



Dynamisch risicomanagement

eenvoudig met behulp van GRC**control**





Mike de Bruijn
Product Owner

- Inleiding
 - Over CompLions
- GRCcontrol management software
 - Risicomanagement
 - Uitdagingen
 - Dynamisch risicomanagement
 - Analyses
 - Risicobehandelingen
 - Maatregelencyclus
 - Governance
 - Compliance

CompLions

Onze doelstelling

Het ondersteunen van organisaties
in het efficiënt en effectief beheersen van
Governance, risico en compliance behoeften

door middel van
het borgen van managementsystemen, normen en standaarden

met behulp van
managementsoftware en ondersteunende (advies)diensten.

Portfolio

Adviesdiensten

Business Consultancy

- Privacy- & Informatiebeveiliging
- Business Continuity
- Kwaliteits- en milieumanagement
- Certificering (ISO 27001, NEN7510, BIG, ISO 22301, etc.)
- Interne audits & risico assessments

Software Consultancy

- Installatie en implementatie

**Project-
doelstellingen**

Management software

GRCcontrol suite

- Basis
- Standaard
- Modules
 - IRM (IT Risk Man.)
 - IMM (Incident Man.)
 - DMS (Doc. Man.)
 - PIA
 - ERM
 - AAM

Training

- Basis GRC
- Expert GRC

**Inzicht &
controle t.b.v.
G – R – C**

Operationele ondersteuning

Abonnementen

- Security Officer as a Service
- Security Manager as a Service
- IT Audit as a Service (IAS)
- GRCcontrol Functioneel beheer as a Service

Ontzorging

**S
E
C
T
O
R
E
N**

- **Zorg**
- **ICT & telecom**
- **Publieke Sector**
- **Accountancy**
- **Handel & diensten**
- **Financieel**

GRCcontrol management software

- **Doelstelling**
 - **Eén geautomatiseerd managementsysteem**
 - Voor beheersing (**Governance & Riskmanagement**)
 - Inzicht in het voldoen aan (**Compliance**)
 - normenkader(s)
 - managementsystemen (certificering)
 - wet- en regelgeving

- **Van ISMScontrol naar GRCcontrol (1)**
 - **Van vakinhoudelijke gebruikers met proceskennis van een ISMS naar brede gebruikerskring**
 - Vereist eenvoudigere management functionaliteit en workflows om complexe processen te beheersen.
 - **Meer gebruikers buiten het ISMS (security) domein:**
 - Kwaliteitsmanagement
 - Business continuïteit
 - Milieumanagement
 - Procesmanagement
 - Etc.
 - Vereist eenvoud in gebruik, schermen en taakafhandeling

- **Van ISMScontrol naar GRCcontrol (2)**
 - **Van ISMS bereik naar Governance, Riskmanagement en Compliance**
 - Beheersen van veelvoud van managementsystemen
 - Certificering
 - Assurance
 - Vereist enerzijds complexe functionaliteit maar eenvoudiger management functies en workflows om complexe brede materie en grote diversiteit aan gebruikers(niveaus) te beheersen.

Risicomanagement De uitdagingen!

- **Uitdagingen**
 - **Organisatiedoelstellingen veranderen door:**
 - ambities
 - wijzigingen in bijvoorbeeld wet- en regelgeving
 - markten
 - etc.

Door veranderingen ontstaan kansen (doelstellingen), maar ook risico's.

- **Uitdagingen**

- **Inzicht nodig in risico's om:**

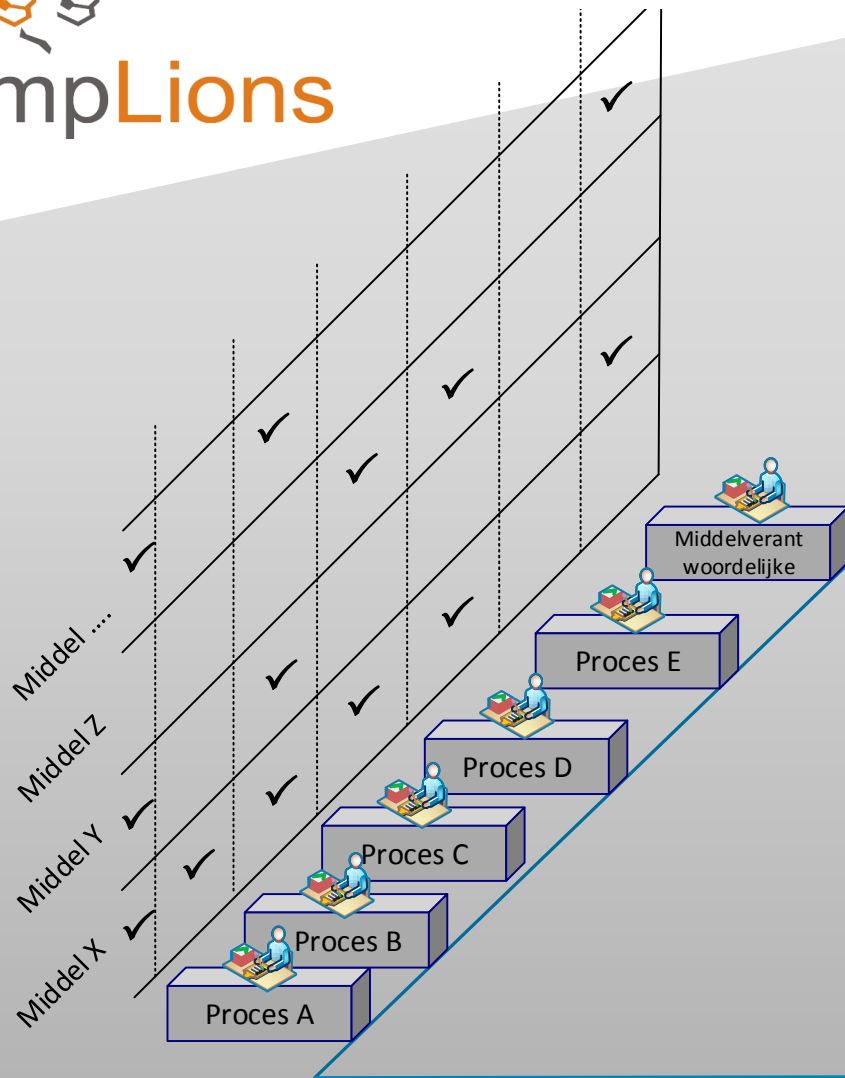
- Risico's te nemen, te verminderen, te vermijden of over te dragen

- **Input komt uit:**

- uit de eigen organisatie
 - en/of externe(keten)partijen
 - systemen

- **Uitdagingen**
 - **Actueel inzicht en grip behouden over:**
 - Assetrisico's
 - Procesrisico's & doelstellingen
 - Organisatierisico's & doelstellingen

