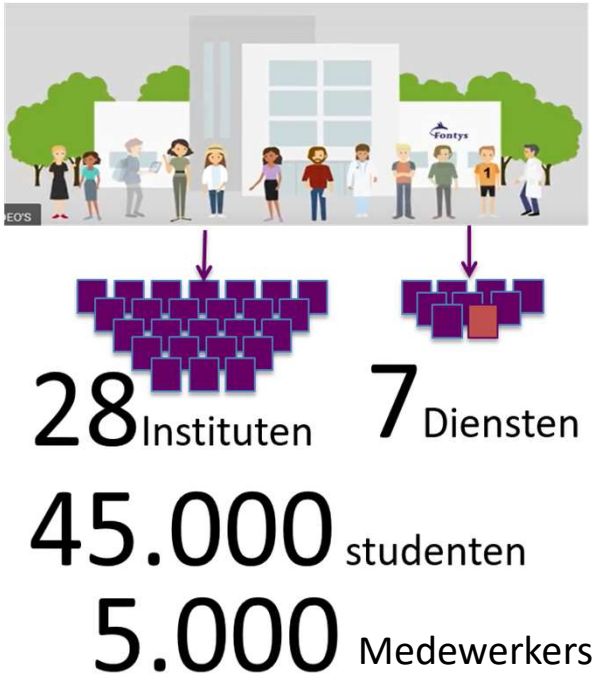
Maesbruggen III & Fontys Hogescholen

Fontys Hogescholen



Max Webber

Ing. MSc. CISSP CISA CISM CIPP/e

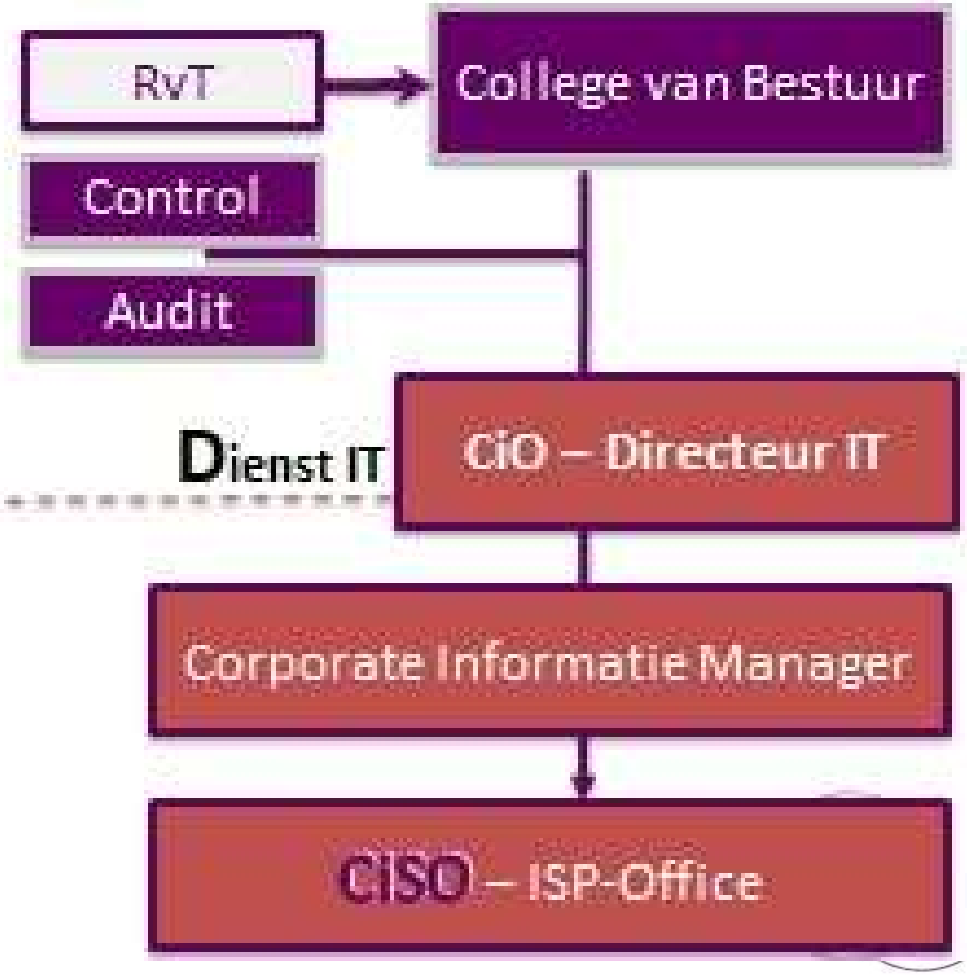
Privacy security expert

CISO Fontys Hogescholen
(sinds oktober 2018)

