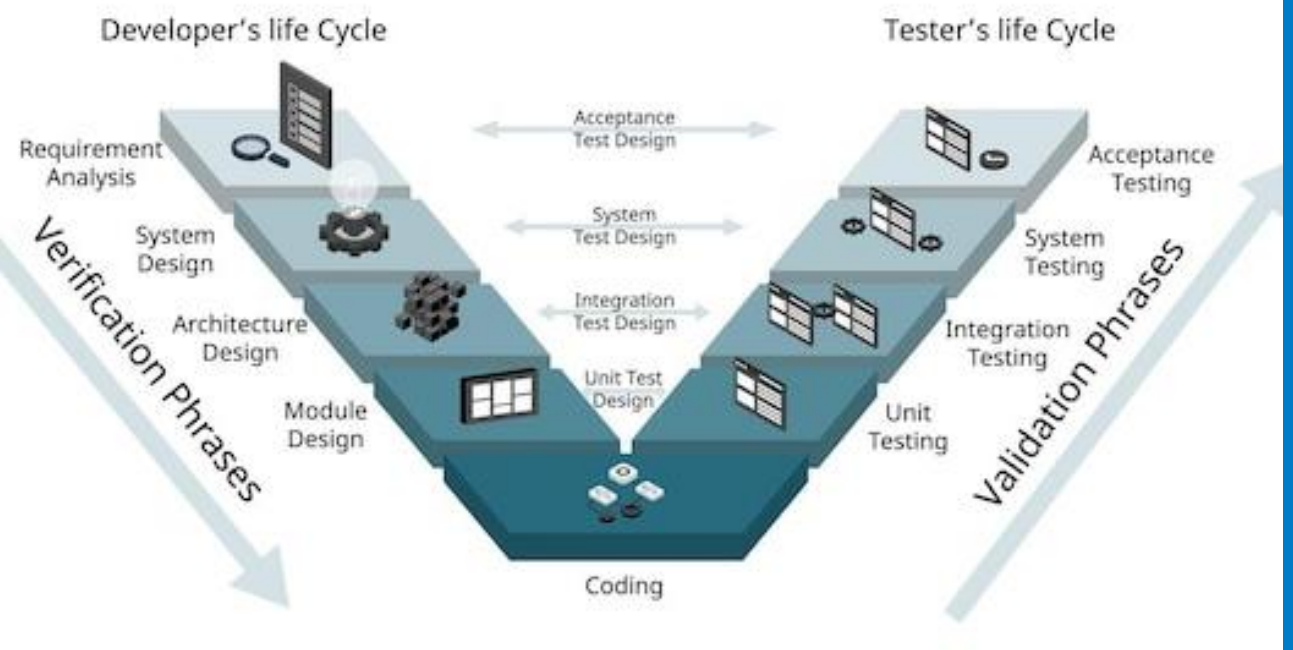



Inspectie Gezondheidszorg en Jeugd
*Ministerie van Volksgezondheid, Welzijn en Sport*

# Validatie van gecomputeriseerde systemen

## Ervaringen uit het toezicht en verwachtingen bij groothandels

Sebastiaan Hoekema, GMP inspecteur
Roelof Mol, GMP-inspecteur

# Wat vinden wij hiervan?


Kern CSV:

1. Borging data-integriteit van e-data (inclusief cyberveiligheid)
2. Business continuity

# Rol RP volgens GDP richtsnoer

1.1 ... Het kwaliteitssysteem staat onder de verantwoordelijkheid van de bedrijfsdirectie en vereist hun leiderschap en actieve deelname en moet worden geschraagd door het engagement van het personeel.

1.2 ... De bedrijfsleiding moet een verantwoordelijke aanwijzen die op basis van een duidelijk omschreven bevoegdheid en verantwoordelijkheid moet zorgen voor de toepassing en de handhaving van het kwaliteitssysteem. (*de RP!*)

...De omvang, structuur en complexiteit van de activiteiten van de distributeur moeten in beschouwing worden genomen bij de ontwikkeling of wijziging van het kwaliteitssysteem.

... Er moet in een wijzigingsbeheersysteem zijn voorzien. Dit systeem moet de beginselen inzake kwaliteitsrisicobeheer bevatten, en evenredig en doeltreffend zijn. (*verantwoordelijkheid van de RP!*)

# Rol RP bij CSV

CSV speelt mogelijk een rol in o.a.:
- Voorraadbeheerssysteem
- Temperatuurcontrole
- Cyberveiligheidsmaatregelen
- Orderafhandelingssystemen
- KMS indien elektronisch (retouren, statuswijzigingen)
- Contractbeheer voor e-diensten
- ...

