Beyond Compliance

Nieuwe standaard: alles weer opnieuw?

AVG regiodag - SEP

8 februari 2024 – Tim Florack – Cuccibu

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Cuccibu
Wie zijn wij

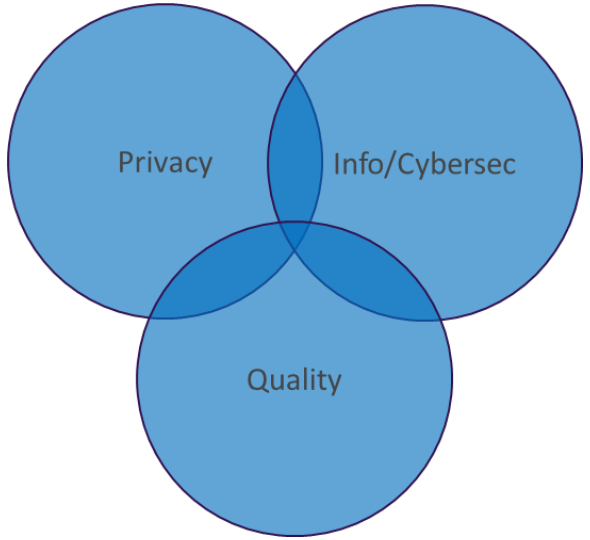
› Cuccibu helpt organisaties om verantwoord om te gaan met gegevens, nieuwe technologie en processen

› Integrale benadering: Juridisch (Privacy), Organisatorisch (InfoSec), Technisch (Cyber), Kwaliteit en duurzaamheid(QHSE)

› We faciliteren in het bereiken van doelen op een verantwoorde manier en zijn altijd op zoek naar toegevoegde waarde:

Reduce Risk, Create Value!

› Opgericht in 2014
› Eindhoven & Rijswijk
› >100 bedrijfskundigen, juristen, techneuten

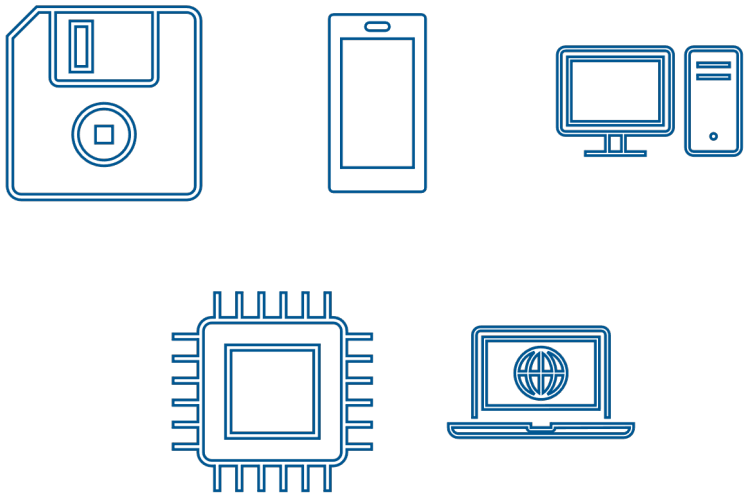


Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie

En de rol van compliance daarin

De noodzaak voor een weerbare organisatie
Ontwikkelingen volgen elkaar steeds sneller op



› AI Act

Over het algemeen kan de ontwikkeling van ChatGPT als een belangrijke mijlpaal in de voortdurende evolutie van kunstmatige intelligentie worden beschouwd, met aanzienlijke gevolgen voor de manier waarop we leven, werken en communiceren.

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie
Afhankelijkheid van digitalisering

› Wat is kritiek voor een organisatie?

