cuccibu

Reduce Risk, Create Value

“Beat the auditor”

Tips voor een soepele audit!

Tim Florack

September 2022

Dit document is de rode draad van een presentatie. Zonder de voice-over is dit materiaal incompleet. Het dient als naslagwerk.

Beat the auditor
Waar gaan we het over hebben?

- ENSIA - Snel opfrissen
- ENSIA - Wijzigingen 2022 en verder
- Aanpak van de auditor
- Voorbeelden
  - Controls
  - Vastlegging
  - Toetsing
  - Risicoinschatting

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

ENSIA
Snel opfrissen

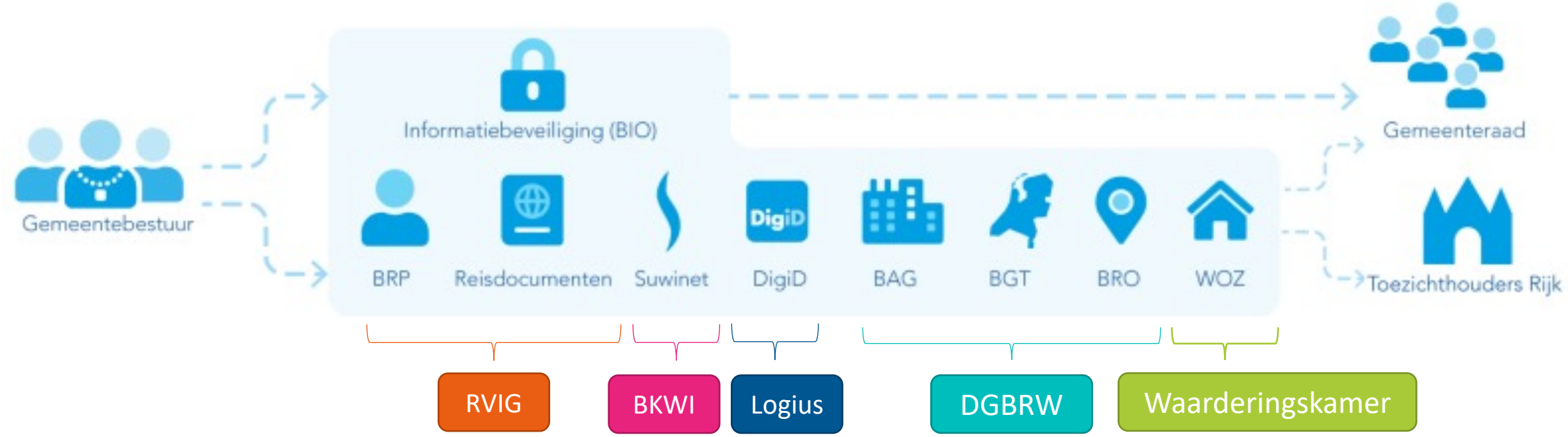
ENSIA – Snel opfrissen
Structurele verbetering Informatieveiligheid

- Gemeenten verantwoordelijk voor allerlei soorten informatie
- Auditlast binnen gemeenten - Verschillende normenkaders
- Ketenbenadering: Gemeente verantwoordt, ook bij uitbesteding.
- Verschillende toezichthouders stellen dezelfde vragen (of niet!?)
- **Verantwoording aan gemeenteraad en rijksoverheid**