Maatregelen beginnen bij het in kaart hebben van de risico's (EU-GDP 1.5), dus ...
*Eerst denken, dan doen*.

# Wat zegt de GDP over CSV (3.3.1.)?

Voordat een **computersysteem** in gebruik wordt genomen, moet door ...**validatie**... **Data-integriteit** em de gewenste resultaten op een nauwkeurige, consistente en reproduceerbare wijze kunnen worden verkregen. ...

Gegevens moeten ... worden beveiligd en tegen onopzettelijke of onbevoegde wijzigingen worden beschermd. ... Gegevens moeten worden bevei **Business-continuity** ken. ... Er moeten op te dien het systeem het begeeft of defect is. Hierin moeten systemen voor gegevensherstel worden opgenomen.

# Recente reeks pilot inspecties op CSV

Twee fases:

1. 1-daags inspectie bezoek door 2 inspecteurs naast het reguliere GMP/GDP-inspectiebezoek. Vooraf informatie opgevraagd.
2. Op basis van opgedane ervaringen hebben de 2 inspecteurs bij andere bedrijven die zij (los van elkaar) gingen inspecteren een aantal uren tot een dag besteed aan dit onderwerp.

# Voorbereiding fase 1

Voorafgaand aan de inspecties werd de volgende informatie bij firma’s opgevraagd:

- Een lijst met elektronische systemen incl. kwalificatiestatus, toepassing en type data die wordt gegenereerd.
- Op basis van deze lijst werd de URS van een aantal systemen opgevraagd.
- Enkele dagen voorafgaand aan de inspectie werd een lijst met vragen naar de firma gestuurd o.b.v. de URS.

# Uitvoering fase 1 - inspectiedag

- Bewijsstukken voor de uitgestuurde vragen werd beoordeeld (kwalificatiedocumentatie – IOPQ)
- Beleid rond data-integriteit/cyberveiligheid (in de brede zin van het woord) werd doorgenomen

Afgesproken om niet meer dan 1 belangrijke tekortkoming te geven op deze onderwerpen tijdens deze pilot.

# Wettelijk kader

- GMP deel 1, Hfst. 3 (gebouwen en faciliteiten)
- UPDATE GMP deel 1, Hfst. 4 (data-integriteit)
- UPDATE GMP Annex 11 (Computerized systems)
- GMP Annex 15 (Validation)
- Binnenkort GMP Annex 22

NEW

- **Maar EU-GDP benoemt deze elementen ook (beknopt)**

# Controls (ETSI TR 103 305-1 V4.2.1)

European Telecommunication Standards Institute

Geïnspecteerd op **EU-GMP/GDP** èn op de **ETSI** normen voor Cyberveiligheid:

ETSI is een publieke standaard (dus gratis toegankelijk). Het is geen wet maar bevat handige overzichten die aangeven waar je aan moet denken.

Alles begint met een risico-analyse: eerst denken, en daarna pas iets gaan doen.

# 18 Controls (ETSI TR 103 305-1 V4.2.1)

1: Inventory & Control of Assets Control
2: Inventory and Control of Software Assets
3: Data Protection
4: Secure Configuration of Assets and Software
5: Account Management
6: Access Control Management
7: Continuous Vulnerability Management
8: Audit Log Management
9: Email and Web Browser Protections
10: Malware Defenses
11: Data Recovery
12: Network Infrastructure Management
13: Network Monitoring and Defence
14: Security Awareness and Skills Training
15: Service Provider Management
16: Application Software Security
17: Incidence Response Management
18: Penetration Testing

# Geïnspecteerde bedrijven

| Datum | Firma, land | fase | Karakterisering firma |
|---|---|---|---|
| 06-11-2025 | Firma 2, NL | pilot | Batch certificering en vrijgifte. Groot in omvang. Global IT-team. |
| 10-11-2025 | Firma 1, NL | pilot | Ompakken van parallel-geïmporteerde producten. Groot in zijn soort. IT door moederbedrijf (extern). |
| 20-11-2025 | Firma 3, Singapore | pilot | API Biotech. Groot en high-compliant. Groot global IT-team. |
| 24-11-2025 | Firma 4, Singapore | regulier | Drug product. Zeer grote multi-national. High compliant. Eerder groot incident gehad. Grote global IT-hub. |
| 15-01-2026 | Firma 5, India | regulier | Finished product. Groeiend bedrijf (mid-size), compliant, lokale IT-groep. |
| 04-02-2026 | Firma 6, NL | regulier | IMP. Spin-off van apotheek. Klein, IT-grotendeels uitbesteed. |
| 10-02-2026 | Firma 7, NL | regulier | FP + IMP. Ziekenhuis. IT van ziekenhuis. |
| 02-03-2026 | Firma 8, China | regulier | Biotech DS en FP, zeer ambitieus en groeiend. Eerste bezoek. |