› Onmogelijk om terug te vallen op analoge manier van werken

› NIS2

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

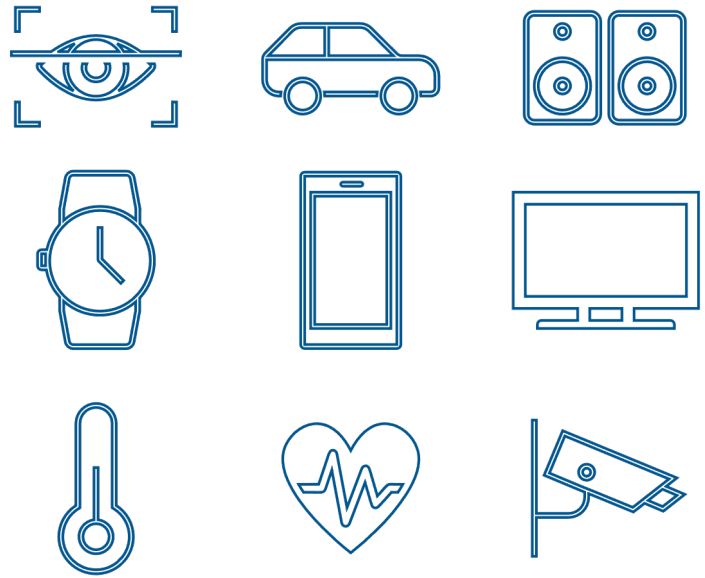
De noodzaak voor een weerbare organisatie
Alles en overal verbonden

› De fysieke en digitale wereld raken steeds verder verweven

› Alles wordt SMART

› Operational Technology

› Aanvalsoppervlak wordt steeds groter



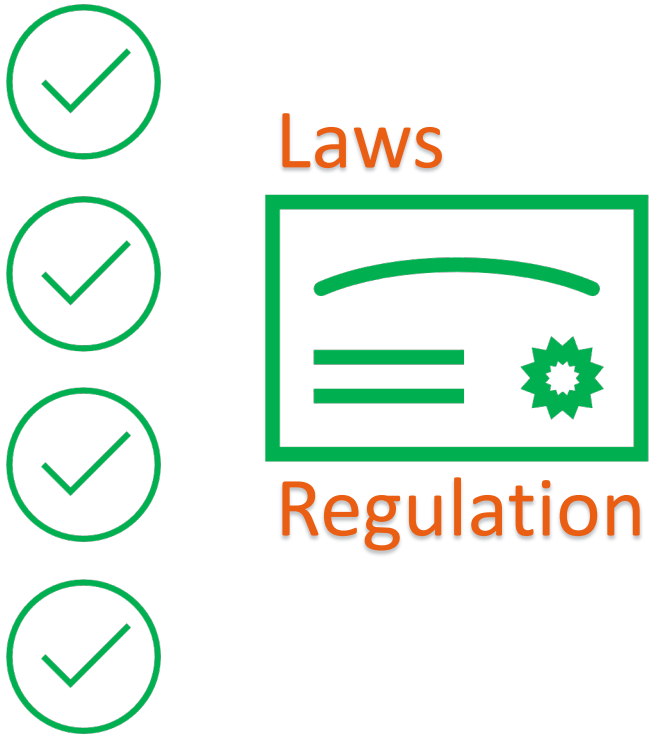
› Cyber Resilience Act

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie

Vinken alleen is nooit voldoende

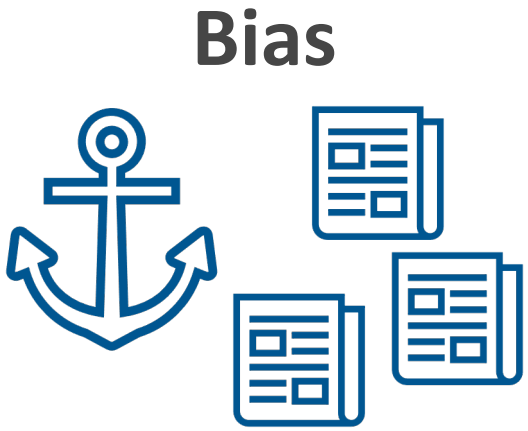
Bron: Onbekend - US Coast Guard - 100421-G-XXXXL