ENSIA | Eenduidige Normatiek Single Information Audit

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

ENSIA – Snel opfrissen
Traject van ENSIA 2022



Bron: https://vng.nl/projecten/ensia
www.cuccibu.nl

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

ENSIA – Snel opfrissen

Traject van ENSIA 2022

ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad		Verantwoording aan toezichthouders
Zelfevaluatie	• Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO). • Domeinspecifieke vragenlijsten voor diverse stelsels. • Zelfevaluatie afronden en vastleggen in ENSIA.	1 JUL 2022 31 DEC 2022	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO. • Waarderingskamer: Informatiebeveiliging, systeembeheer en architectuur WOZ.
Opstellen	• Genereren en opstellen verantwoordingsrapportages. • Audit door gecertificeerde IT-auditor over collegeverklaring Suwinet en DigiD. • Opstellen rapportage ENSIA t.b.v. de gemeenteraad.		Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Rapportage WOZ door college van B&W. • Uittreksels BRP en Reisdocumenten. • Rapportage ENSIA voor de gemeenteraad.
Verantwoorden	• Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. • Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Uittreksels BRP en Reisdocumenten via Kwaliteitsmonitor).	30 APR 2023	Resultaten: • De toezichthouders BKWI, Logius, DGBRW en Waarderingskamer krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt de Uittreksels BRP en Reisdocumenten via de Kwaliteitsmonitor aangeleverd.
Versturen	• Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag. • Gemeenteraad neemt kennis van rapportage ENSIA. • College van B&W stelt jaarverslag vast. • Gemeenteraad keurt jaarverslag goed. • Het college van B&W stuurt het gemeentelijk jaarverslag aan BZK.	15 JUL 2023	• De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. • De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Bron: https://vng.nl/projecten/ensia

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

ENSIA – Snel opfrissen
Rol van NOREA – de auditor

- Nederlandse Orde Register EDP Auditors - Beroepsorganisatie IT Auditors (RE's)
  - Kennisgroepen DigiD en ENSIA
  - Borging vaktechniek (assurance)
  - Sparringspartner Logius/VNG/BKWI

- **Handreiking ENSIA (laatste versie: Handreiking ENSIA, versie 4.0 (Update 2021))**
  - **Versie 2022 nog niet definitief (lopende discussie DigiD normering en 'elektronische handtekening')**

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

ENSIA
Wijzigingen 2022 en verder

ENSIA - Wijzigingen 2022 en verder
Wijzigingen voor 2022

- Suwinet guidance VNG en NOREA handreiking met elkaar in lijn gebracht
- Onder voorbehoud: Logius heeft B.01 (Informatiebeveiligingsbeleid) toegevoegd aan het DigiD normenkader per 1 augustus 2022.

Werking

- De invoering van de toetsing op werking voor DigiD normen U/TV.01, U/WA.02, C.07, C.08 en C.09
  - Vanaf inleverperiode **1 januari - 1 mei 2024 (over het voorgaande jaar 2023)** **mogen** DigiD-aansluithouders de 5 normen laten toetsen op werking.
  - Vanaf inleverperiode **1 januari - 1 mei 2025 (over het voorgaande jaar 2024)** **moeten** DigiD-aansluithouders de 5 normen laten toetsen op werking.