Risicomanagement – De uitdaging



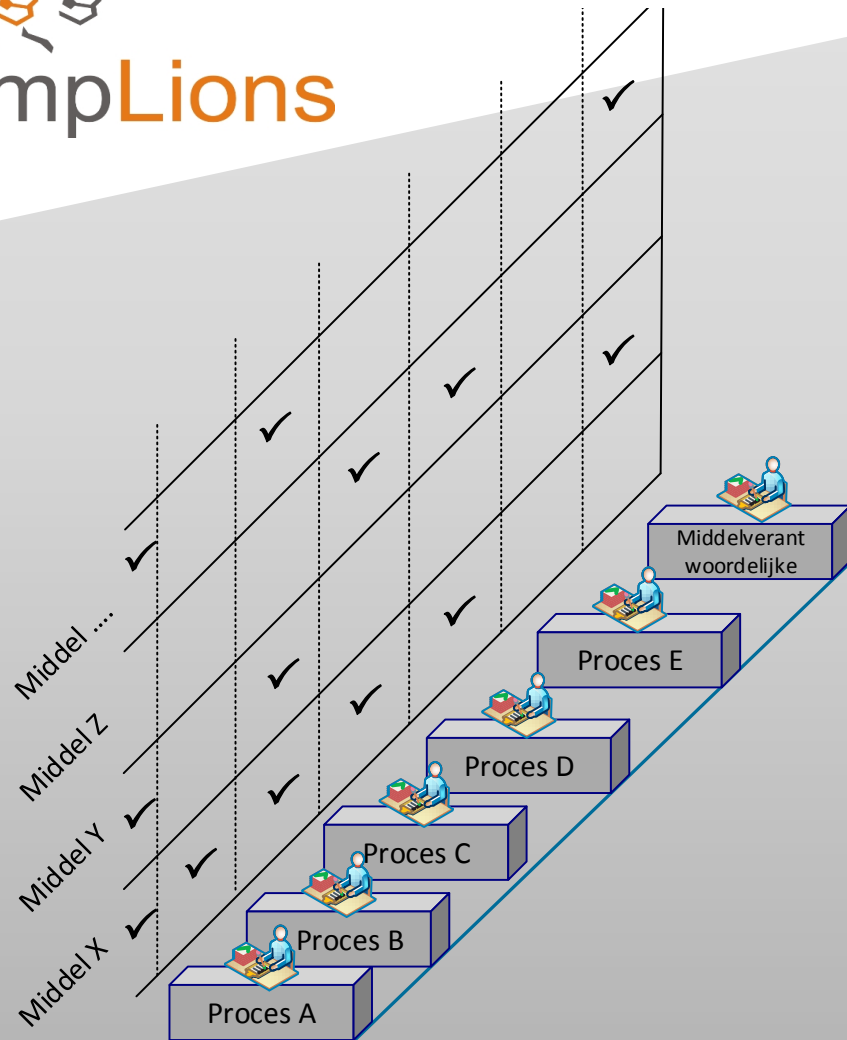
- Grip op middelrisico's

- ICT middelen
- Applicaties
- Gegevens
- Gebouwen
- etc.

Risicomanager



Risicomanagement – De uitdaging



- Grip op middelrisico's

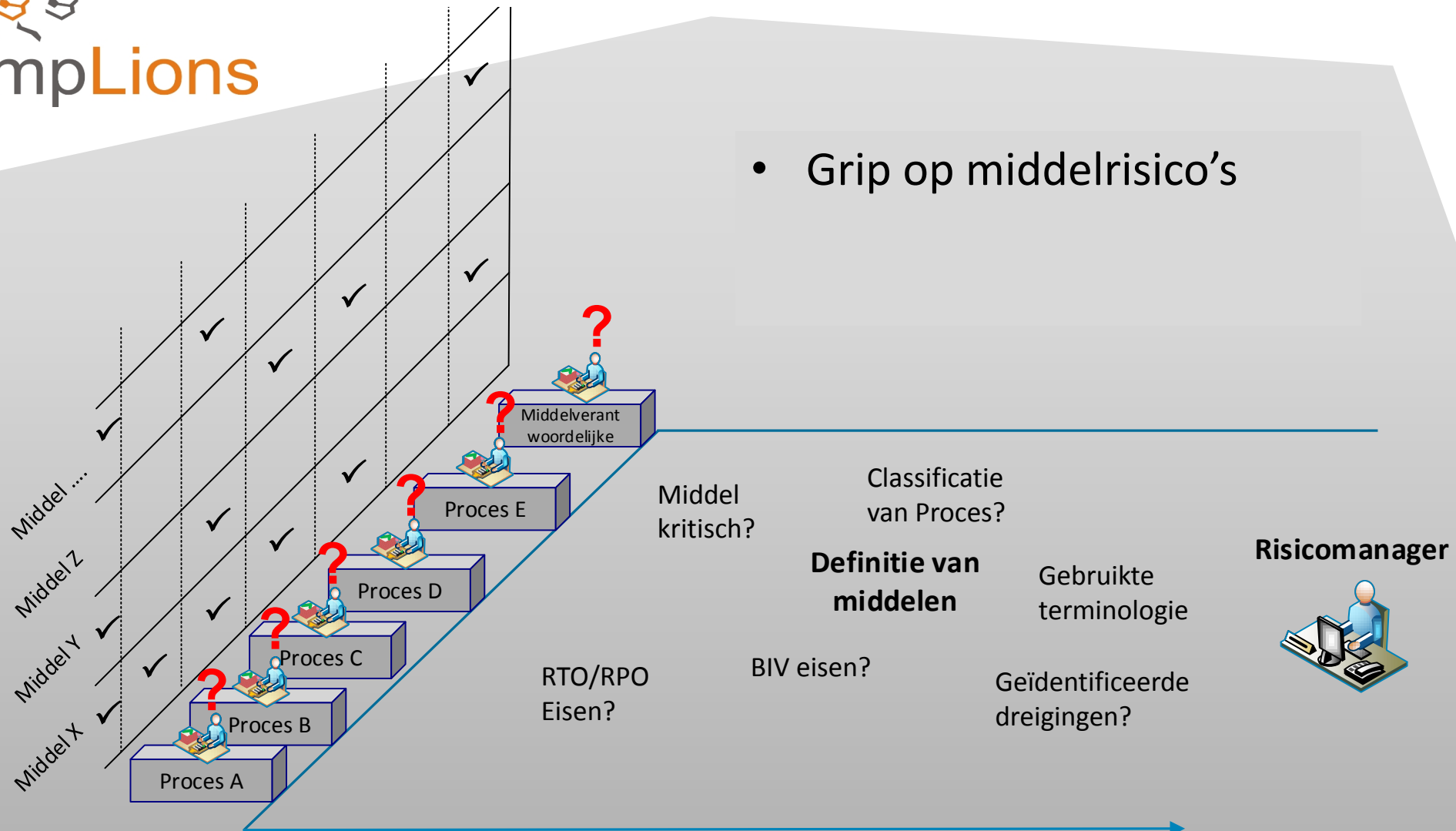
- ICT middelen
- Applicaties
- Gegevens
- Gebouwen
- Etc.

