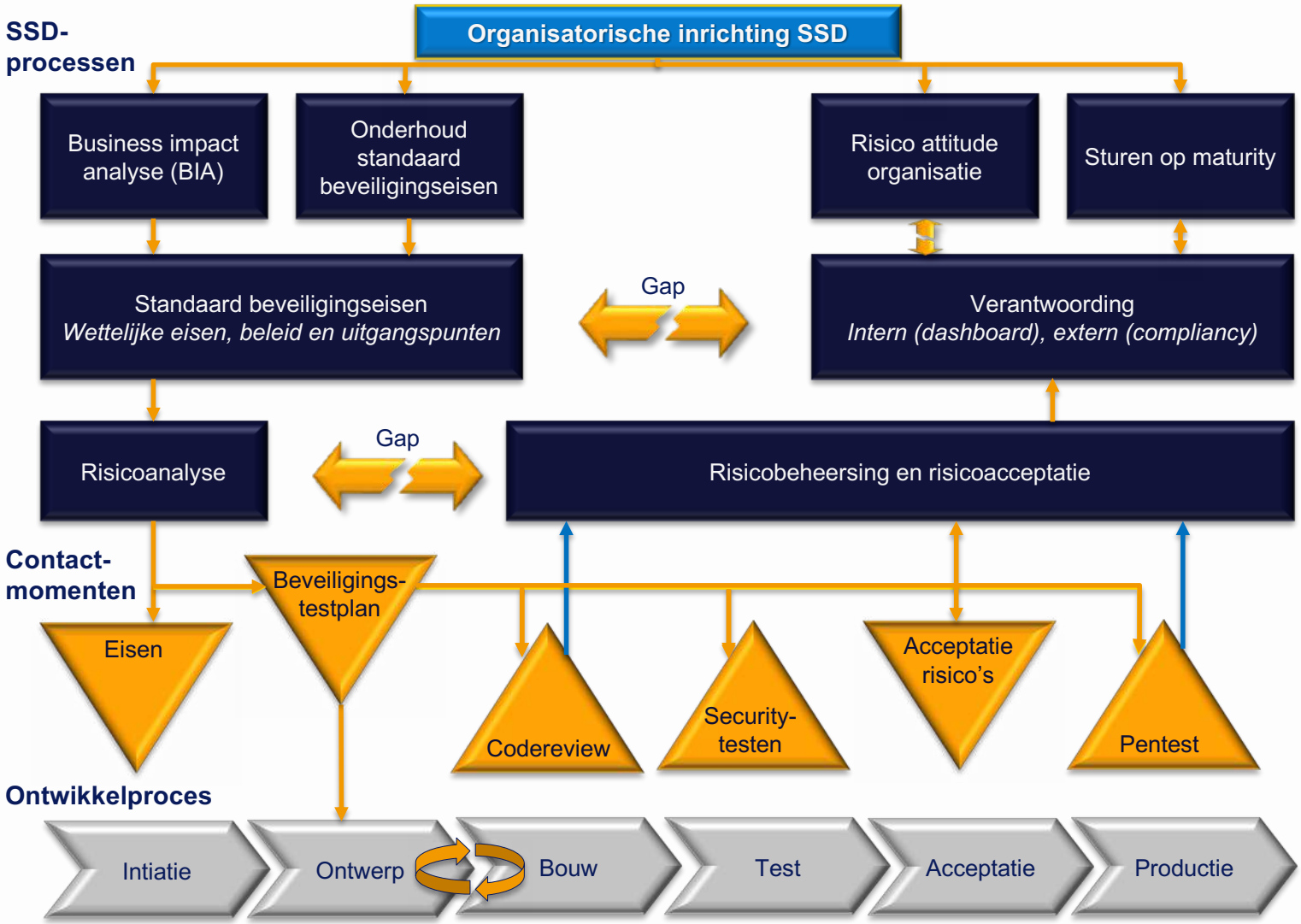
Secure Software Alliance



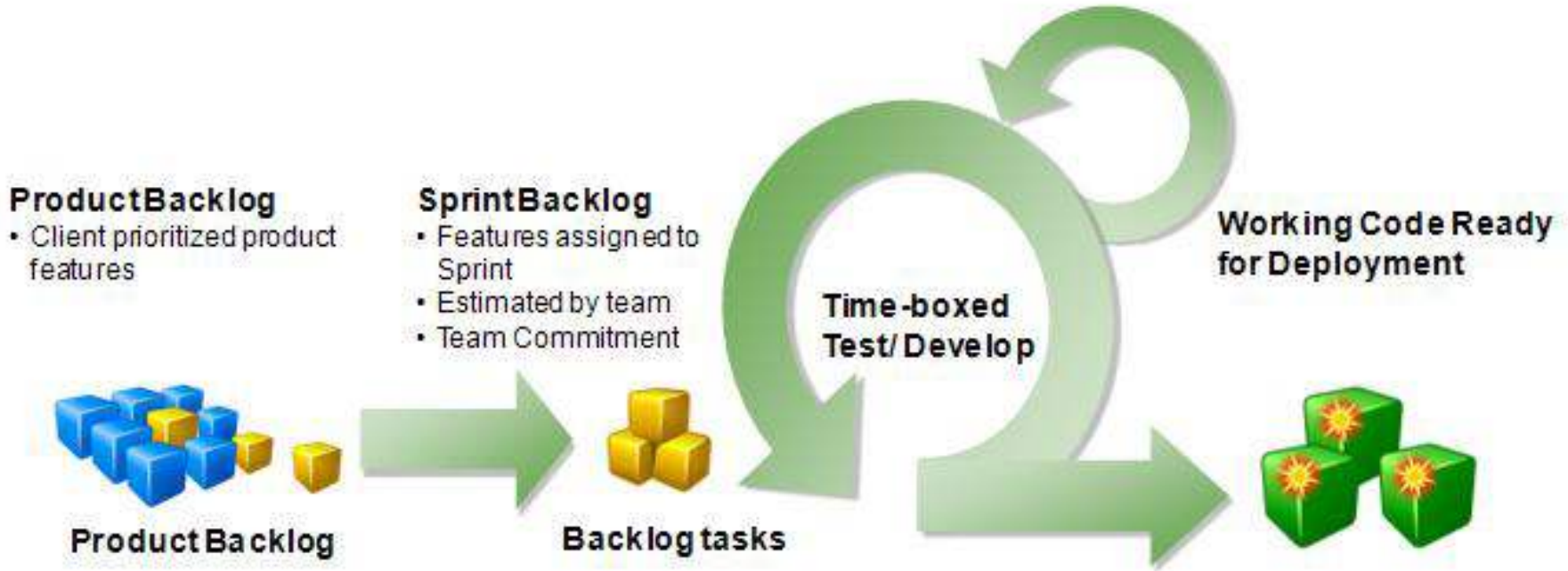
SSD model

centrum informatiebeveiliging en privacybescherming




Uitdaging:
Scrum
SDLC

Scrum in een notendop



Sprint Planning Meeting
- Review Product Backlog
- Estimate Sprint Backlog
- Commit

Daily Scrum Meetings
- Done since last meeting
- Plan for today
- Roadblocks/Accelerators?

Sprint Review Meeting
- Demo features to all
- Retrospective on the Sprint Adjustments