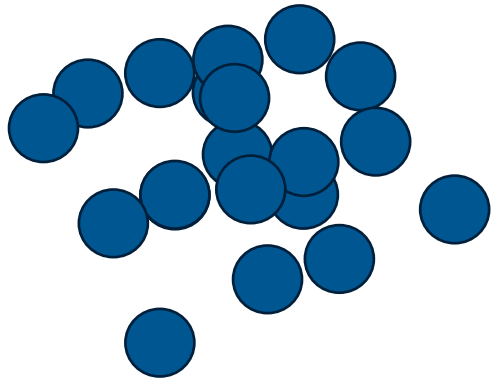


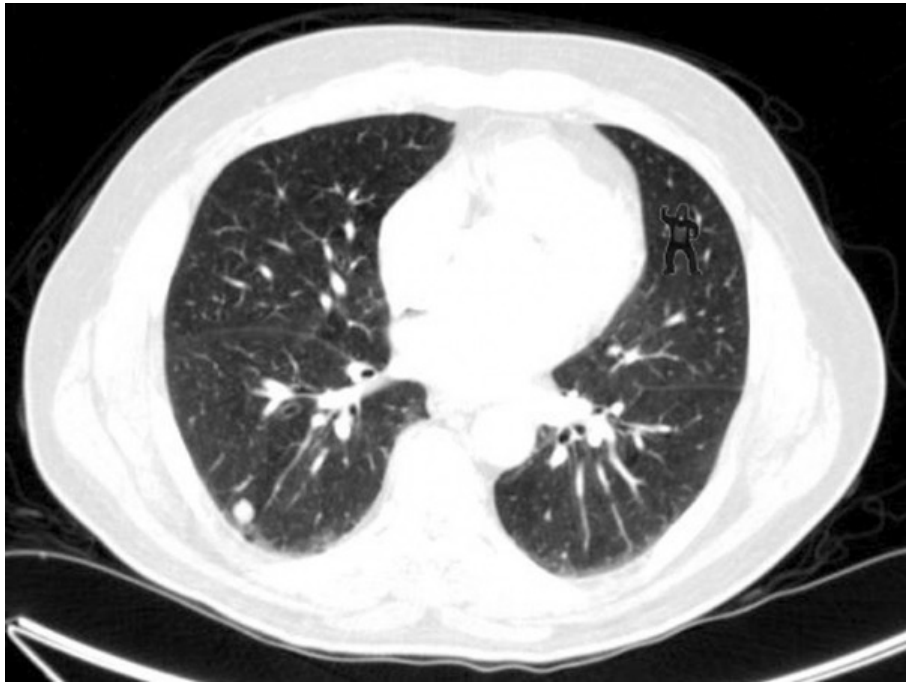
Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie

In hoeverre kunnen we alles overzien?







Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie
Veranderend denken over risico's

- Risicomanagement vanuit reactief en preventief denken zorgt voor maatregelen gericht op voorkomen. Vanuit een idee dat je alles kunt overzien.
- Wat als de ontwikkelingen te snel gaan? Wat als de bedreigingen nieuw zijn? Een nieuwe kwetsbaarheid? Een nieuw virus?

Voorkomen is beter dan genezen?

Beyond Compliance!