Governance en uitdagingen

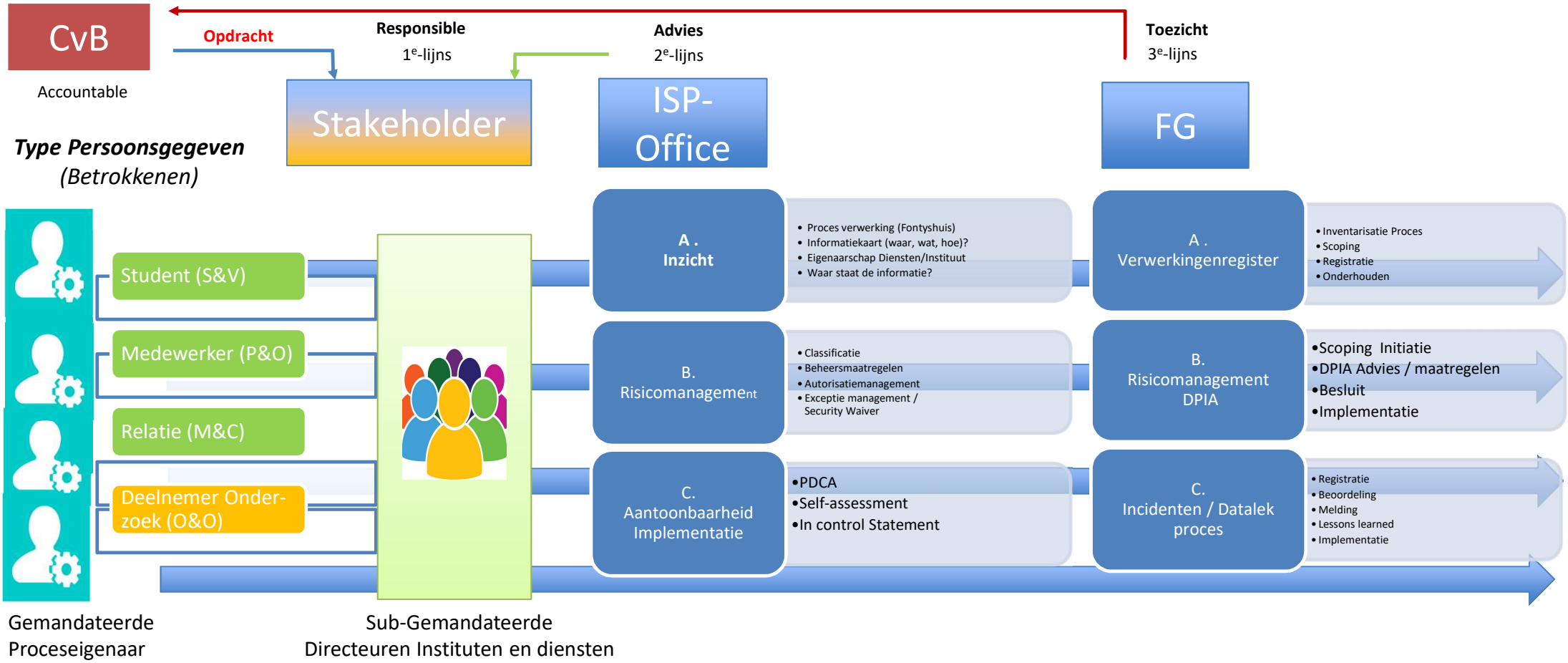
28 Instituten

7 Diensten



Fontys

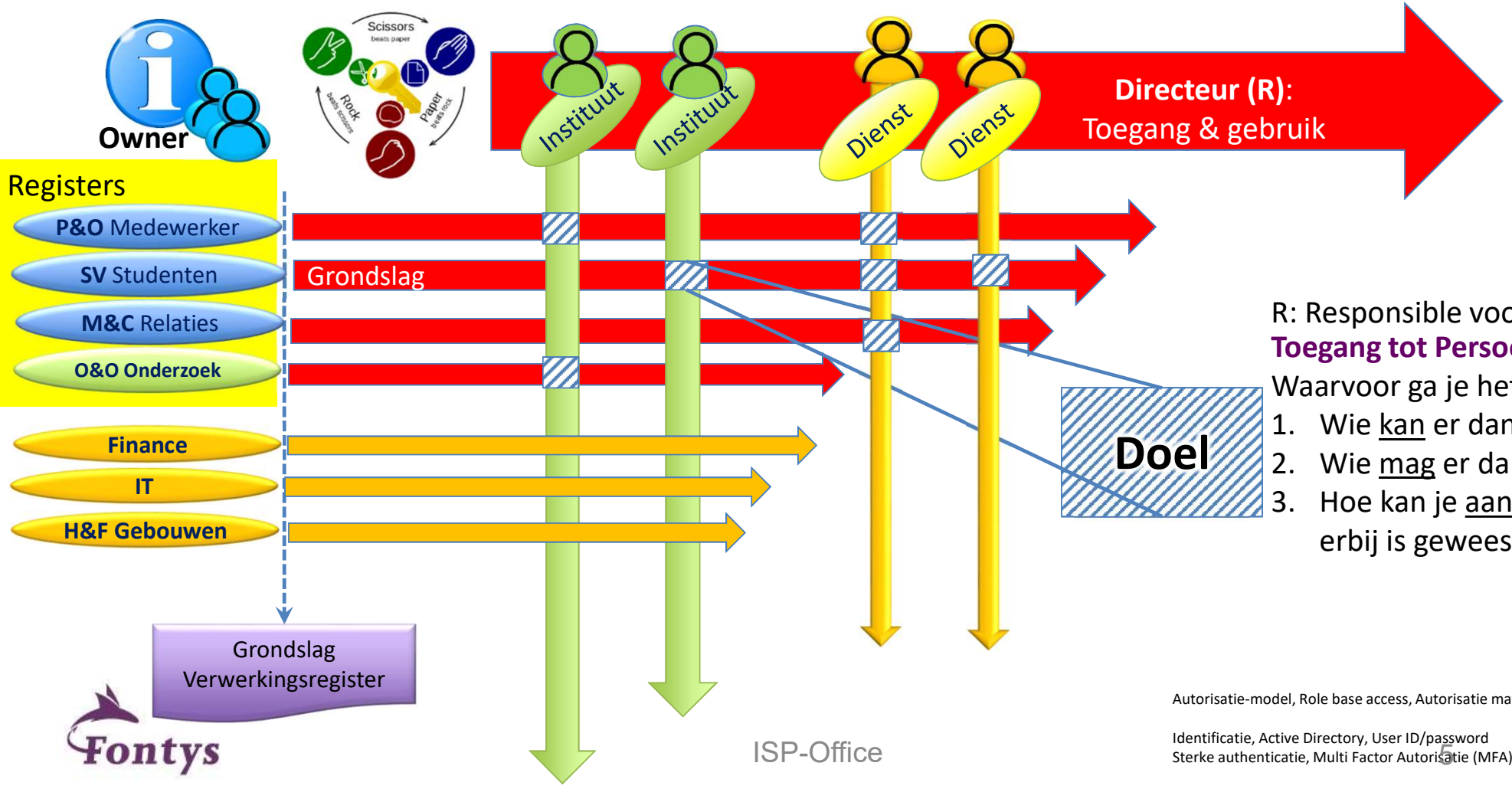
Toezicht & Privacy Fontys



Eigenaarschap Persoonsgegevens

Spelregels Informatie Gebruik

Owner: Accountable
Grondslag
(Verwerkingsregisters)



R: Responsible voor…
Toegang tot Persoonsgegevens
Waarvoor ga je het gebruiken?

1. Wie <u>kan</u> er dan bij?
2. Wie <u>mag</u> er dan bij (doel)
3. Hoe kan je <u>aantonen</u> wie erbij is geweest

Autorisatie-model, Role base access, Autorisatie matrix

Identificatie, Active Directory, User ID/password
Sterke authenticatie, Multi Factor Autorisatie (MFA)

Fontys

ISP-Office

DENK GROTER

Hoelang duurde uw kortste opdracht?

1. Minder dan 1 week.
2. Minder dan 1 maand.
3. Minder dan 1 jaar.
4. Meer dan 1 jaar.

Waar zit uw kracht?

1. Communicatie en inlevingsvermogen.
2. Processen en techniek doorzien.
3. Risico- en probleemanalyse.
4. Anders te weten….