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

Aanpak van de auditor
Inzicht in de werkwijze van de RE

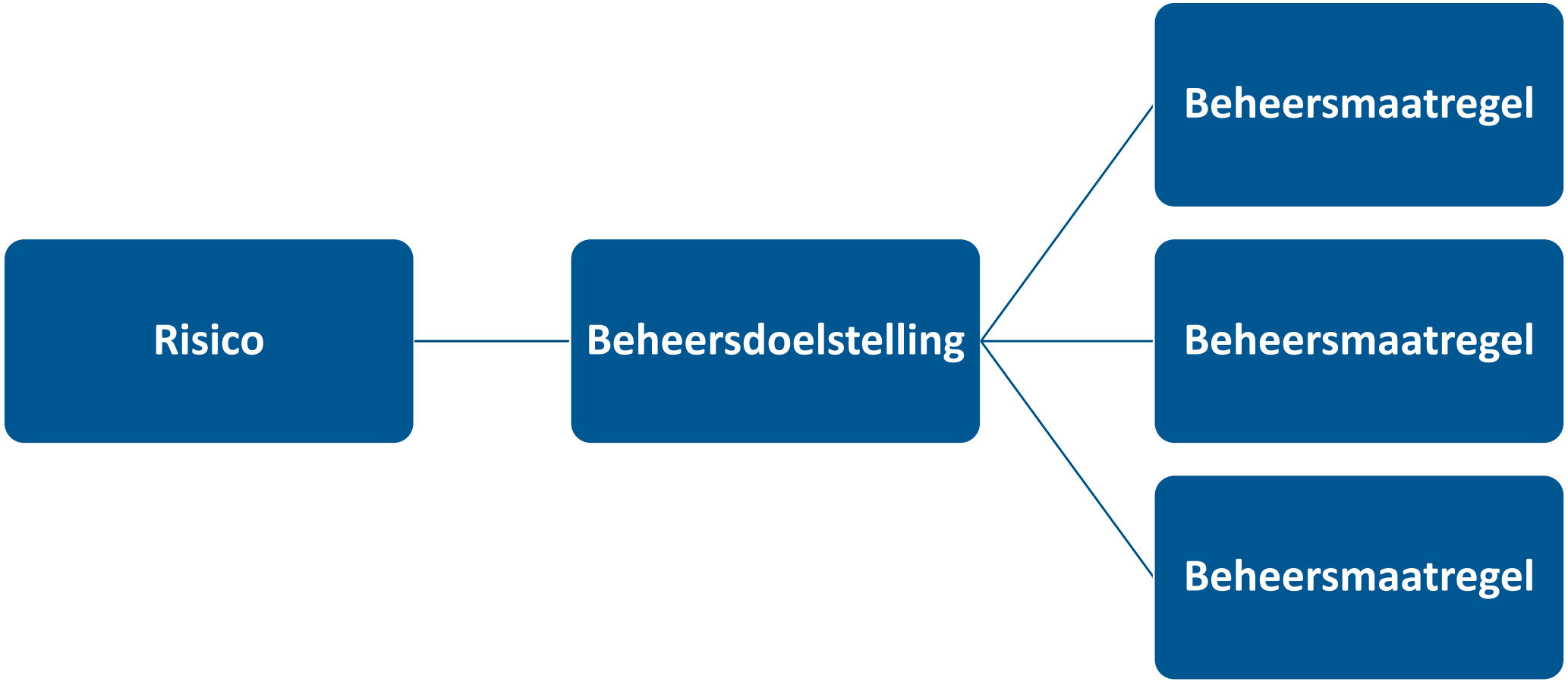
Aanpak van de auditor
Hoe waarheidsgetrouw is de collegeverklaring…?

- Scope: Collegeverklaring (Suwi en DigiD)
  - Collegeverklaring bevat een bewering (‘assertion’) die door de auditor beoordeeld dient te worden via de zelfevaluatie. Anders dan een ‘directe’ audit, waarbij de auditor zelf de lead heeft.
  - Op basis van een risico inschatting dient de auditor te bepalen in hoeverre de bewering betrouwbaar is (bijvoorbeeld: volwassenheid organisatie)
  - In de praktijk worden vaak alle normen geëvalueerd al dan niet door zelfstandige werkzaamheden
- Diepgang 2022: opzet en bestaan
- Resultaat: Assuranceverklaring over de collegeverklaring

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

Aanpak van de auditor

Van risico naar norm en weer terug



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

Aanpak van de auditor

Diepgang – Opzet, Bestaan, Werking

Opzet
(design)

- Is de norm gedefinieerd?
- Is er een ontwerp? (beleid, procedures, procesbeschrijving)

Bestaan
(implementation)

- Bestaat het proces (conform de opzet)?
- Is het proces geïmplementeerd?
- Kan aan de norm getoetst worden?

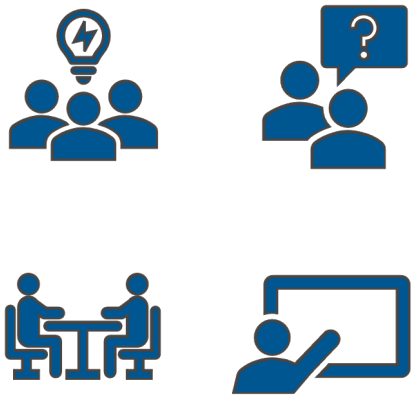
ENSIA

Werking
(operating effectiveness)

- Is de maatregel gedurende de gehele periode effectief geweest?