Time-boxed "Sprint" Cycles

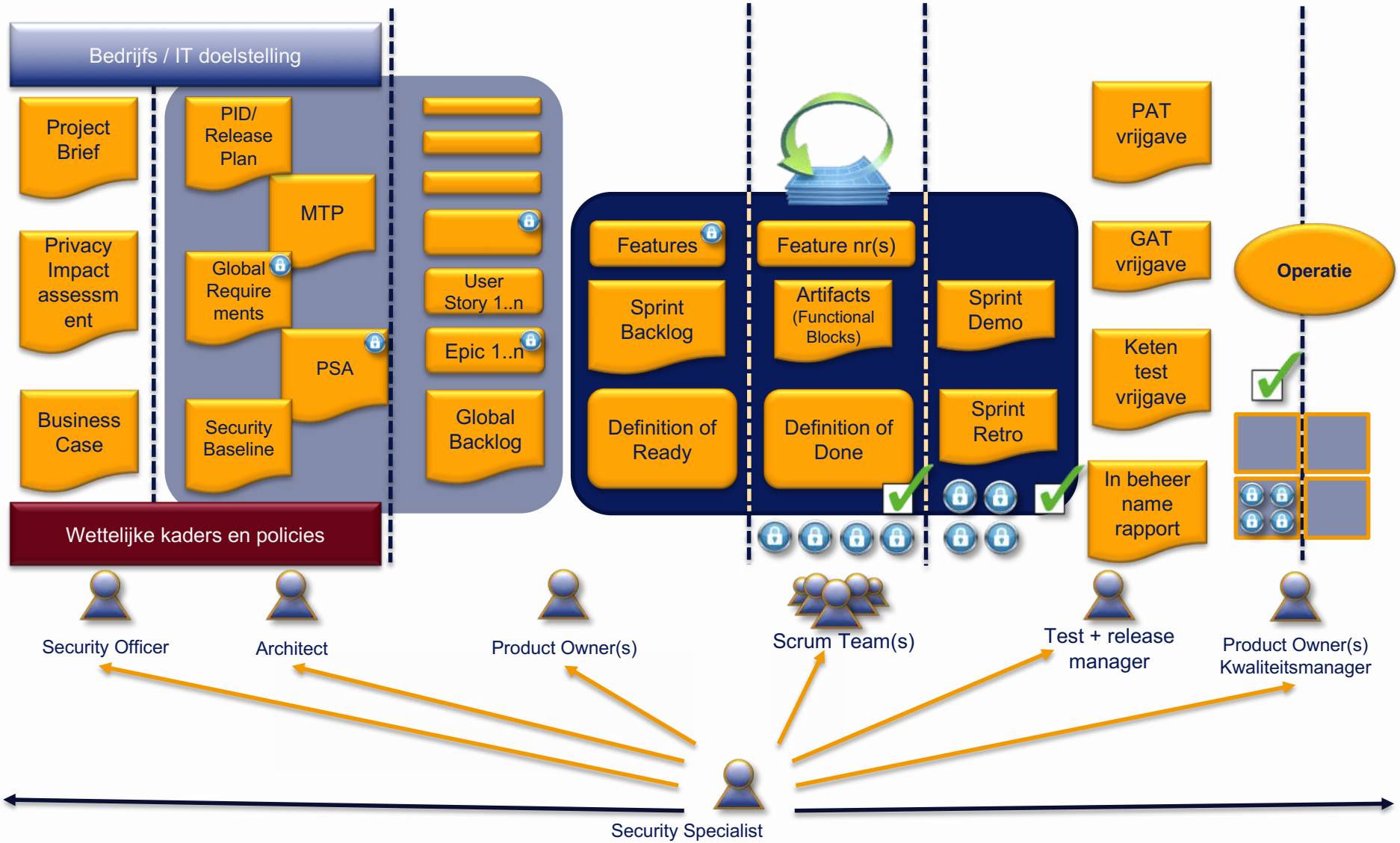
Bring Security to Scrum

Van Waterval naar Agile

How is Secure Agile Development Different?