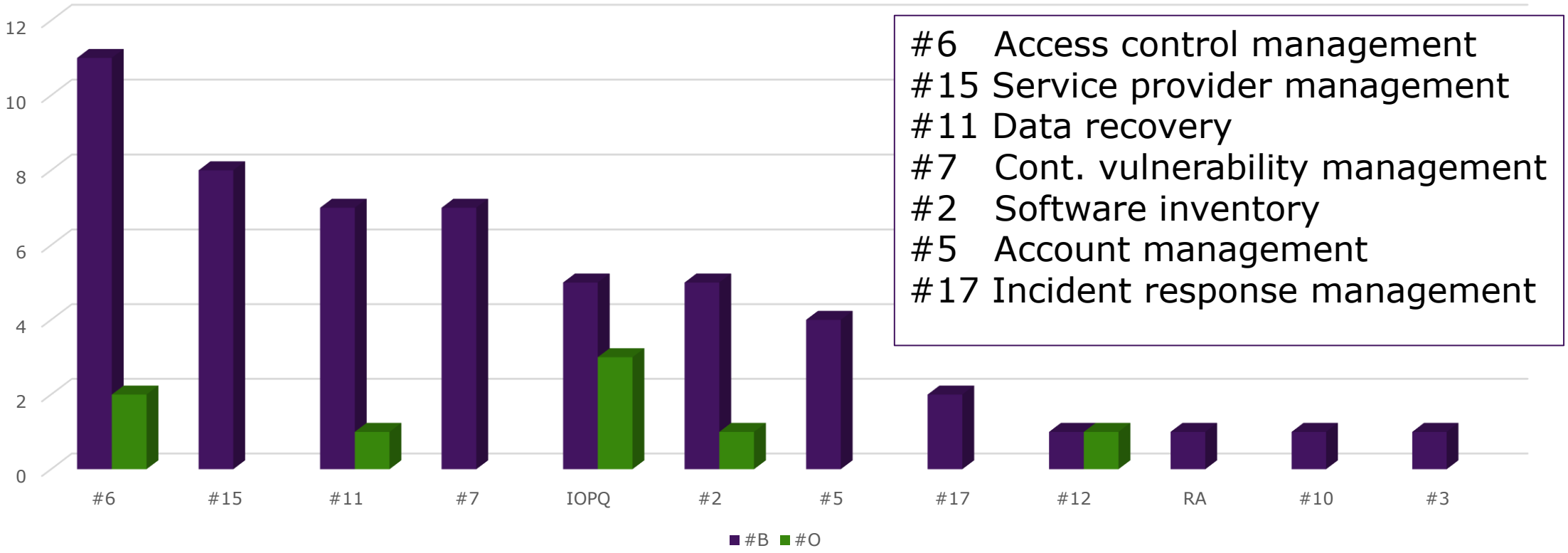
**Er zijn zowel systemen relevant voor GMP als voor GDP beoordeeld!**

# Resultaten – Uitkomst

| datum | Firma, land | fase | Duur besteed aan CSV | **uitkomst[1]** |
|---|---|---|---|---|
| 06-11-2025 | Firma 1, NL | pilot | 1 dag (2p) | **1B** |
| 10-11-2025 | Firma 2, NL | pilot | 1 dag (2p) | **1B 4O** |
| 20-11-2025 | Firma 3, Singapore | *pilot* | 0,75 dag (1p) | **3O** |
| 24-11-2025 | Firma 4, Singapore | regulier | 0,5 dag (1p) | **2O** |
| 15-01-2026 | Firma 5, India | regulier | 0,5 dag (1p) | **1B** |
| 04-02-2026 | Firma 6, NL | regulier | 2 uur (1p) | **1B 1O** |
| 10-02-2026 | Firma 7, NL | regulier | 0,5 dag (1p) | **1B** |
| 02-03-2026 | Firma 8, China | regulier | 0,75 dag (1p) | **4O** |

[1] B = Belangrijke tekortkoming; O = Overige tekortkoming

# Resultaten –uitwerking: frequentie type tekortkomingen




#6 Access control management
#15 Service provider management
#11 Data recovery
#7 Cont. vulnerability management
#2 Software inventory
#5 Account management
#17 Incident response management

# Welke tekortkomingen komen veel voor (1 van 3)

- Toegang tot systemen (Control 6)
  - Reconciliatie van gebruikers niet gedaan of niet gedocumenteerd;
  - Geen inzicht in wie de gebruikers van het systeem zijn;
  - Gebruik maken van generieke accounts (bijv. admin – admin);
  - Meerdere rollen toegewezen aan 1 persoon zonder noodzaak;
  - Gebruikers loggen niet uit.
- Service providers (Control 15)
  - Audits van leveranciers van kritische systemen op basis van een vragenlijst;
  - Kwaliteitsovereenkomsten waarin niets staat over beheer van veiligheid;
  - Geen afspraken over hoe de verantwoordelijkheden verdeeld zijn.