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

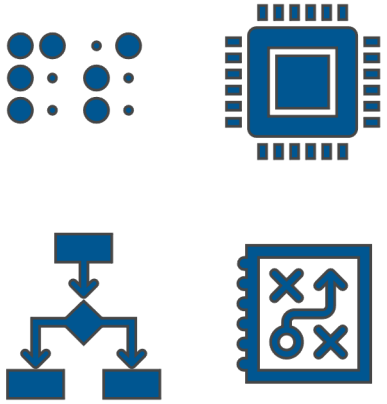
Aanpak van de auditor
Toetsen van de opzet



Interview
Afstemmend vraaggesprek
Workshop

Beleid
Procedures
Werkinstructies

Systeemdocumentatie



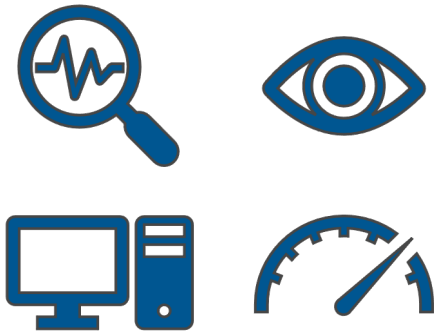
Processchema
Applicatiediagram
Netwerkdiagram

- Actualiteit/geldigheid/volledigheid van documentatie
- Formele vaststelling van beleid/procedures
- Verificatie van standpunten/meningen/feiten
- Beantwoord vragen feitelijk (en eerlijk)
- Geef niet meer dan gevraagd (smoking gun)

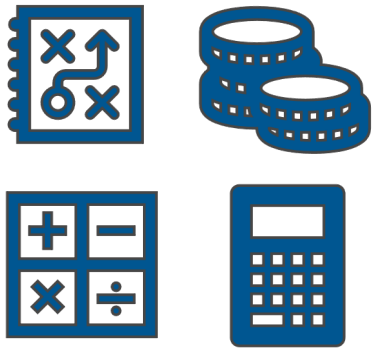
Aandachtspunten

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

Aanpak van de auditor
Toetsen van het bestaan

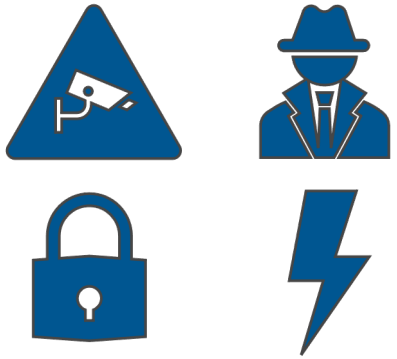


Inspectie
Waarneming
Systeemobservatie



Herberekenen

Lijncontrole
Walkthrough
Reperformance



Vulnerability scan
Pentest
Social engineering

- Trial & Error
- Afwijken van ‘happy flow’
- What could go wrong?

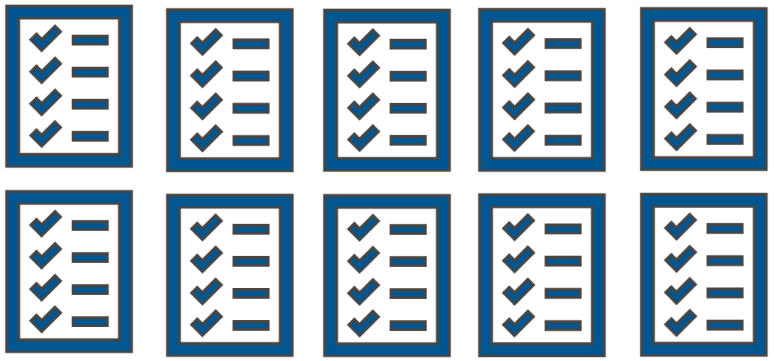
- Geldigheid van screenshots
  - Datum & volledig scherm
- Volledigheid evidence (lijsten)

Aandachtspunten

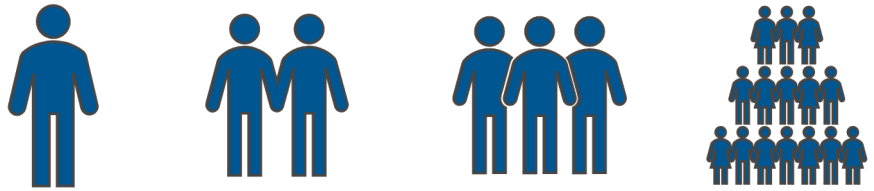
Cuccibu BV - Any reproduction of these slides is prohibited
without written permission of Cuccibu BV

Aanpak van de auditor

Toetsen van werking ((**nog**) niet voor ENSIA)