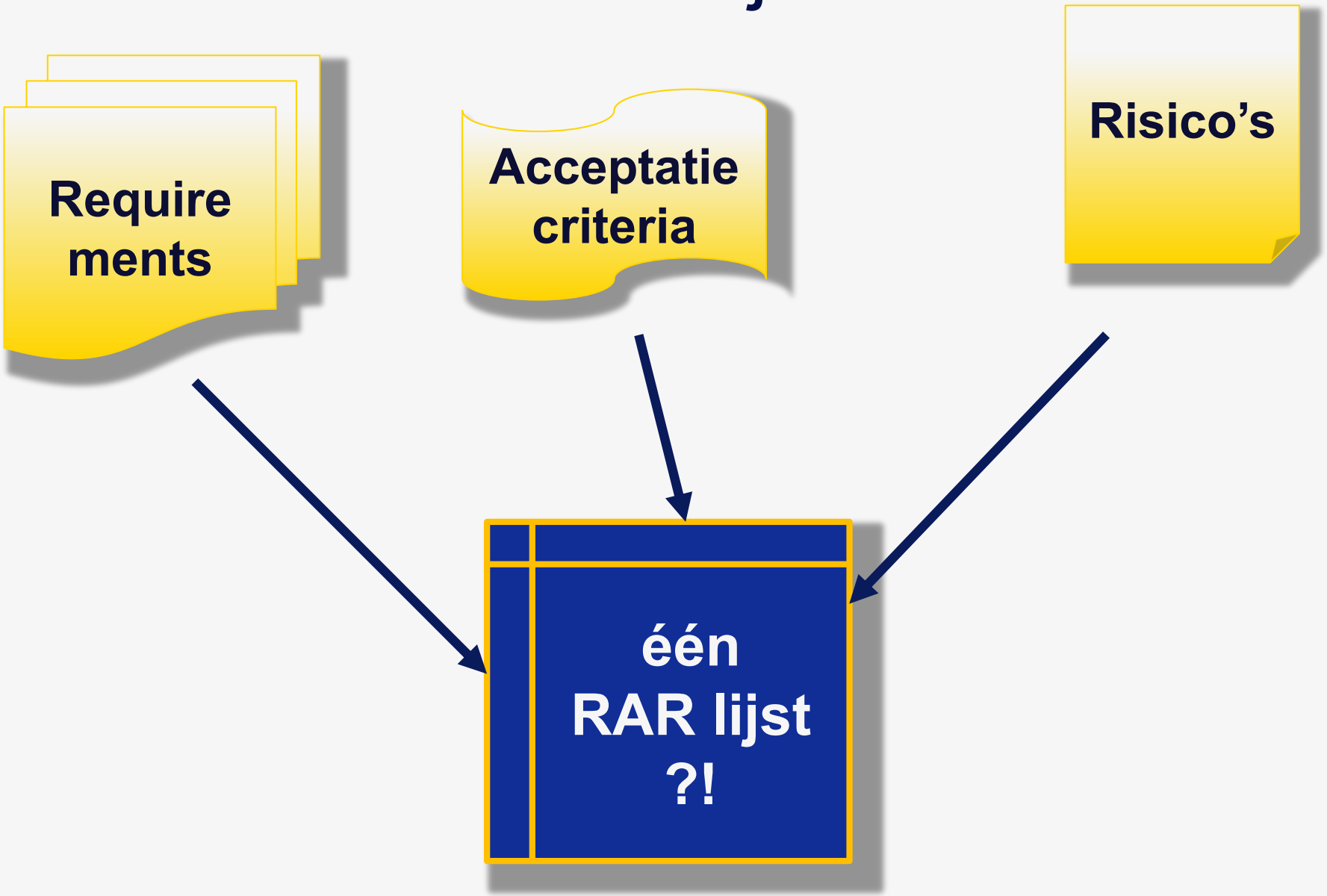
Traditional / Waterfall		Agile
• Distinct security-focused project phases, often at beginning and end of project	Security Timing	• Every iteration considers security, but is not limited by it.
• Security skills brought in from outside project, often disconnected from dev/test resources	Security Resources	• Every team member is responsible for security. Security skills are embedded in the team.
• Specific security testing phase, often at end of project.	Security Validation	• Hybrid security and functionality testing, throughout project.

Agile Application Security Testing



Security risico’s

Gebruik een RAR lijst



Wat heb je hieraan?