Risicomanager



- Organisatie- /personele wijzigingen
- Materie wordt als complex ervaren

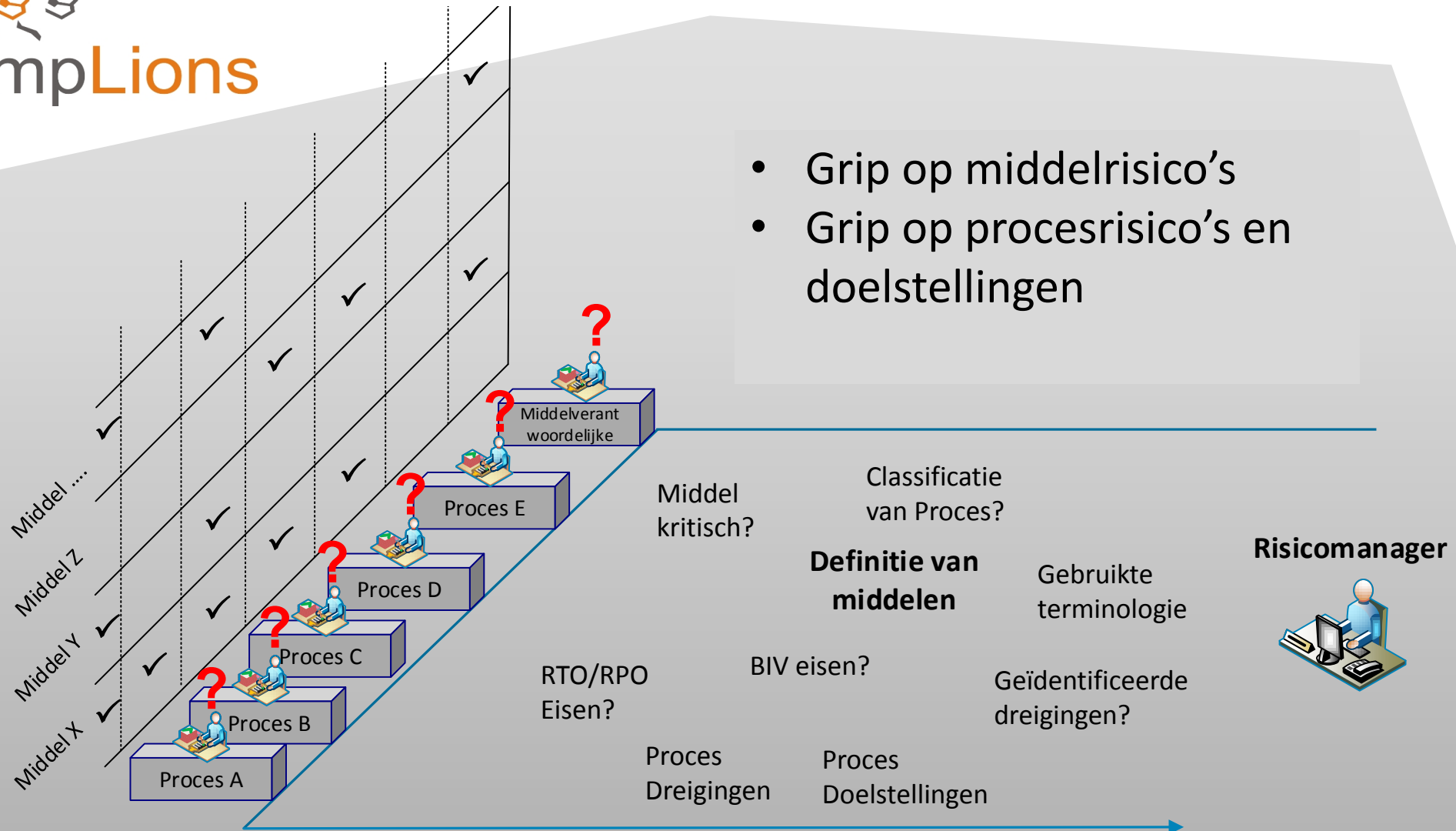
- Grip op middelrisico's



- Organisatie- /personele wijzigingen
- Materie wordt als complex ervaren

Risicomanagement – De uitdaging

- Grip op middelrisico's
- Grip op procesrisico's en doelstellingen



- Organisatie- /personele wijzigingen
- Materie wordt als complex ervaren

- Grip op middelrisico's
- Grip op procesrisico's en doelstellingen

Moeilijke materie, moeilijk proces!
Waar vind ik eerdere analyses?

Middel
Middel X

Proces A

Proces B

Proces C

Kwetsbaarheden analyse middelen

Kwetsbaarheden analyse proces

Business impact analyses

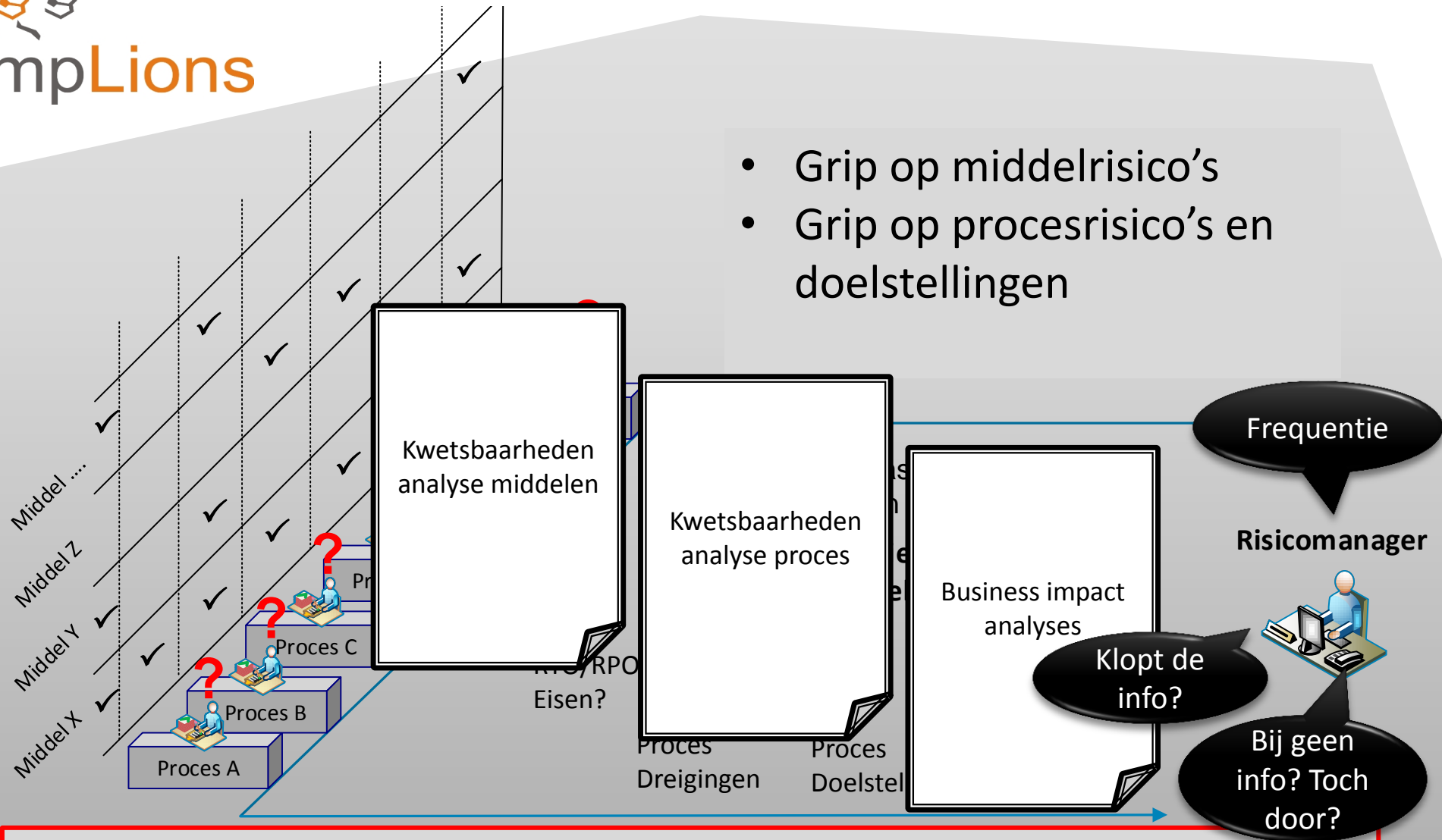
Risicomanager



- Organisatie- /personele wijzigingen
- Materie wordt als complex ervaren

Risicomanagement – De uitdaging

- Grip op middelrisico's
- Grip op procesrisico's en doelstellingen



- Organisatie- / personele wijzigingen
- Materie wordt als complex ervaren

Dynamisch risicomanagement beheersing met GRCcontrol

Dynamisch risicomanagement beheersing met GRCcontrol

Plan
middel- / proces analyses

- BIA's
- DA's

Plan
risicobehandeling

- Per middel
- Per proces

Maatregelcyclus
Van Plan naar
implementatie (Do)
voor verdere
Governance en
Compliance (Check en
Act)