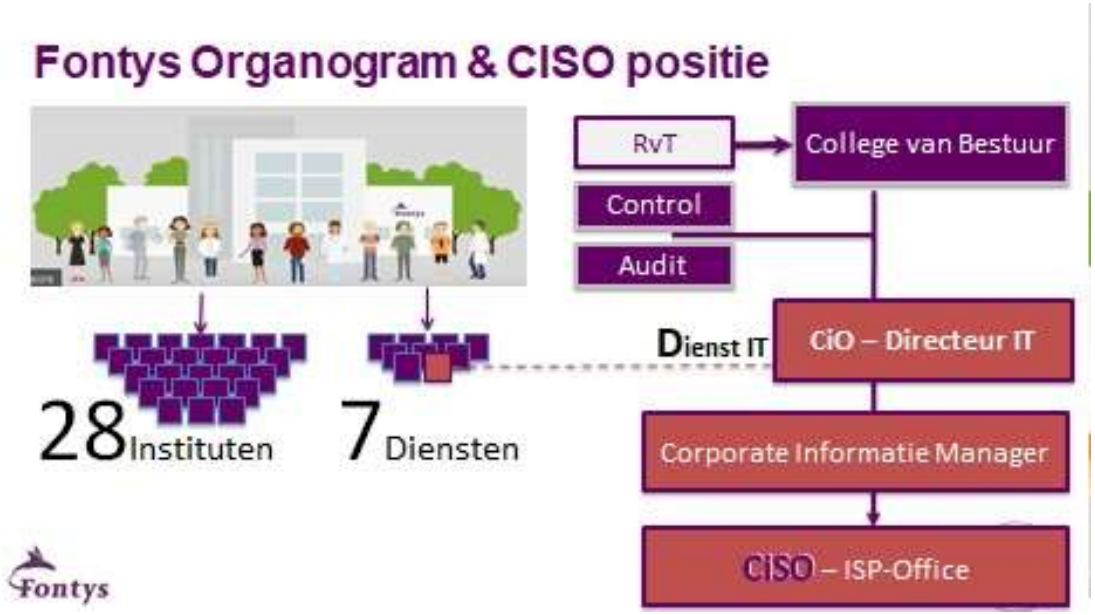
Vakjargon, hoe gaat u er mee om?

1. Blaas het management van zijn sokken.
2. Leg alles in Jip en Janneke uit.
3. Gebruik vakjargon gepast en gedoceerd met uitleg.
4. Gebruik een sterk vereenvoudigd model.

Verantwoordelijkheden wat is meest effectief?

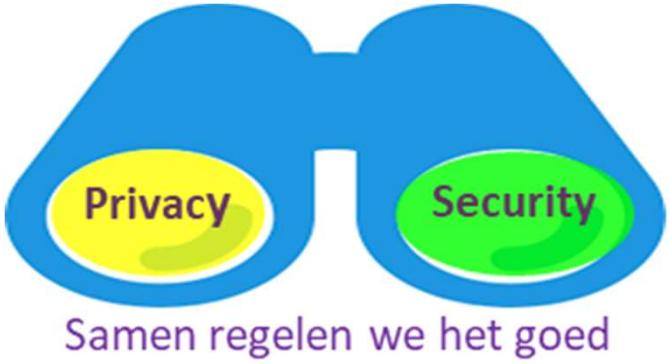
1. We benaderen het praktisch en vertrouwen op de hiërarchie.
2. We passen Zero trust model op ICT omgeving toe.
3. RASCI wordt 100% Rol Based ingeregeld.
4. Goed Risicomanagement is de sleutel.

Waar zou u de CISO positioneren?



1. Is minder relevant het gaat om de rol.
2. Dichter bij College van Bestuur.
3. Huidige positie onder CIO & CIM-er is oké
4. Anders, te weten....

Wie zou inzicht en controle in verwerking moeten verkrijgen? (opdracht geven)