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

De noodzaak voor een weerbare organisatie
Waarom compliance toch van belang is

- **Risicomanagement**: compliance helpt risicomanagement goed in te richten, denken vanuit het risico in plaats van vanuit de maatregel/norm is cruciaal
- **Reputatie**: compliance helpt bij het opbouwen van een positieve reputatie, non-compliance juist (dubbel zo erg) voor het tegenovergestelde
- **Efficiency**: bepaalde regelgeving helpt processen te stroomlijnen
- **Duurzaamheid**: een positieve bijdrage aan de maatschappij (ESG)
- **Licence to operate**: soms '*moet*' het toch echt

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Certificering/Assurance? Verschillende vormen van zekerheid

Certificering/Assurance
Verschillende standaarden

- De wet…
- ISO/NEN – (inter)nationale standaarden
- Richtlijnen vanuit brancheorganisaties (bijv.: VNG, NOREA)

- We lichten er 2 uit vanuit privacy:
  - ISO27701
  - BC5701

Certificering/Assurance
Wat is het verschil

Assurance

- Verstrekken van vertrouwen over de manier waarop een bepaald proces/activiteit wordt uitgevoerd
- Toetsen van normen of beweringen
- Breed toepasbaar
- **Momentopname of periode, maar altijd zekerheid over het verleden. En resultaten in het verleden….**
- Toetsing door RE (in NL)
- ISAE/NOREA/SOC1,2,3/TPM

BC5701

Certificering

- Gericht op het aantonen dat een organisatie voldoet aan een specifieke, extern gedefinieerde standaard
- Audit om te toetsen of aan standaard wordt voldaan
- **Vanuit ISO, doorgaans gericht op een managementsysteem (kwaliteit/ISMS), daardoor meer zekerheid naar toekomst**
- Toetsing door Certificerende Instelling
- ISO27x, ISO9001, NEN

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Certificering/Assurance
ISO27701 – aanvulling op 27001

- De ISO27701 richt zich op het Privacy Information Management System (PIMS)
- Integratie met ISMS mogelijk, internationaal geaccepteerde standaard
- Richt zich niet op één specifiek proces maar op de wijze waarop privacy in de organisatie is georganiseerd
- **Biedt geen zekerheid over de compliance van een specifieke verwerking met de AVG**

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Certificering/Assurance
BC5701 – Net iets anders

- Gericht op een specifieke verwerking
- Managementsysteem is niet het object van onderzoek (wel onderdeel van de toetsing)
- Mogelijkheid tot aantonen of een specifiek proces/gegevensverwerking voldoet aan de gestelde normen (ofwel: de AVG)
- Qua “waarde” en toetsing heeft het daardoor meer weg van assurance dan de “typische” ISO certificering

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Certificering/Assurance

ISO27701 en BC5701: Wanneer welke gebruiken?

ISO27701

- Organisatiebrede certificering
- Aansluiten op (bestaande) kwaliteitssystemen
- Combinatie met ISO27001
- Internationaal erkend

V.S.

BC5701

- Toetsing specifiek proces en dus zekerheid over die verwerking van persoonsgegevens
- Voor (kritieke) processen met een bepaalde gevoeligheid→vertrouwen naar betrokkenen
- Verantwoordelijke/verwerker relaties
- Goedkeuring AP