Governance ▾

Risicomanagement ▾

Compliance ▾

Rapportages

Incidenten

Beheer ▾

Piet Officer

Instellingen ▾

Afmelden

Welkom bij GRCcontrol

GRCcontrol beheer

Organisatie

Brontabellen »

Instellingen middelanalyse

Geef de geldigheidsduur op van middelanalyses *

365 Dagen

De gebruiker kan de aanmaakdatum bepalen

Ja ☐

De gebruiker kan de geldigheidsdatum bepalen

Ja ☐

Een dreiginganalyse is *

☐ Verplicht

☐ Optioneel

☒ Optioneel, maar verplicht als één van de BIV-scores gelijk is of hoger dan:

3

☐ Uitsluitend

Middelbehandelingen

Geef de geldigheidsduur op voor de middelbehandelingen *

365 Dagen

Verlooptermijn middelbehandelingen instelbaar?

Ja ☐

Instellingen procesanalyse

Geef de geldigheidsduur op van procesanalyses *

365 Dagen

De gebruiker kan de aanmaakdatum bepalen

Ja ☐

De gebruiker kan de geldigheidsdatum bepalen

Ja ☐

Procesbehandelingen

Geef de geldigheidsduur op voor de procesbehandelingen *

365 Dagen

Verlooptermijn procesbehandelingen instelbaar?

Ja ☐

Waarde	Impact*	Betekenis*
1	Niet significant	Verwaarloosbaar
2	Laag	Beperkte problemen voor het behalen doelstelling / niet zichtbaar buiten organisatie
3	Midden	Problemen voor het behalen doelstelling / mogelijk zichtbaar buiten organisatie
4	Hoog	Behalen doelstelling ernstig bedreigd / image- en reputatieschade in de markt
5	Catastrofaal	Continuïteit loopt gevaar

Heatmaps dreigingen

Heatmap objectwaarde

Hoog

Selecteer risicoklassekleur

Extreem



Klik in de heatmap om de kleur toe te passen

Kans	5	15	30	45	60	75
	4	12	24	36	48	60
	3	9	18	27	36	45
	2	6	12	18	24	30
	1	3	6	9	12	15
		1	2	3	4	5
		Impact				

Heatmaps BIV waardering middelen

Heatmap asset classificaties

Hoog

Selecteer risicoklassekleur

Laag



Klik in de heatmap om de kleur toe te passen

Beschikbaarheid		0				1				2				3			
Integriteit		0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
Vertrouwelijkheid	3	9	12	15	18	12	15	18	21	15	18	21	24	18	21	24	27
	2	6	9	12	15	9	12	15	18	12	15	18	21	15	18	21	24
	1	3	6	9	12	6	9	12	15	9	12	15	18	12	15	18	21
	0	0	3	6	9	3	6	9	12	6	9	12	15	9	12	15	18

BIV hulpvragen

Beschikbaarheid

Volgnr.

Vraag*

1

management besluiten negatief beïnvloed kunnen worden bij uitval?



2

orders/contracten verloren kunnen worden als gevolg van het niet beschikbaar zijn?



3

fraude of misbruik van goederen en/of fondsen kunnen voorkomen bij uitval?



4

imago, vertrouwen en reputatie bij klanten, publiek, of aandeelhouders- of leveranciersloyaliteit schade lijden bij uitval?



5

additionele kosten ontstaan (bijv. overwerk, inhuur etc.) bij uitval?



Plan
middel- / proces analyses

- BIA's
- DA's

Plan
risicobehandeling


- Per middel
- Per proces

Maatregelcyclus

Van Plan naar
implementatie (Do)
voor verdere
Governance en
Compliance (Check en
Act)

We zijn bij GRCcontrol

[PLAN](#) »[DO](#) »[CHECK](#) »[ACT](#) »



Governance ▾

PLAN » Nieuwe algemene taak

DO » Implementaties plannen / uitrollen

CHECK » Controles op maatregelen plannen / uitrollen

ACT » Audits »

Risicomanagement ▾

Compliance ▾

Rapportages

Incidenten

Beheer ▾

Piet Officer

Instellingen ▾

Afmelden

Analyses »

Mijn middelen

Mijn processen

Gebruiker ziet altijd op dezelfde plek alle 'verlopen' of 'nieuwe' analyses die uitgevoerd moeten worden.

[Governance](#) ▾[Risicomanagement](#) ▾[Compliance](#) ▾[Rapportages](#)[Incidenten](#)[Beheer](#) ▾[Piet Officer](#)[Instellingen](#) ▾[Afmelden](#)

Uitvoeren middelanalyses

Toon alle middelen ☐ Nee

Geldig tot	Status	Actie	Middelnaam	Bron	Middeleigenaar	Proceseigenaar
	In uitvoering	Bewerken	ISMScontrol		Piet Officer	
	In uitvoering	Bewerken	ISMScontrol	Audit management	Piet Officer	Audrey Audit
		Nieuw	ISMScontrol	Security Management	Piet Officer	Piet Officer

1

10

items per pagina

items 1 - 3 van 3

[Governance](#)[Rapportages](#)[Incidenten](#)[Beheer](#)[Sofie Proces](#)[Instellingen](#)[Afmelden](#)

Formulier Business impact analyse

Middel: Personeelsdossier

Gebruik hulpvragen

☒ Ja

Middel is kritisch voor dit proces

☒ Ja

Aanmaakdatum

3-11-2015



Ingevuld door

Sofie Proces

Maximaal toegestane hersteltijd (RTO)

Uren

Maximaal toegestane dataverlies (RPO)

Uren

Geldig tot

2-11-2016



Status

— Hulpvragen voor beschikbaarheid

Volg nr.	Vraag	0	1	2	3
0	Welk niveau is nodig om te voorkomen dat managementbesluiten negatief beïnvloed kunnen worden bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	Welk niveau is nodig om te voorkomen dat orders/contracten verloren kunnen gaan als gevolg van uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	Welk niveau is nodig om te voorkomen dat fraude of misbruik van goederen en/of fondsen plaats kan vinden bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	Welk niveau is nodig om te voorkomen dat imago, vertrouwen en reputatie bij klanten, publiek, of aandeelhouders- of leveranciersloyaliteit schade lijden bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	Welk niveau is nodig om te voorkomen dat additionele kosten ontstaan (bijv. overwerk, inhuur etc.) bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	Welk niveau is nodig om te voorkomen dat wettelijke-, reglementaire- of contractuele verplichtingen verbroken kunnen worden bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	Welk niveau is nodig om te voorkomen dat het moreel van het personeel aangetast kan worden bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	Welk niveau is nodig om te voorkomen dat de bedrijfsvoering/werkzaamheden niet worden verstoord bij uitval?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[← Terug](#)[Naar optionele dreiginganalyse →](#)[Analyse afronden ✓](#)

[Governance](#)[Risicomanagement](#)[Compliance](#)[Rapportages](#)[Incidenten](#)[Beheer](#)[Piet Officer](#)[Instellingen](#)[Afmelden](#)

Dreigingenanalyse

Middel: ISMScontrol

Aanmaakdatum*

28-10-2015



Geldig tot*

27-10-2016



Ingevuld door

Piet Officer

Dreigingenset

CompLions Migratie

Assesment dreiging

Relevant?

