

Ervaringen uit het MKB



informatiebeveiliging
ZORG ZUID

Informatiebeveiliging

Ir. Gilbert van Zeijl (CISM)
g.vanzeijl@zorgzuid.nl

Informatiebeveiliging Zorg Zuid

- Gecertificeerd security officer
- > 20 jaar ICT ervaring
- >15 jaar ervaring in de zorg
- Informatie kwaliteit en veiligheid
- Privacy
- IT Risk management
- IT auditor



- SAAS Leveranciers
- Zorg (Care & cure)
- Medisch wetenschappelijk onderzoek



MKB overzicht

99% van de bedrijven binnen de marktsectoren is een mkb'er

61% van het bbp op conto van het mkb

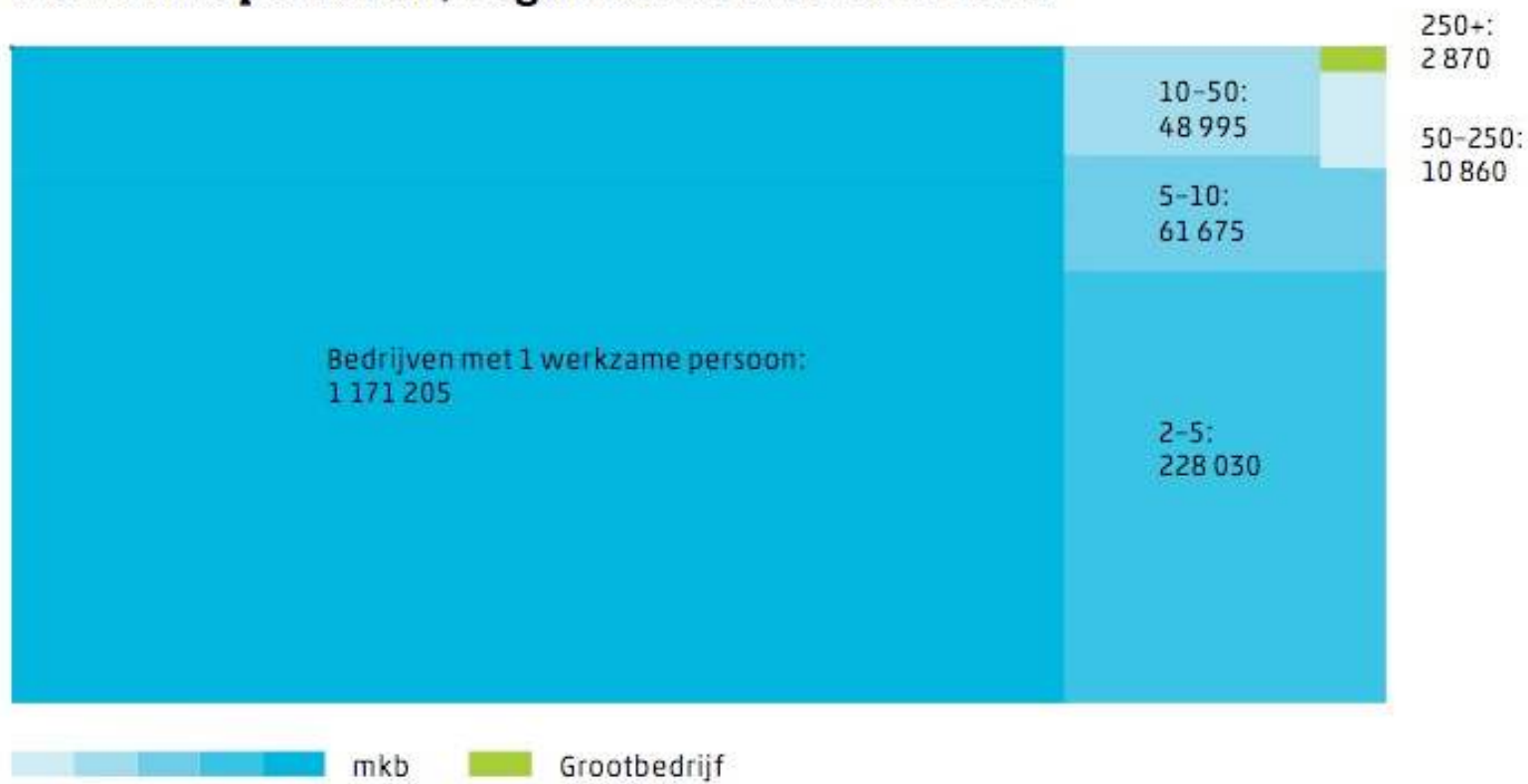
70% werkzame personen marktsector in mkb