# Welke tekortkomingen komen veel voor (2 van 3)

- Data recovery (Control 11)
  - Er worden geen back-ups gemaakt, de frequentie van backups is te laag;
  - Data retentie periode is te kort;
  - Geen controle op leesbaarheid van de back-up.

- Beheer kwetsbaarheden (Control 7)
  - Geen gedocumenteerde controle en herziening firewall regels;
  - Uitrol van kritische patches niet inzichtelijk of te laat;
  - Geen afspraken met service providers

# Welke tekortkomingen komen veel voor (3 van 3)

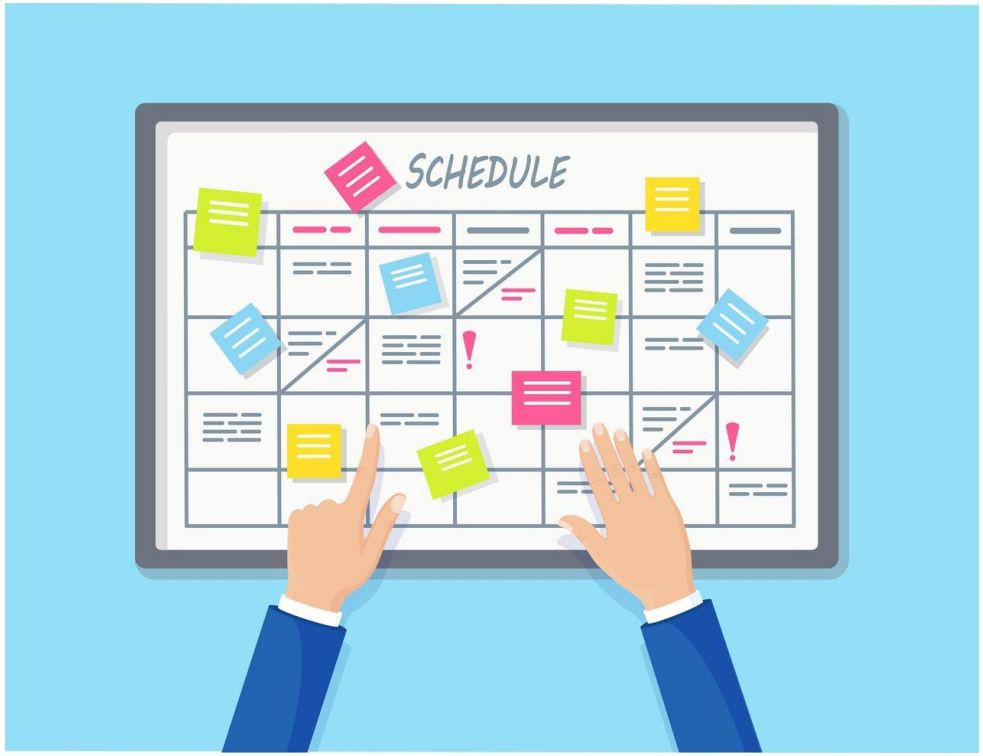
- Systeem kwalificatie (GMP - IOPQ)
  - URS te compact
    - Folder leverancier overgenomen / geen toets aan eigen behoefte
  - Geen DQ uitgevoerd
  - URS Eisen niet of niet volledig geïmplementeerd
  - URS Eisen niet gedocumenteerd getest
  - Alleen ‘happy flow’ getest / geen negatieve controles
  - TRM niet compleet

# Meest risicovolle tekortkomingen

- Te korte wachtwoorden in combinatie met de afwezigheid van multi-factor authenticatie
- Niet tijdige uitrol van updates en kritische patches
- Firewalls niet goed beheerd
- Toegangsbeheer computersystemen
- Leverancierbeheer onvoldoende
- Cyberveiligheidsmaatregelen niet op basis van risico's genomen

**En dan ben je kwetsbaar .....**

# Wat vereist dit van groothandels en RPs?




Een goede voorbereiding:

- Kwalificeer uw gecomputeriseerde systemen gedegen
- Voer een risico-beoordeling uit op cyberveiligheid
  - Voer eventuele acties uit

- **Het is de taak van de RP om dit te overzien**

# Vragen?