Ja



Software storing

[Kwetsbaarheid invullen / tonen](#)

Kans

1 2 3 4 5



Impact

1 2 3 4 5



RK

20

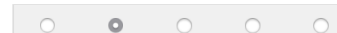
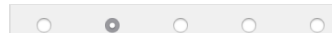
Relevant?

Ja



Geen toegang tot gebouwen of ruimtes

[Kwetsbaarheid invullen / tonen](#)



4

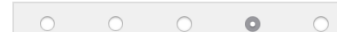
Relevant?

Ja



Sabotage door medewerkers

[Kwetsbaarheid invullen / tonen](#)



12

Terug

Terug

Analyse afronden



**Plan
middel- / proces Analyses**

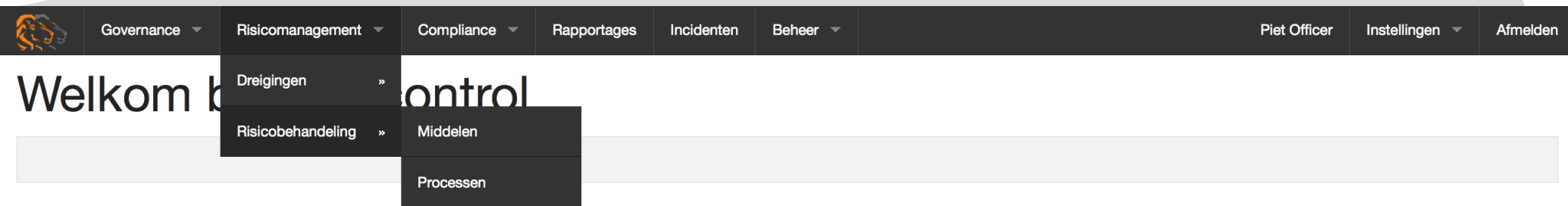
- BIA's
- DA's

**Plan
risicobehandeling**

- Per middel
- Per proces

Maatregelcyclus

Van Plan naar
implementatie (Do)
voor verdere
Governance en
Compliance (Check en
Act)





Risicomanager ziet altijd op dezelfde plek alle 'verlopen' of 'nieuwe' behandelingen automatisch

[Governance](#)[Risicomanagement](#)[Compliance](#)[Rapportages](#)[Incidenten](#)[Beheer](#)[Piet Officer](#)[Instellingen](#)[Afmelden](#)

Risicobehandeling middelen

Toon alle middelen ☐ Nee

Middel	Verantwoordelijke	Acceptant	Datum laatste be...	Nieuw risico aan...	Status behandeling	Status akkoord	Actie
Middel A	Piet Officer	Audrey Audit	28-10-2015	—	In uitvoering	Open	Bewerken
Arbeidscontract	Sofie Proces	Audrey Audit	28-10-2015		In uitvoering	Open	Bewerken
Personeelsdossier	Sofie Proces	Sofie Proces	28-10-2015		In uitvoering	Geaccordeerd	Bewerken
Samsung Galaxy S10	Piet Officer	Sofie Proces	29-10-2015		Afgerond	Geaccordeerd	Nieuw

10 items per pagina

items 1 - 4 van 4

Risicobehandeling

1 Definitie

2 BIAs beoordelen

3 BIA maatregelen selecteren

4 Accorderen

5 Afronden

Middel

Personeelsdossier

Verantwoordelijke

Sofie Proces

Middeltype

Belangrijke documenten

Titel*

345

Volgnr.

4

Status behandeling

In uitvoering

Behandelaar / risicomanager

Piet Officer

Acceptant*

Sofie Proces

Startdatum

28-10-2015

Behandeling afgerond op



Behandeling baseren op:*

Business impact analyses (BIA)

Ja

☐

Dreiginganalyses (DA)

Nee

☐

Er zijn nieuwe business impact analyses aanwezig

Stapsgewijs proces

[Governance](#)[Risicomanagement](#)[Compliance](#)[Rapportages](#)[Incidenten](#)[Beheer](#)[Piet Officer](#)[Instellingen](#)[Afmelden](#)

Risicobehandeling

[1 Definitie](#)[2 BIA's beoordelen](#)[3 BIA maatregelen selecteren](#)[4 Accorderen](#)[5 Afronden](#)

Middel

Personeelsdossier

Verantwoordelijke

Sofie Proces

Middeltype

Belangrijke documenten

Huidige BIV

Classificatie

Beschikbaarheid

Integriteit

Vertrouwelijkheid

RTO

RPO

Uren

Uren

BIA beoordeling

Classificatie*

Hoog

Beschikbaarheid*

1

Integriteit*

2

Vertrouwelijkheid*

2

RTO

Uren

RPO

Uren

Berekende BIA-risicoklasse:

15

⚠ Let op: De BIA-risicoklasse wijkt af van de hoogste risicoklasse uit de BIA-analyses.

Toelichting

BIA-resultaten procesverantwoordelijken

BIA-resultaten middelverantwoordelijke

Gerelateerde middelen

Toon ook processen zonder ingevulde BIA-analyse

☐ Nee

[Terug](#)

[Volgende stap](#)

Visuele heatmap

Beoordeling dreiging

Hoofdcategorie

STANDARD

Categorie

MAPG

Titel

Ongeautoriseerde toegang tot gegevens

Voor behandeling

Kans

2

Impact

3

Classificatie

Middel

Kans - toelichting

2 - Zeldzaam:

Jaarlijks 5 - 20% kans van optreden

Impact - toelichting

3 - Midden:

Problemen voor het behalen doelstelling / mogelijk zichtbaar buiten organisatie

Impact dreiging voor behandeling op:

Beschikbaarheid

☐ Nee

Integriteit

☒ Ja

Vertrouwelijkheid

☒ Ja

Behandelaanpak

☒ Verminderen

☐ Accepteren

☐ Vermijden

☐ Overdragen / delen



Inzicht in risico's vóór en na de behandeling

Risicobehandeling



Middel

Personeelsdossier

Verantwoordelijke

Sofie Proces

Middeltype

Overige

Te behandelen dreigingen

Dreiging titel	K...	I...	RK voor...	Behandelaanpak	Nieuwe kans	Nieuwe impact	Nieuwe RK
Ongeautoriseerde toegang tot gegevens	2	3	 12	Verminderen	2	3	 12
Ongeautoriseerd gebruik van programma's	3	3	 18	Verminderen	2	2	 8