Expliciet en controleerbaar risicomanagement

- In een Scrum setting mogelijk

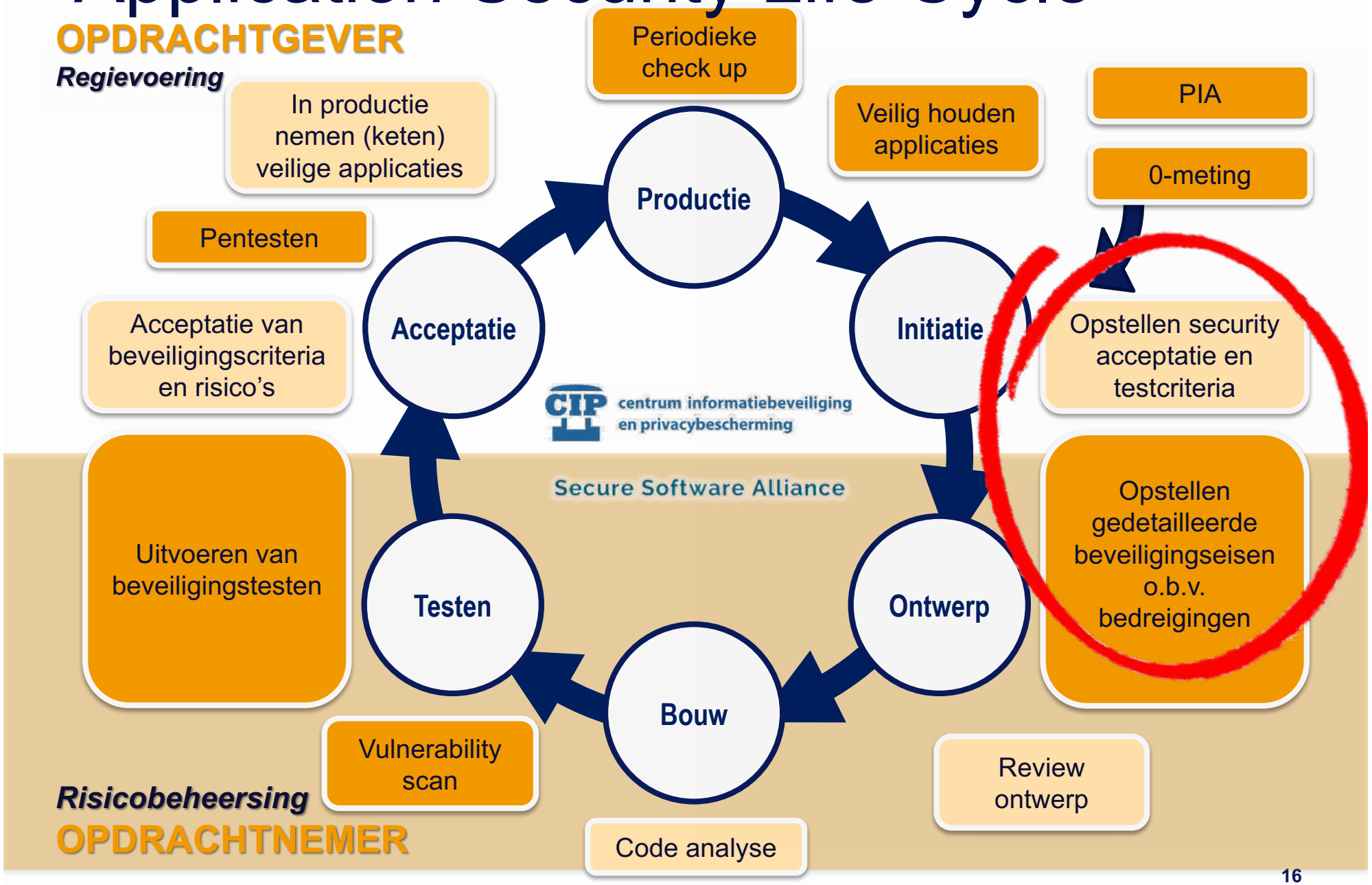
Met borging van elk risicotype

- Elk risico is te mappen

Zonder Scrum te frustreren

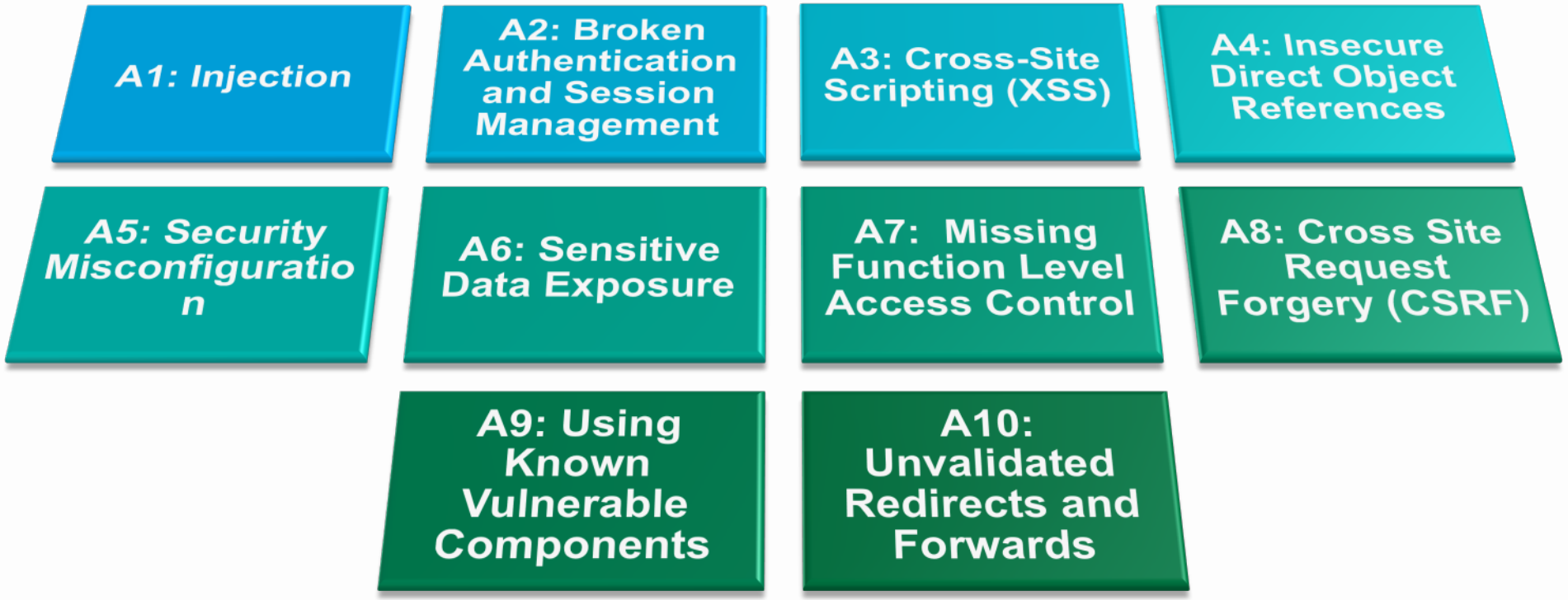
- Weinig extra’s toevoegen

Application Security Life Cycle



Application Security Life Cycle

OWASP top 10 (2013)



Security by design

Ontwikkelteam	Penetratietest
In alle fasen van de software levenscyclus	Net voor of na in productiename
Test: Aantonen defect / vulnerability	Vinden en diepgaand onderzoeken van een vulnerability (forensics)
Ontwikkelteam	Ethical hacker (extern)
Belangrijke kwetsbaarheden en/of bedreigingen	Verdieping en onderzoek naar specialistische aanvallen
Onderdeel application life cycle en vrijgaveadvies	Separaat rapport

Securitytest en penetratietest vervangen elkaar dus niet;

> het vult elkaar aan <

Mogelijkheden securitytesten

Mogelijk uit te voeren securitytesten:

- Authenticatie en autorisatie
- (SQL) Injectie
- Syntactisch / semantisch
- Parameters aanpassen
- Sessie overnemen
- HTTPS

Met reguliere tools

- Encryptie
- Sensitieve data
- Cross site scripting (XSS)
- Cross site request forgery
- Redirects

