Informatiebeveiliging & Privacy - by Design

Steven Debets

–

Verdonck, Klooster & Associates

VERDONCK KLOOSTER & ASSOCIATES

Even voorstellen

e steven.debets@vka.nl
m 0651588927

Informatiebeveiliging

Informatiebeveiliging– houdt zich bezig met het beschermen van uw bedrijfsinformatie, in termen van:

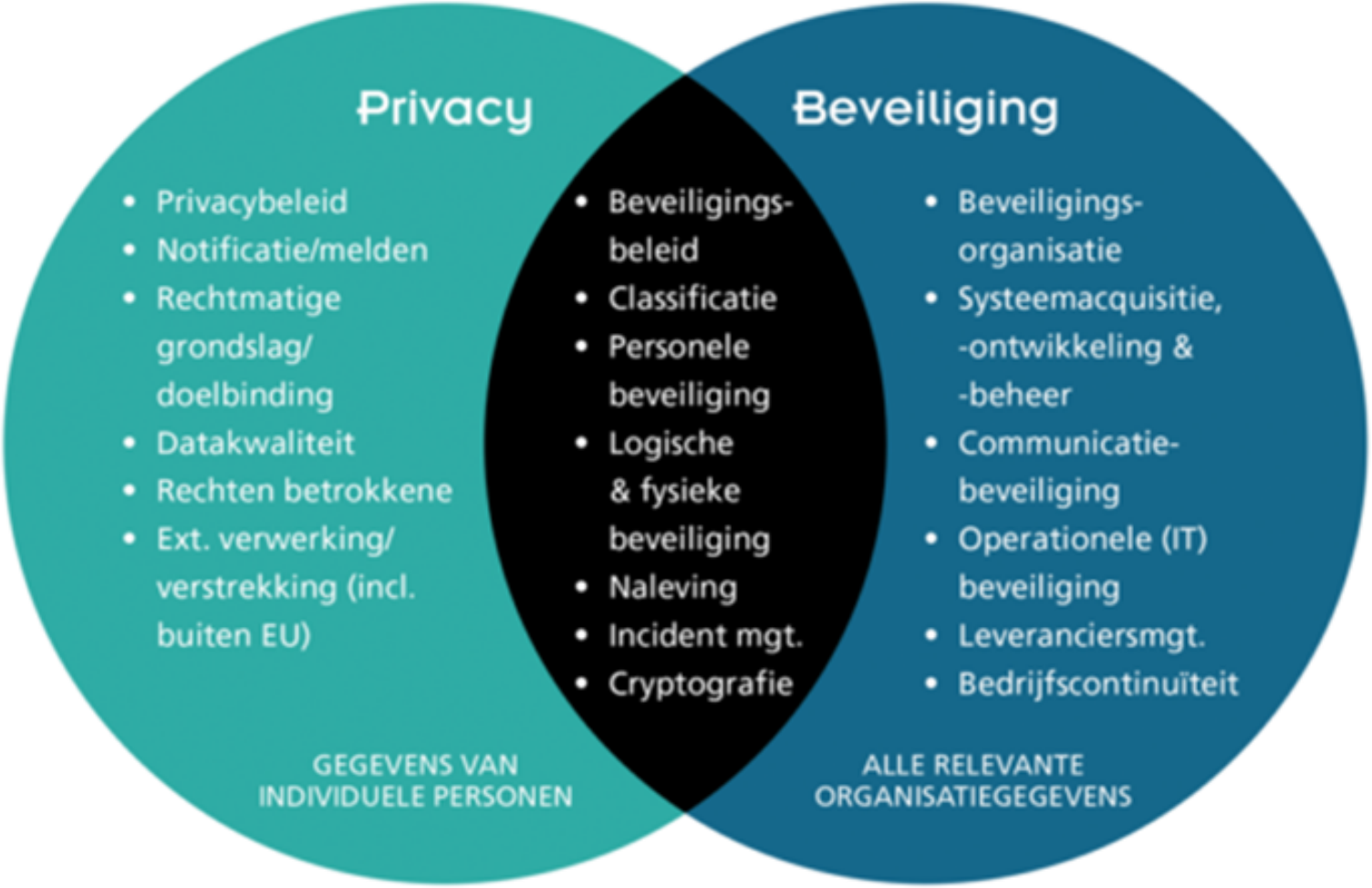
- **Beschikbaarheid** – Het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen
- **Integriteit** – Het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan.
- **Vertrouwelijkheid** – Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.

Privacy

Privacy beschermt de persoonlijke levenssfeer van mensen:

1. Dataminimalisatie (min=max)
2. Gegevenskwaliteit (geautomatiseerde controles)
3. Doelbinding en verenigbaarheid
4. Limitering van gebruik (ontvangst, opslag en verzenden)
5. Beveiliging van gegevens (encryptie en LTB)
6. Transparantie (beleid, certificering, gedragscode)
7. Rechten van betrokkenen (zeggenschap)
8. Verantwoording (controles)

… en wat hebben ze met elkaar te maken?