Bron: De Staat van het MKB 2015; CBS



MKB overzicht

werkzame personen, begin vierde kwartaal 2015



Bron: De Staat van het MKB 2015; CBS



MKB overzicht

MKB in beeld

Het midden- en kleinbedrijf bestaat uit ondernemingen met maximaal **250 werknemers**. Van alle Nederlandse bedrijven valt **96% in deze categorie**.



**MICRO
ONDERNEMING**
< 10 werknemers
omzet van
€ 700K



**KLEINE
ONDERNEMING**
< 50 werknemers,
omzet van
€ 12 miljoen



**MIDDELGROTE
ONDERNEMING**
< 250 werknemers
omzet van
€ 40 miljoen

Bron: MKB in beeld (MKB servicedesk.nl)

MKB overzicht

werkgelegenheid in mkb

In de periode 2011–2013 is het aantal mensen dat werkzaam is in het mkb met ongeveer 34 duizend afgenomen. Weliswaar kwamen er veel nieuwe bedrijven bij, maar niet elk bedrijf neemt werknemers in dienst. In 2010 waren er 343 duizend mkb-bedrijven die als werkgever actief waren. In de periode 2010–2013 kwamen daar nog eens ruim 45 duizend bedrijven bij. Maar er stopten ook 88 duizend bedrijven met het werkgeverschap, zodat in 2013 er in totaal nog 300 duizend werkgevers in het mkb over waren.

Bij bijna de helft van de bedrijven met personeel kromp het personeelsbestand in de periode 2010–2013, terwijl bij een derde het aantal werknemers in die jaren toenam; 17 procent van de bedrijven met personeel bleef in omvang gelijk. Het overgrote deel van de bedrijven die startten in 2010 is na drie jaar niet

Bron: De Staat van het MKB 2015; CBS



Samenvattend: MKB is

- Grote markt
- Grotendeels kleine bedrijven >50 medewerkers



Ervaring in MKB

Informatiebeveiliging en privacy bescherming

Propositie

- Deeltijd Information Security & Privacy Officer
- Inrichting ISO27001/ NEN7510
- Begeleiding naar certificering

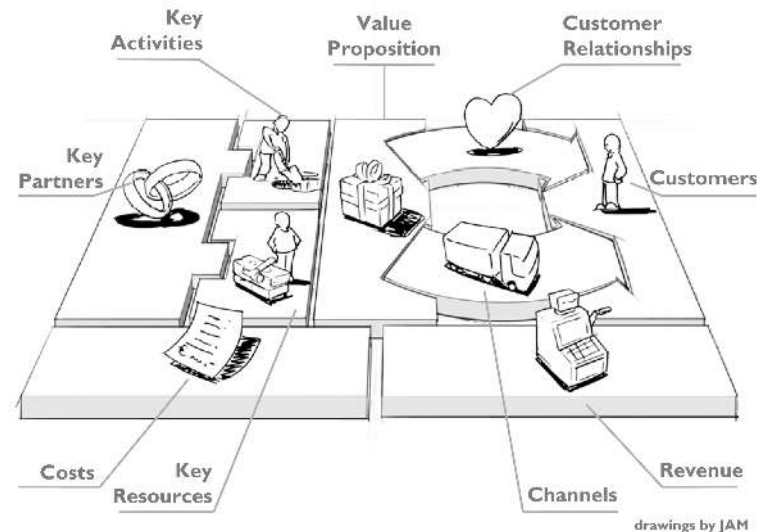


Een bedrijf met bijzondere identiteit Maar met standaard risico's

Branche specifiek

- Key activities
- Key resources
- Kostenstructuur
- Bedrijfsrisico's
- Informatie- en privacyrisico's
- Maatregelenkader