Tool, zoals *Burp Suite* nodig!

Groeipad

SSD Beveiligingseisen

Normalisatie en validatie van input

- **SSD-18:** Inregelen van HTTP validatie
- **SSD-19**: Normaliseren van invoer voor validatie
- **SSD-22:** Toepassen van invoervalidatie
- **SSD-20:** Controle op de codering van dynamische onderdelen
- **SSD-21:** Afdwingen van geparameteriseerde queries

Invoervalidatie

Naam Vul hier uw naam in

Naam 123456

Naam !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Naam !@#$%^&*()_:”<>?;’,./\|{}

Naam ÁáÉéÍíÓóÚúÄäËëÏïÖöÜüÀàÈèÌìÒòÙù

Naam aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Verdiepen vanuit invoervalidatie

Naam test

Naam <font size="6" color="#FF0000" face=“comic sans>rood</f

Naam klik hier

Naam SELECT naam FROM naam WHERE naam = ‘naam‘ AND

Checken invoervalidatie

- Op GUI zelf (respons)
- In bericht
- Middleware
- Back-end
- Logging
- Gekoppelde applicaties
- Database


```
<Name>Tim van Loon</Name>
<Phone>0612123123</Phone>
```

```
<Name><i>Pim van Loon</i></Name>
<Phone>!@#$%^&*(</Phone>
```

Oplossing

Zorgen dat slechts een naam mogelijk is via veld en services. Beperking tot alfabetisch, beperkt non alfanumeriek, (min en) max van X aantal karakters.

Afsluiting