# NEN 7510 & ziekenhuizen

Beer Franken, *Piasau*

Hans van Hemert, *Maasstad Ziekenhuis*

# Beer Franken

- VUmc, 7 jaar
- VWS, 10 jaar
- ZonMw, 7 jaar
- AMC, 8 jaar
- Consultant, 5 jaar (Z-cert, Wolters Kluwer, ZonMw, Quintiles IMS, NEN, Baker McKenzie)
- Privacybescherming en informatiebeveiliging
- Avg (GDPR) en NEN 7510 (en meer)

# Maatregelen om risico's te beperken en kansen te benutten (deel 1 § 6.1)

- Voer risicoanalyse uit
- Selecteer maatregelen vast
- Gebruik deel 2 als checklist
- Stel verklaring van toepasselijkheid op

- 80 × veel werk voor hetzelfde resultaat
- Tijd voor een baseline

# Structuur

- Gebaseerd op SIVA-methode van Wikram Sewarie
- O.a. toegepast in «Grip op SSD» van CIP:

| **SSD-nr 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. | | | | |
| *Referentie* | Bron 1 | Bron 2 | … | | |
| | | | | | |

Ieder trefwoord vormt een indicator, waaraan voldaan moet worden. Om die reden is ieder trefwoord uitgewerkt. Het gebruikte template voor trefwoorden is:

| **SSD-nr Onderwerp van de norm** | |
|---|---|
| | *indicatoren* |
| /01 | trefwoord |
| /01.01 | indicator 1.1 |
| /01.01 | indicator 1.2 |
| … | … |

# Geadopteerde structuur (concept)

- Maatregel
- Doel (naast de doelstelling van hoofdmaatregel)
- Risico
- Toelichting
- Conformiteitsindicatoren (afgeleid uit maatregel)

# Voorbeeld (eerste concept)

**8.3.1(a)** **Beheer van verwijderbare media (algemeen)**

Maatregel Voor het beheren van ①verwijderbare media behoren ②procedures te worden ③geïmplementeerd ④in overeenstemming met het classificatieschema dat ⑤door de organisatie is vastgesteld.

Doel Beschermen van gegevens die zich op verwijderbare media bevinden of kunnen bevinden, voor zover zulke gegevens bescherming behoeven.

Risico Gegevens op verwijderbare media kunnen op apparatuur die niet onder het beheer van de organsatie staan, worden benaderd door onbevoegden.

Toelichting Verwijderbare media zijn passief, waardoor zaken als toegangsbeheer technisch niet evident zijn.

**Conformiteitsindicatoren**

***8.3.1(a)1*** ***verwijderbare media***

8.3.1(a)1.1 De organisatie kent alle soorten verwijderbare media en heeft deze gedocumenteerd.

8.3.1(a)1.2 De organisatie is in staat de verwijderbare media automatisch te herkennen zodra deze wordt aangesloten.

...

# En toen was er discussie...

- Kunnen we niet met zekerheidsklassen werken?
  Inspiratie: NEN 7512 Vertrouwensbasis voor gegevensuitwisseling
  Gebruik: hoe ver wil je gaan? (risk appetite)

- Kunnen we niet iets met volwassenheid doen?
  Inspiratie: NIAZ/NOREA toetsingskader ZZ3
  Gebruik: hoe goed doen we het? (maturity)

# Maturiteit, maar ... (1)

Enerzijds Capability maturity model (CMM)

| | | |
|---|---|---|
| (0 | Not performed | niets) |
| 1 | Performed informally | ad-hoc proces |
| 2 | Planned & tracked | reactief proces |
| 3 | Well defined | proactief proces |
| 4 | Qualitatively controlled | beheerst proces |
| 5 | Continuously improving | proces verbetering |

# Maturiteit, maar ... (2)

Anderzijds Opzet-bestaan-werking:

| | | |
|---|---|---|
| opzet | is er een ontwerp? | design |
| bestaan | zijn de processen er? | implementation |
| werking | werken ze zoals bedoeld? | effect |

# Maturiteitsfusie (concept)

| | | | |
|---|---|---|---|
| M0 | Not performed | | |
| M1 | Performed informally | | *oordeel over:* |
| M2 | Planned & tracked | opzet | de vastgelegde, beschreven situatie |
| M3 | Well defined | bestaan | mate van overeenstemming van vastgelegde en onderzochte situaties |
| M4 | Qualitatively controlled | werking | bestaan gedurende een bepaalde periode |
| M5 | Continuously improving | | |

# Zekerheid: gevolgklassen

Gevolgen voor informatiebeveiliging:

- voor beschikbaarheid
- voor integriteit
- voor vertrouwelijkheid

Gevolgen voor de echte wereld:

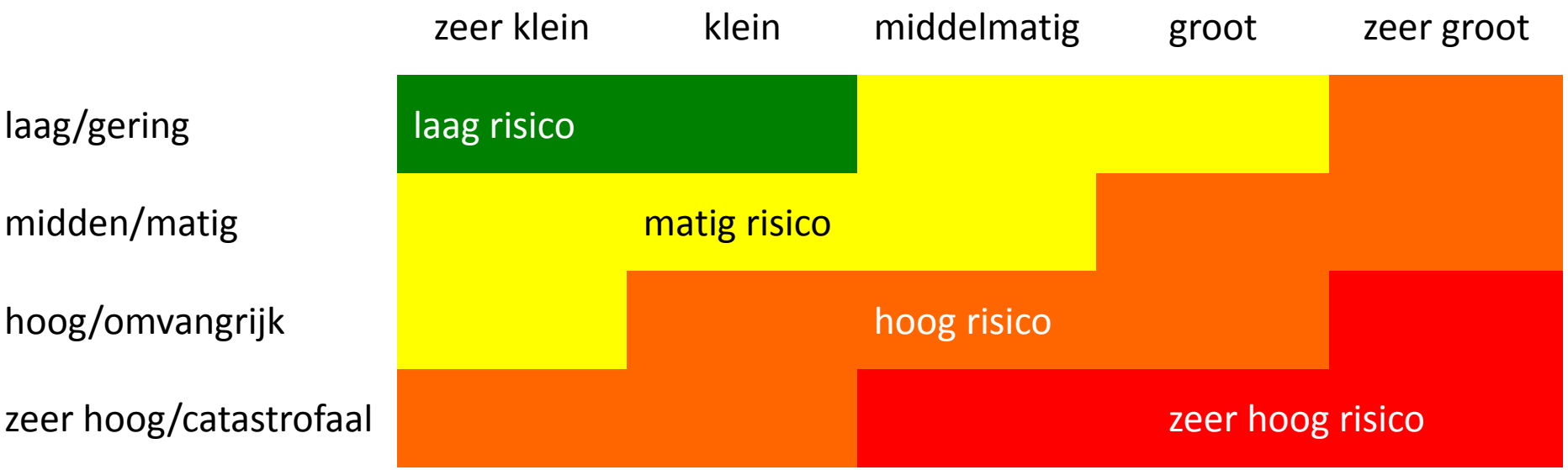
- voor patiënten
- voor de instelling
- voor de maatschappij

# Zekerheid: kansklassen

Kans op zo'n gevolg:

| | | |
|---|---|---|
| Z1 | zeer klein | uiterst kleine kans |
| Z2 | klein | kan, maar meestal niet |
| Z3 | middelmatig | niet onwaarschijnlijk |
| Z4 | groot | zeer goed mogelijk |
| Z5 | zeer groot | zal (vrijwel) zeker optreden |

# Zekerheid = risico = kans × gevolg



# Voorbeeld (tweede concept)

**5.1.1(a)** **Beleidsregels voor informatiebeveiliging (algemeen)**

Maatregel Ten behoeve van informatiebeveiliging behoort een ①reeks beleidsregels te worden ②gedefinieerd, ③goedgekeurd door de directie, ④gepubliceerd en ⑤gecommuniceerd aan ⑥medewerkers en ⑦relevante externe partijen.

Doel Voorkomen dat ... niet voldoende effectief is.

Risico Informatiebeveiliging is ... effectiviteit onvoorspelbaar is.

Toelichting Beleid ten ... (governance) van de informatiebeveiliging.

**Conformiteitsindicatoren**

...

| | | M | Z |
|---|---|---|---|
| ***5.1.1(a)4*** | ***publiceren*** | | |
| 5.1.1(a)4.3 | Het beleid staat op intranet. | 2 | 1 |
| 5.1.1(a)4.4 | Het beleid staat op intranet en is voor alle medewerkers toegankelijk. | 2 | 2 |

...

# Recapitulatie

- Een ziekenhuis hoeft geen risicoanalyse uit te voeren en elke drie-vier jaar te herhalen
- Vooraf ambitieniveau kiezen die 1-op-1 aansluit bij het zekerheidsniveau dat de RvB vaststelt
- De mate van volwassenheid omtrent de implementatie van maatregelen, kan objectief worden beoordeeld
- Vooraf meer duidelijkheid over waar auditors naar kijken

# Vragen?

Hans van Hemert

06 4135 6753

hans@vanhemert-zorgrecht.nl

Beer Franken, Piasau

06 5534 7977

beer.franken@piasau.nl