VERDONCK KLOOSTER & ASSOCIATES

De kern van informatiebeveiliging

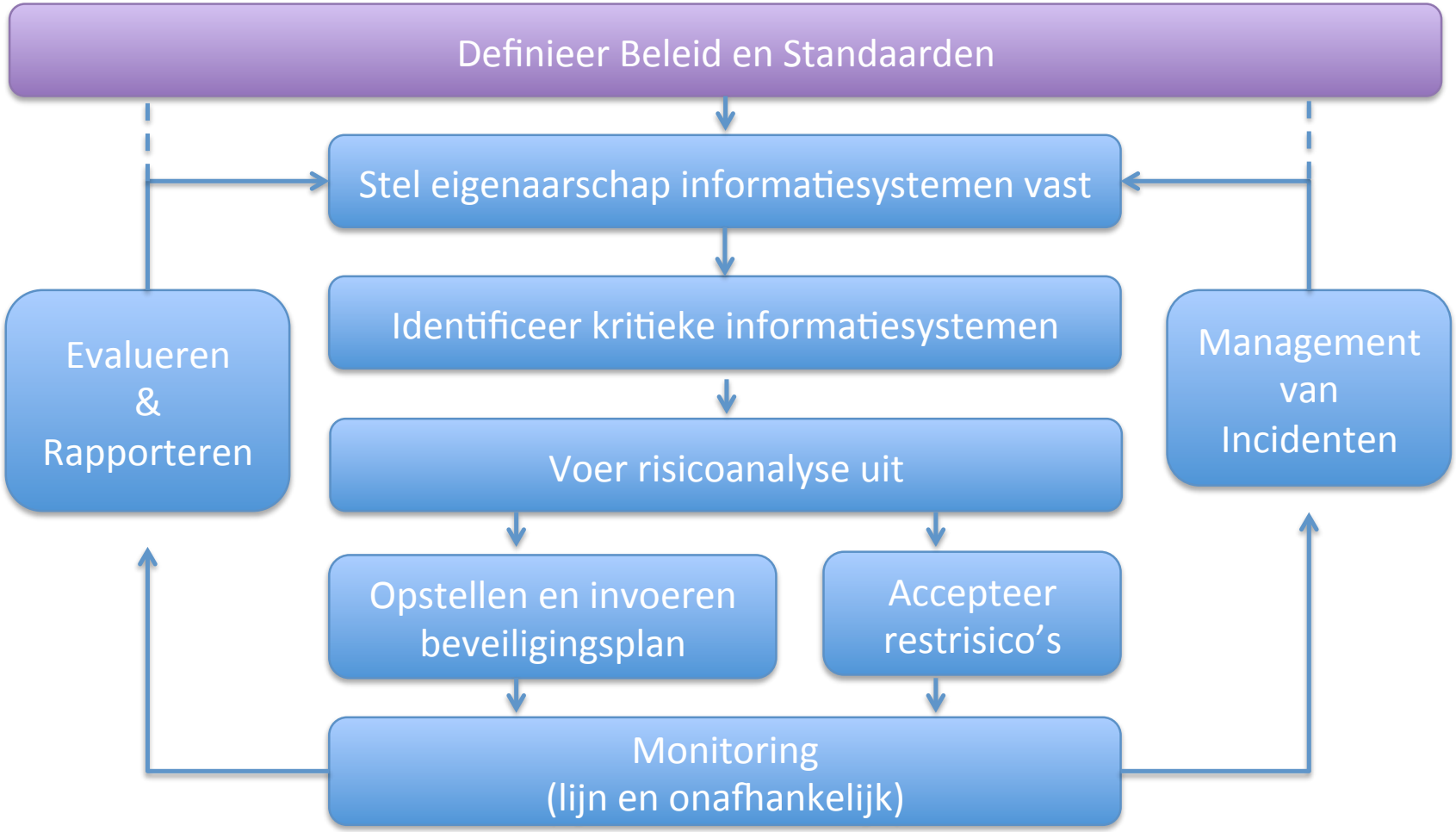
Informatiebeveiliging gaat in principe over het beantwoorden van drie eenvoudige vragen:

1. Wat zijn mijn meest waardevolle informatiemiddelen (applicaties of informatie)

2. Welke gebeurtenissen hebben een gerede kans mijn informatie schade toebrengen

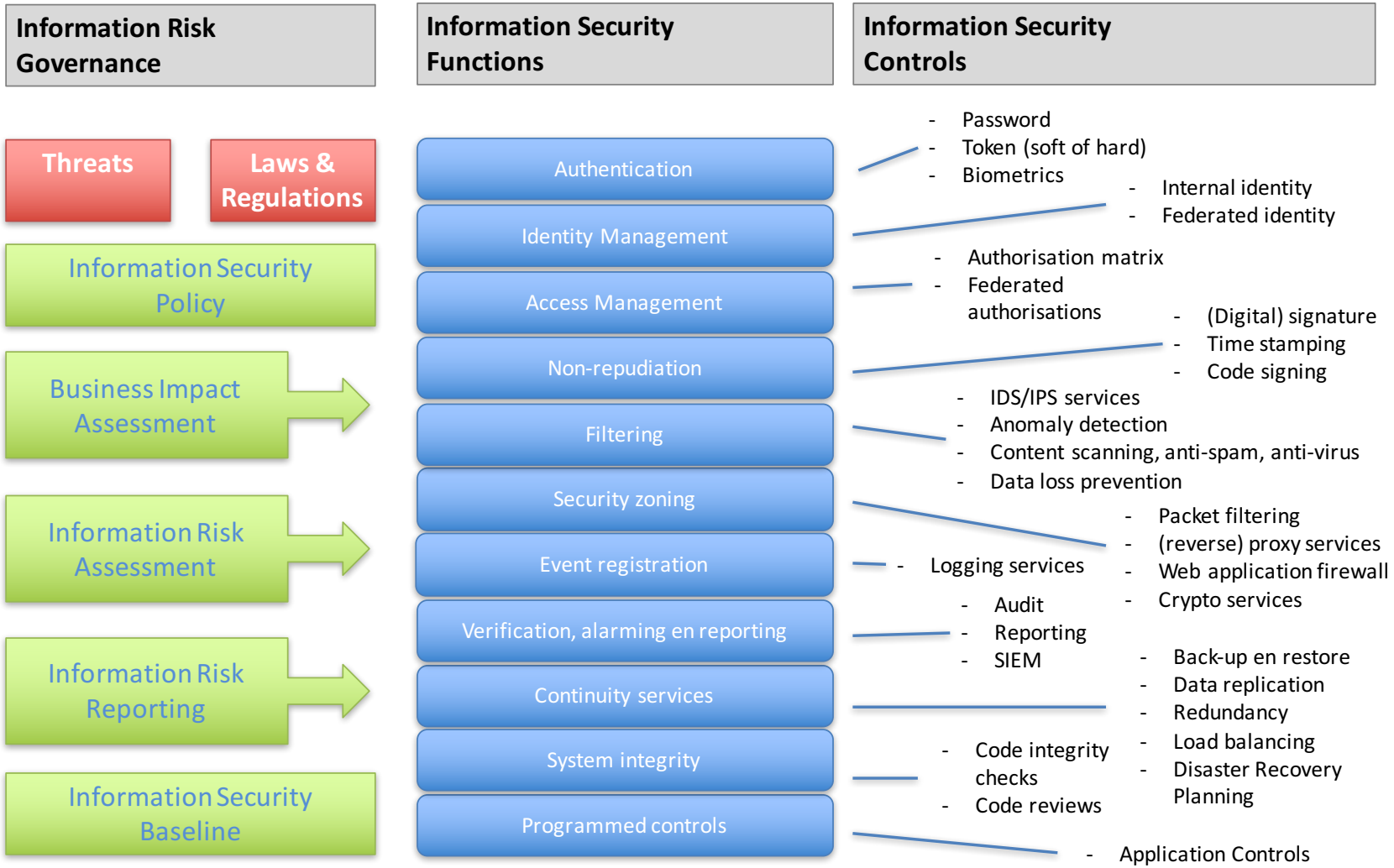
3. Hoe kan ik mijzelf beschermen tegen de meest waarschijnlijke gebeurtenissen

Informatiebeveiliging heeft een proces kant



VERDONCK KLOOSTER & ASSOCIATES

…. en een inhoudelijke kant



? Main question: Which **information security functions** do I need, based on policies, business impact, risk assessments and available reports.
The baseline defines the minimum requirements.

VERDONCK KLOOSTER & ASSOCIATES

And what about privacy?

25 mei 2018

TO DO:

- [ ] Rol van de Privacy Officer binnen uw organisatie (her)definiëren.
- [ ] Registeren waar binnen uw organisatie persoonsgegevens worden verwerkt.
- [ ] Verwerkingen door derden in kaart brengen (ook grensoverschrijdend).
- [ ] Concrete bewerkersovereenkomsten met derden afsluiten conform de nieuwe regelgeving.
- [ ] Datalekprotocol opstellen, periodiek reviewen en oefenen.
- [ ] Privacy Impact Assessments uitvoeren bij potentiële risicovolle verwerkingen.
- [ ] Privacy by Design / Default als standaard in de bedrijfsvoering en ICT invoeren.
- [ ] Processen inrichten voor de uitoefening van rechten van betrokkenen.
- [ ] Transparant, begrijpelijk en toegankelijk privacybeleid opstellen en uitdragen.

Model voor Privacy by Design

Verstandig gebruik

Verzamel alleen wat je nodig hebt
Gebruik gegevens alleen waarvoor je ze gevraagd hebt
Kies bij configuratie standaard de privacy vriendelijke variant
Let op kwaliteit van data
Maak geen onnodige kopieën
Gooi weg wat je niet langer nodig hebt

Passende bescherming

Sla gescheiden op
Beperk de toegang
Verwerk geaggregeerd
Pas versleuteling, pseudonimisering of anonimisering toe

Vragen ?

VERDONCK
KLOOSTER &
ASSOCIATES