10 items per pagina items 1 - 2 van 2

Plan
middel- / proces analyses

- BIA's
- DA's

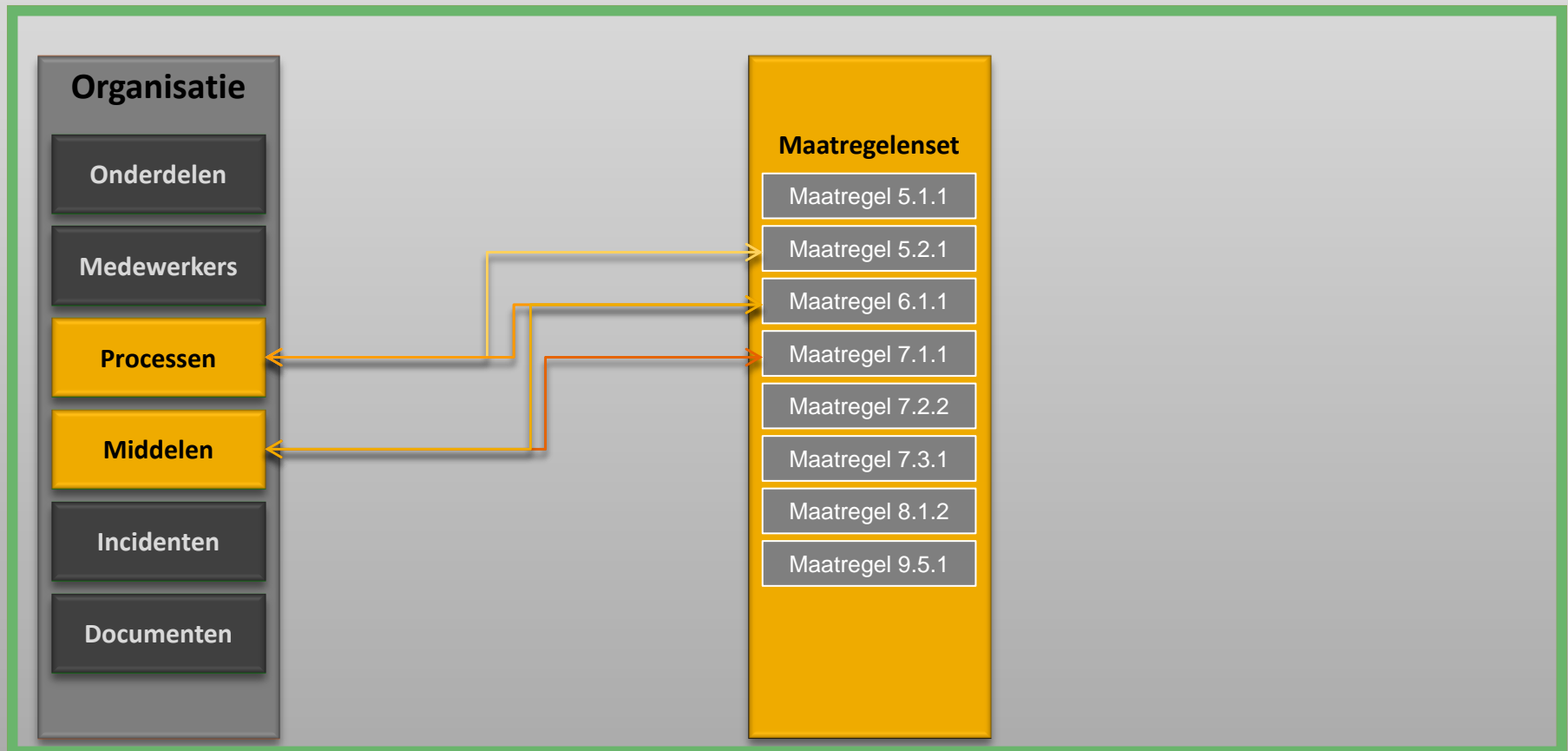
Plan
risicobehandeling

- Per middel
- Per proces

Maatregelcyclus

Van Plan naar
implementatie (Do)
voor verdere
Governance en
Compliance (Check en
Act)