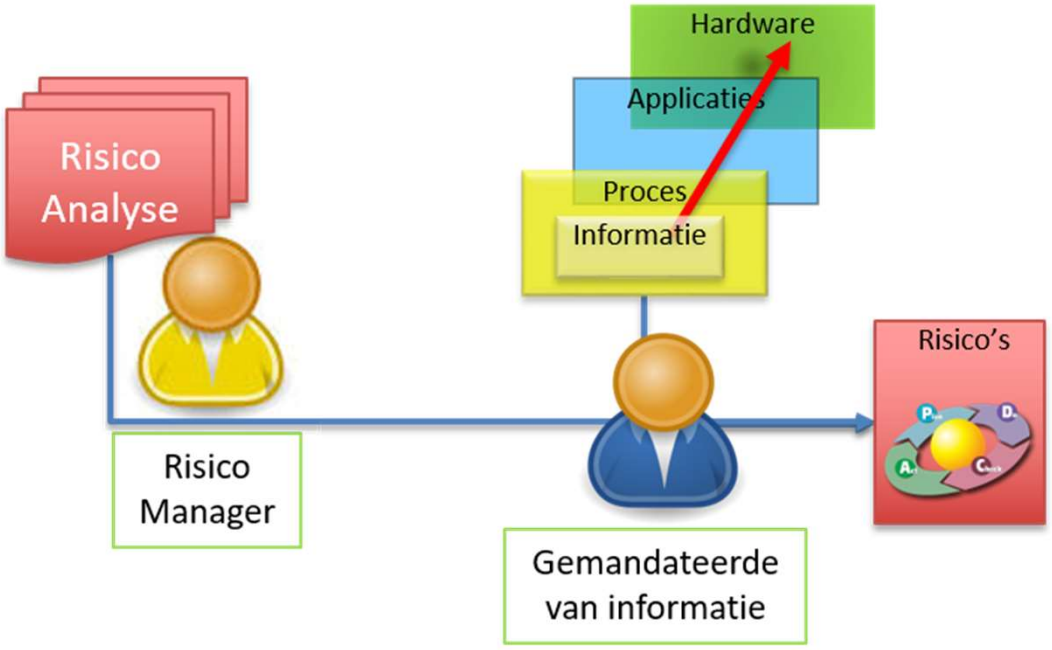


1. College van Bestuur of Gemandateerde (verantwoordelijke).
2. CISO samen met FG (PO en ISO).
3. Directeuren en Informatie managers.
4. CIO / Directeur IT

Wat is er nodig om effectief privacy en security in te richten?

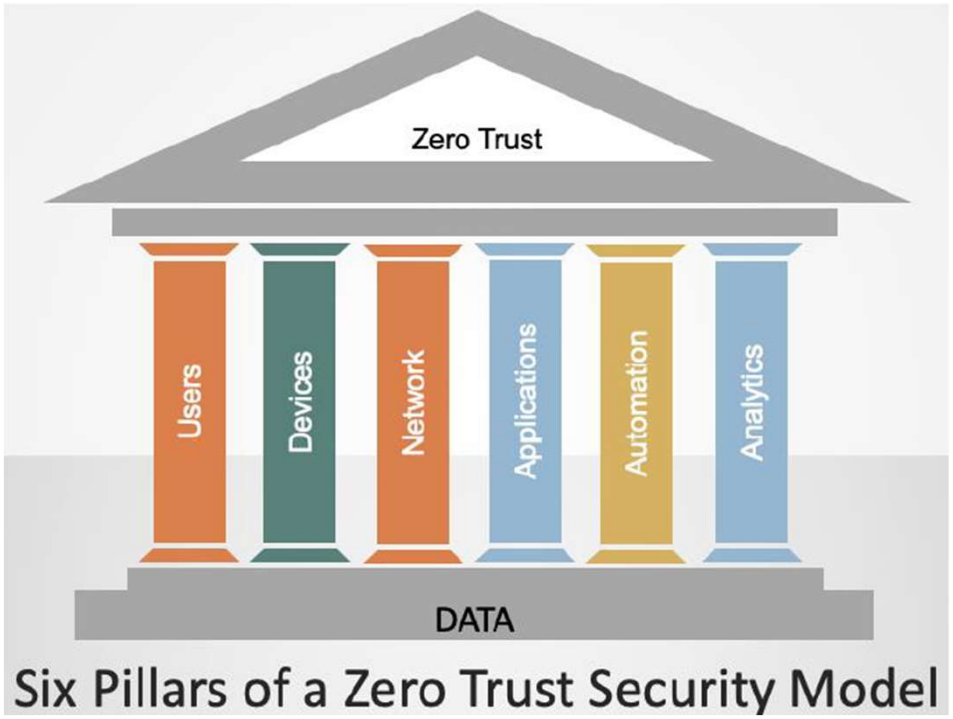
1. Eigenaarschap, risicomanagement, maatregelverantwoordelijke.
2. Verplichte training omtrent rol gebaseerde risico‘s.
3. IAM met inzicht wie er bij info kan, mag en is geweest.
4. Dataclassificatie, logging en monitoring.

Wie moet het onderstaande inrichten?



1. Gemandateerde zelf.
2. CIO / directeur IT.
3. Enterprise (Security) Architect.
4. CISO / FG

9 Kent u het Zero Trust model / aanpak?



Six Pillars of a Zero Trust Security Model

1. Ja
2. Nee
3. Ja we zijn dit aan het implementeren
4. Ja we werken zo

Hoe kijkt u aan tegen zwaardere normen?

1. Doe maar wat nu moet. We hebben al genoeg werk.
2. Nog niet over nagedacht.
3. Afhankelijk van business case. goed idee!
4. Werk altijd al zo.