Bedrijfscontext



MKB risico's (ervaring)

- Compliance leidt tot bureaucratie.
 - Gevaar voor cultuur, innovatie, goede medewerkers gaan lopen.
- Specialistisch personeel, moeilijk te krijgen
 - Key resource. Essentieel voor voortbestaan bedrijf.
- Compliance aantonen
 - We doen de goede dingen maar aantoonbaar maken is lastig.
- Verantwoording ICT supply chain
 - Hosting organisaties zijn lastig te controleren.
 - Als MKB heb je weinig te vertellen richting ICT host/housing partner

ISO27001 : 2013

Past beter bij MKB dan versie 2005

2013

- Meten is weten: SMART doelstellingen, effectiviteit meten.
- Organisatie context
 - Business value
- ISO High Level structure
 - Integratie met andere standaarden.
- Outsourcing

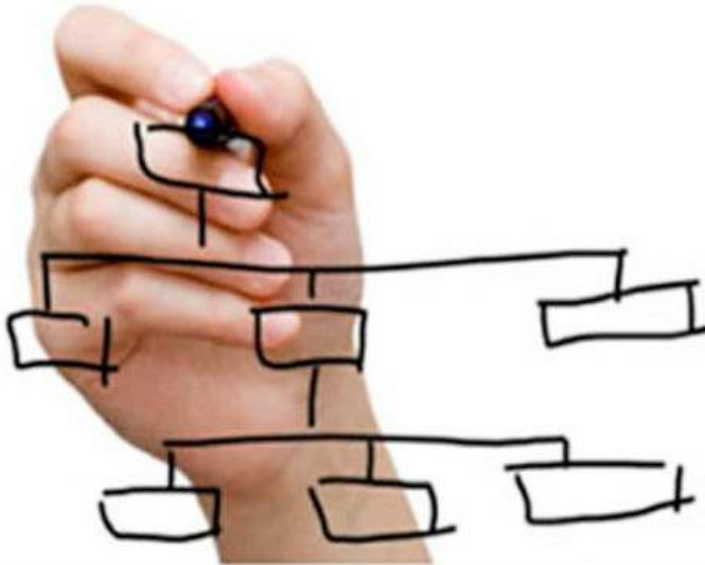
2005

- Hoe in control: handboeken, procedures, etc.
- PDCA nadruk



Uitdaging: Directie is in Control, Maar hoe toon je dat aan?

Organisatiestructuur



Ervaring

- Eenvoudige structuur
- Korte afstand directie tot werkvloer.
- Vertrouwen!
 - Social control.
- Handen uit de mouwen
- Geen bureaucratie