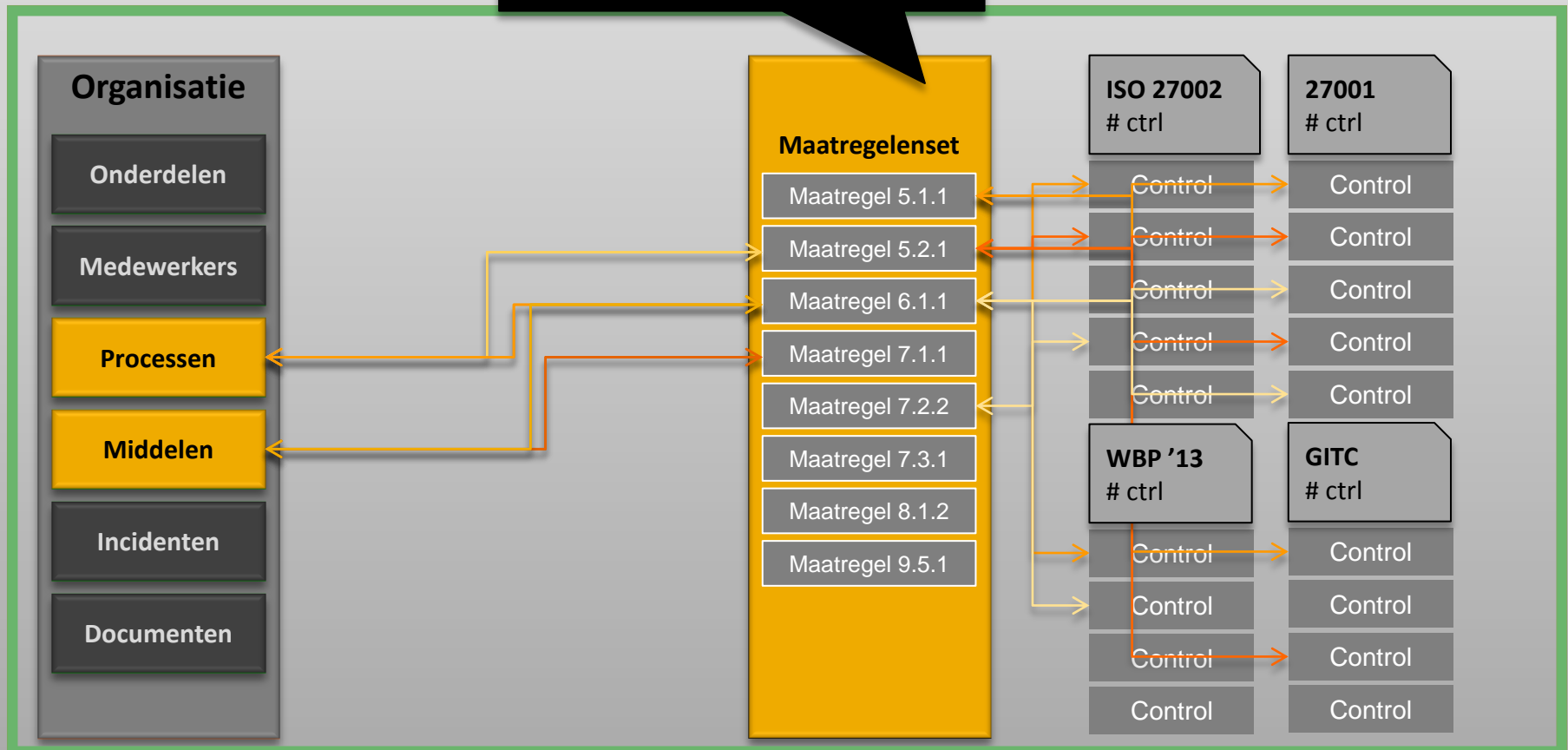
Interne beheersing



Interne beheersing

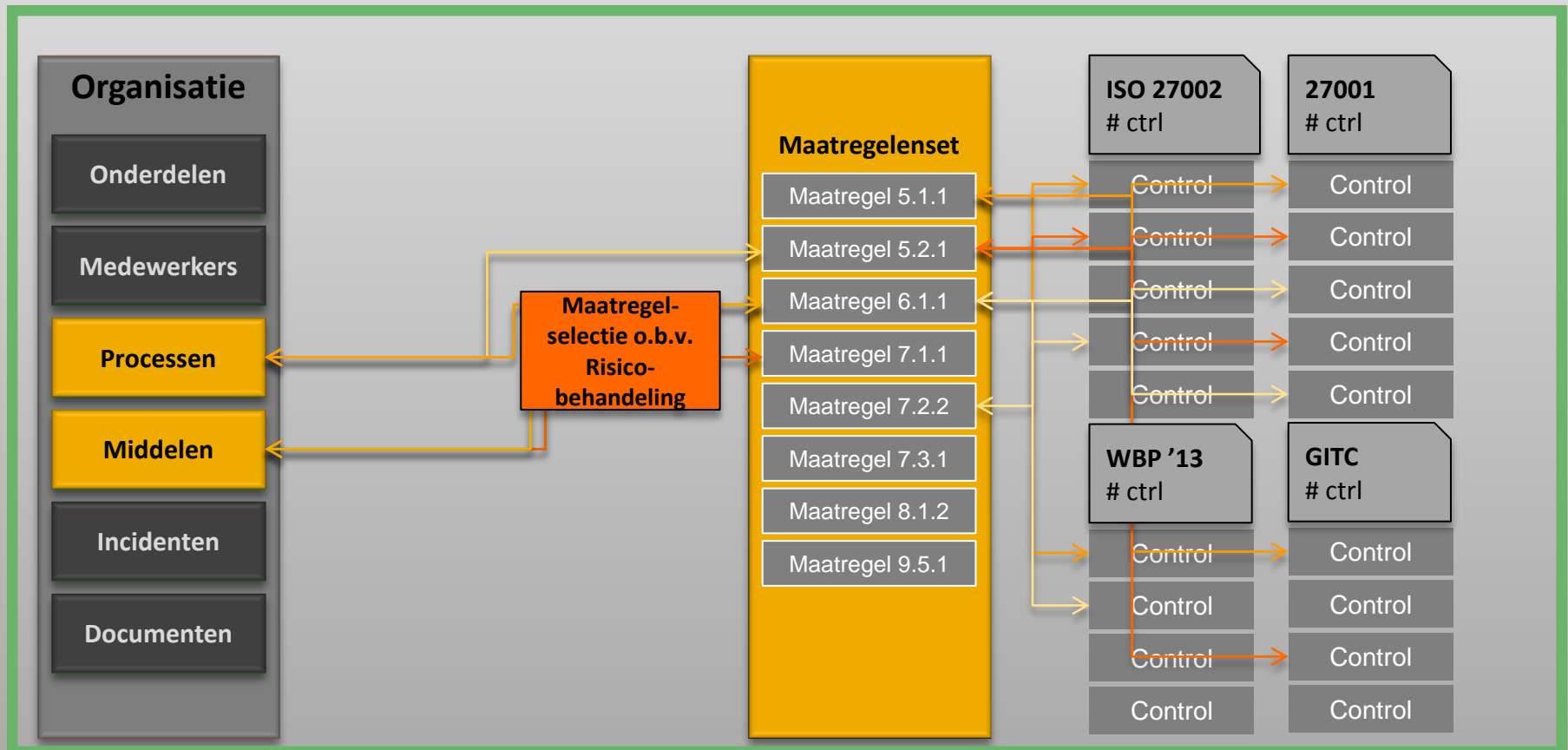
Verzameling van alle
ontdubbelde benodigde
beheersingsmaatregelen

Compliance raamwerk



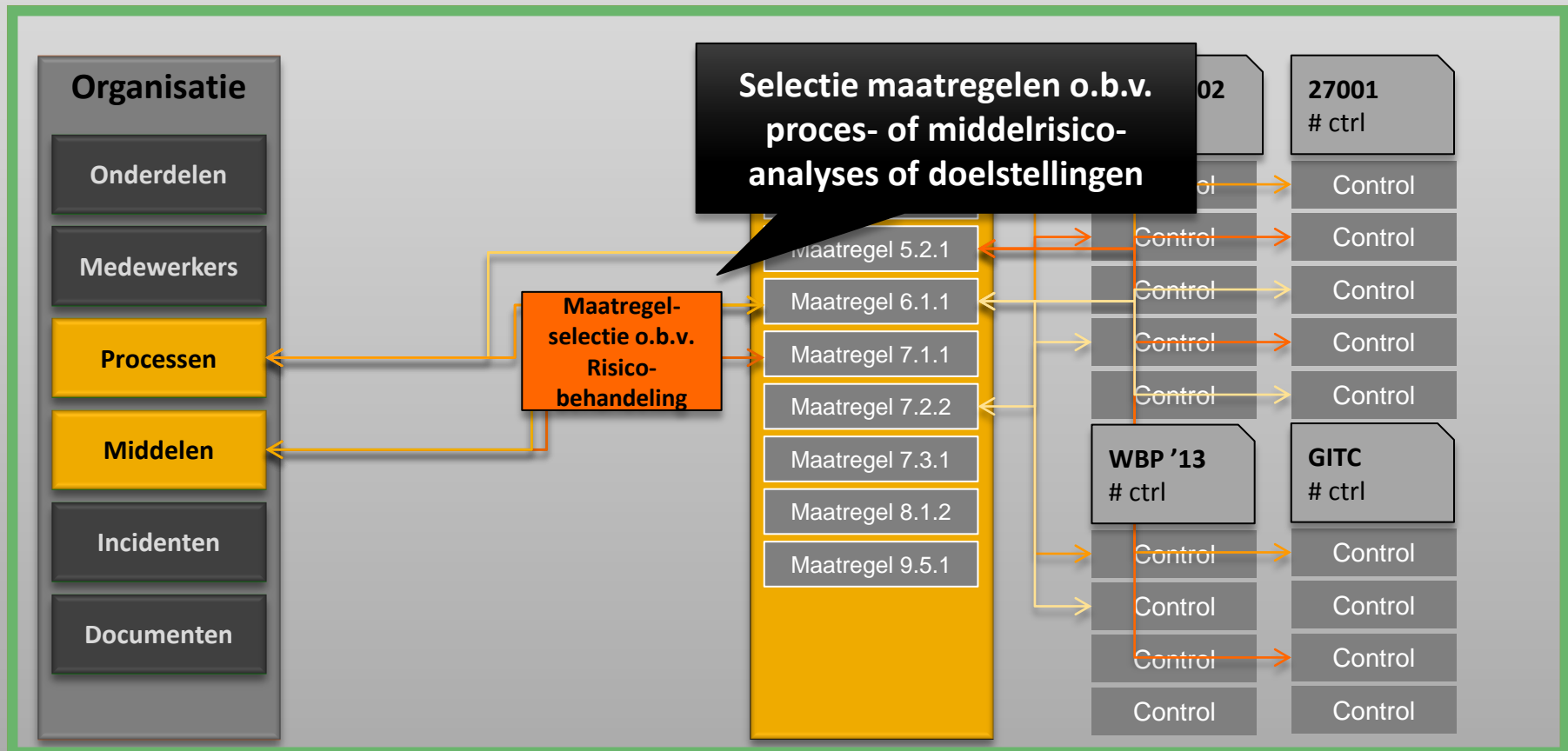
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