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

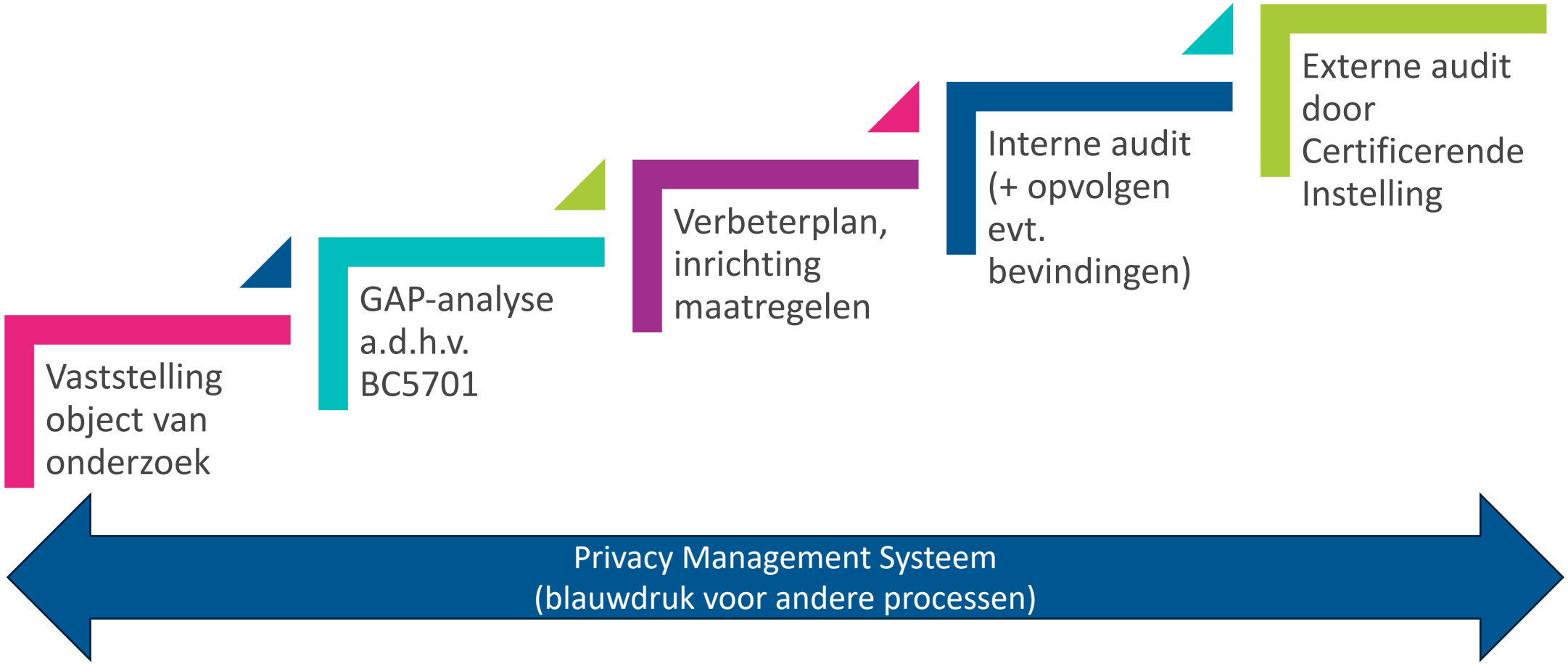
BC5701
Hoe te voldoen?

BC5701
De voorbereiding

- Kritisch op afbakening object van onderzoek: voor welk proces is interne of externe bevestiging van compliance gewenst/gevraagd
- Een DPIA – in de toekomst rekening houdend met toetsingskader BC5701 - biedt samen met het register een goede houvast als basis voor de certificering
  - Risicoanalyse AVG op een specifieke verwerking geeft doorgaans al voldoende antwoord op groot aantal doelstellingen die ook in BC5701 gesteld worden. Ook bevat een (goede) DPIA een omvattende beschrijving van de verwerking
- Voor het managementsysteem is het privacybeleid/governance van de organisatie leidend

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

BC5701
Stappen tot certificering op hoofdlijnen



Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

Next steps
Key take-aways

Next steps en key take-aways
Het hoeft dus niet opnieuw (*hopelijk*)

Key take-aways

› Compliance is een basis, cultuur maakt weerbaar

› BC5701 en ISO27701 ieder haar eigen karakter

› BC5701 zeer geschikt om vertrouwen te geven over kwaliteit/compliance van een proces/verwerking

› Uitstekend toepasbaar in verantwoordelijke/verwerker relatie of een stakeholderbehoefte

Next steps

› Bepalen welke behoefte/vraag er is ten aanzien van de verwerkingen of AVG compliancy

› Proces vaststellen en afbakenen

› Indien BC5701: dan DPIA en register als basis voor vervolgstappen richting certificering

Cuccibu - Any reproduction of these slides is prohibited without written permission of Cuccibu

cuccibu

Reduce Risk, Create Value