Aantonen doelen = auditing In het klein bedrijf

Bruikbaar

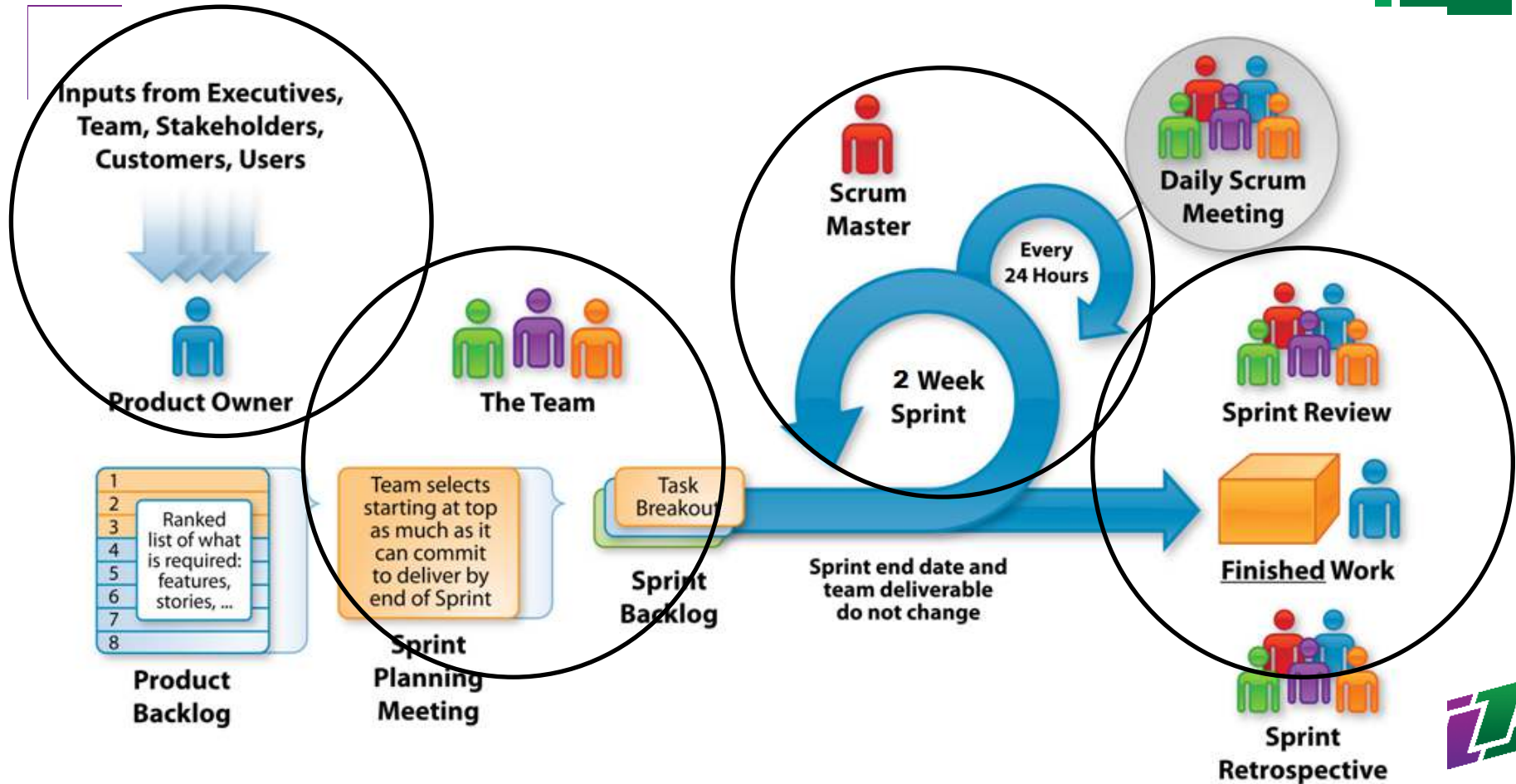
- Interview
 - Gedrag
- Observatie
 - Technische maatregel
 - autorisaties
- Gebruikte registers
 - Support
 - Backlog
 - CRM

Minder bruikbaar

- Procedure
- Handboek
- Formulieren
- Checklists



Agile ontwikkelen



MKB beleidsdoelstellingen

voorbeelden uit de praktijk

- Wij werken op basis van **vertrouwen** naar klanten, medewerkers en leveranciers. Wij gaan er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
- De doelstellingen en beheersmaatregelen van de norm ISO27002 en de privacy richtsnoeren van het CBP vormen, voor zover zij bijdragen aan de informatiebeveiliging het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een **bedrijfseconomische** afweging.
- beschouwt **computercriminaliteit** als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken..

ICT Outsourcing Uitdaging

Verantwoording in de supply chain

Opdrachtgever (MKB)

- Prijs & Kwaliteit
- Uitbesteden taken & risico's
- Gedwongen afname van standaard dienst.
- Kan overstapen naar ander hosting / housing partij

Leverancier

- Geen gedoe
- Rekening op tijd betaald krijgen
- Wil standaard dienstverlening leveren
- Volume

Hoe verantwoordelijk wij informatiebeveiliging naar elkaar?



Oproep:

Verantwoording in de supply chain.

- Hoe doe je dat?
- Graag een spreker die verantwoording veiligheid regelt vanuit Hosting bedrijf.