Steekproef & data-analyse



- Grootte van steekproef
- Let op de juistheid van de periode

Aandachtspunten

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

Aanpak van de auditor
Voorkom afvinkdiscussies – stem af

- Doelstelling en risico altijd de kern
- Waren compenserende/mitigerende maatregelen (aantoonbaar) effectief?
- Hoor/wederhoor: Vraag vooraf of de observaties afgestemd worden.
- Een norm die faalt is niet direct een risico (challenge de auditor)
- Management reactie: een verantwoorde afweging om een risico te nemen kan ook tot de mogelijkheden behoren. (Let op: Logius verwacht wél verantwoording per norm)
- **Documentatie van risicoanalyse ondersteunt in de samenwerking met de (externe) auditor.**

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

Voorbeelden

Control – vastlegging - toetsing

Voorbeelden
DigiD norm U/TV.01

De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.

Doelstelling:
Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.

› Wat is het risico?

› Welke ‘controls’ mitigeren dit risico?

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

Voorbeelden
DigiD norm U/TV.01 – Mogelijke controls

De organisatie beschikt over een beschreven procedure voor in-door-uitstroom	De organisatie beschikt over een vastgestelde autorisatiematrix	Nieuwe of gewijzigde accounts worden goedgekeurd door een leidinggevende	Accounts van uitdiensttreders worden tijdig verwijderd
Wachtwoorden voldoen aan complexiteitseisen	Accounts worden periodiek geëvalueerd op geldigheid.	Beheerrechten zijn enkel toegekend aan daartoe bevoegde medewerkers	Gebruikersaccounts zijn uniek identificeerbaar

› Wat legt de organisatie vast van bovenstaande controls?

› Hoe toetst de auditor bovenstaande controls (opzet/bestaan/werking)

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

Voorbeelden
DigiD norm U/TV.01 – Risico-inschatting

De organisatie beschikt over een beschreven procedure voor in-door-uitstroom	De organisatie beschikt over een vastgestelde autorisatiematrix	Nieuwe of gewijzigde accounts worden goedgekeurd door een leidinggevende	Accounts van uitdiensttreders worden tijdig verwijderd
Wachtwoorden voldoen aan complexiteitseisen	Accounts worden periodiek geëvalueerd op geldigheid.	Beheerrechten zijn enkel toegekend aan daartoe bevoegde medewerkers	Gebruikersaccounts zijn uniek identificeerbaar

› Welke controls zijn ‘key’ in het mitigeren van het risico?

› Welke compenserende controls/werkzaamheden kunnen het risico beperken/uitsluiten?

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

Voorbeelden
Suwi norm 7.2.2 Bewustzijn, opleiding en training

Criterium BIO:
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Doelstelling:
Het bewustmaken van gebruikers van Suwinet gegevens

› Wat is het risico?

› Welke ‘controls’ mitigeren dit risico?

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

Voorbeelden
Suwi norm 7.2.2 – BIO controls

7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.

7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.

7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.

› Wat legt de organisatie vast van bovenstaande controls?

› Hoe toetst de auditor bovenstaande controls (opzet/bestaan/werking)

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

Voorbeelden
Suwi norm 7.2.2 – Risico-inschatting

7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.

7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.

7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.

› Welke controls zijn ‘key’ in het mitigeren van het risico?

› Welke compenserende controls/werkzaamheden kunnen het risico beperken/uitsluiten?

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

ENSIA Tips

Tot slot

ENSIA Tips
(Webinar ENSIA 2020 - Cuccibu)

- Tip 1: Ken de achtergrond
- Tip 2: Weet wat er gewijzigd is
- Tip 3: Governance van informatiebeveiliging is key
- Tip 4: Een goede voorbereiding... Ken je scope!
- Tip 5: Het wiel is al uitgevonden... Gebruik standaarden
- Tip 6: Inzicht in de aanpak van de RE voor een soepele audit
- Tip 7: Risico’s, Risico’s, Risico’s…
- Tip 8: Neem het volgende jaar mee in deze cyclus

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

cuccibu

Reduce Risk, Create Value

Eindhoven | Delft | www.cuccibu.com | info@cuccibu.nl | +31 (0) 85 303 2984