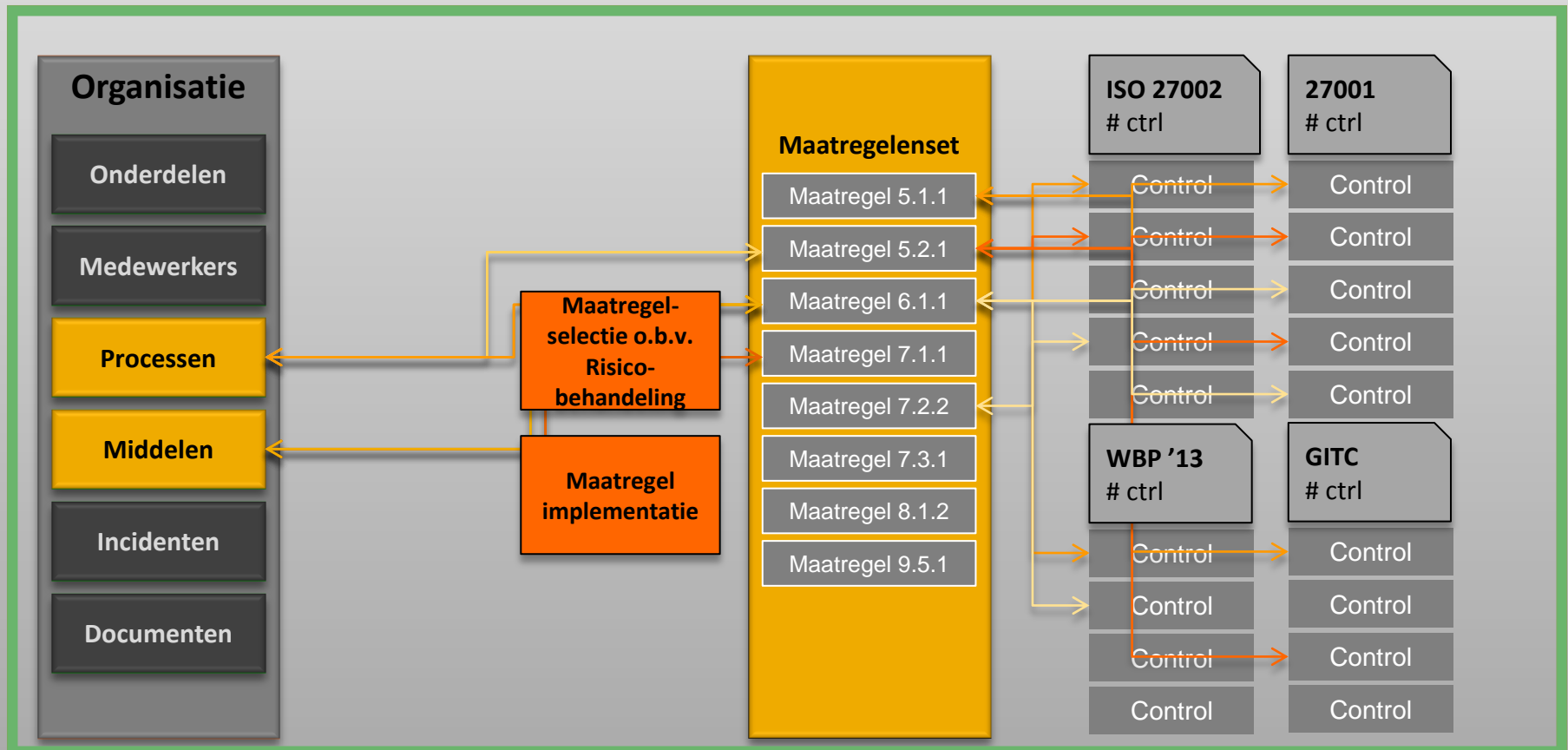
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



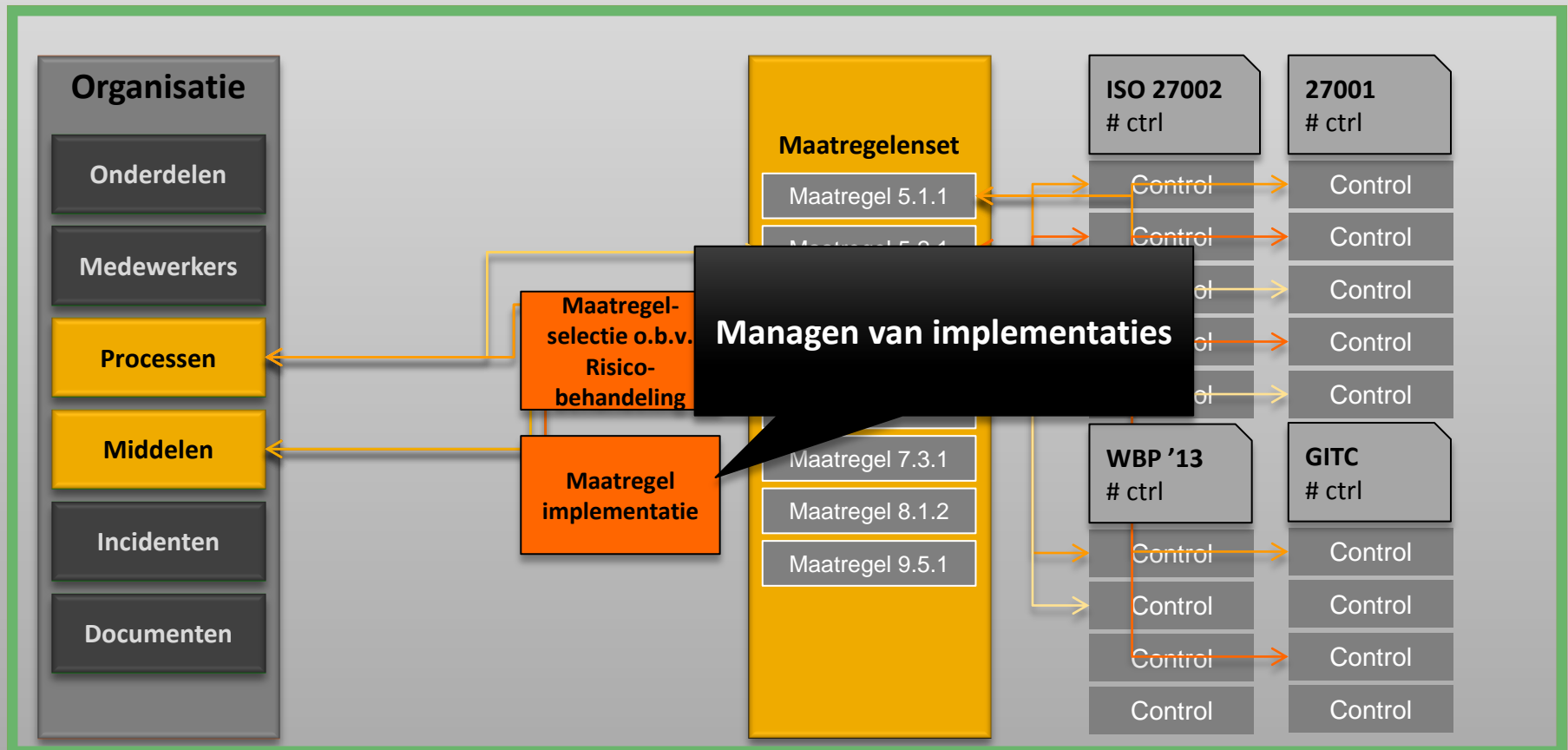
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



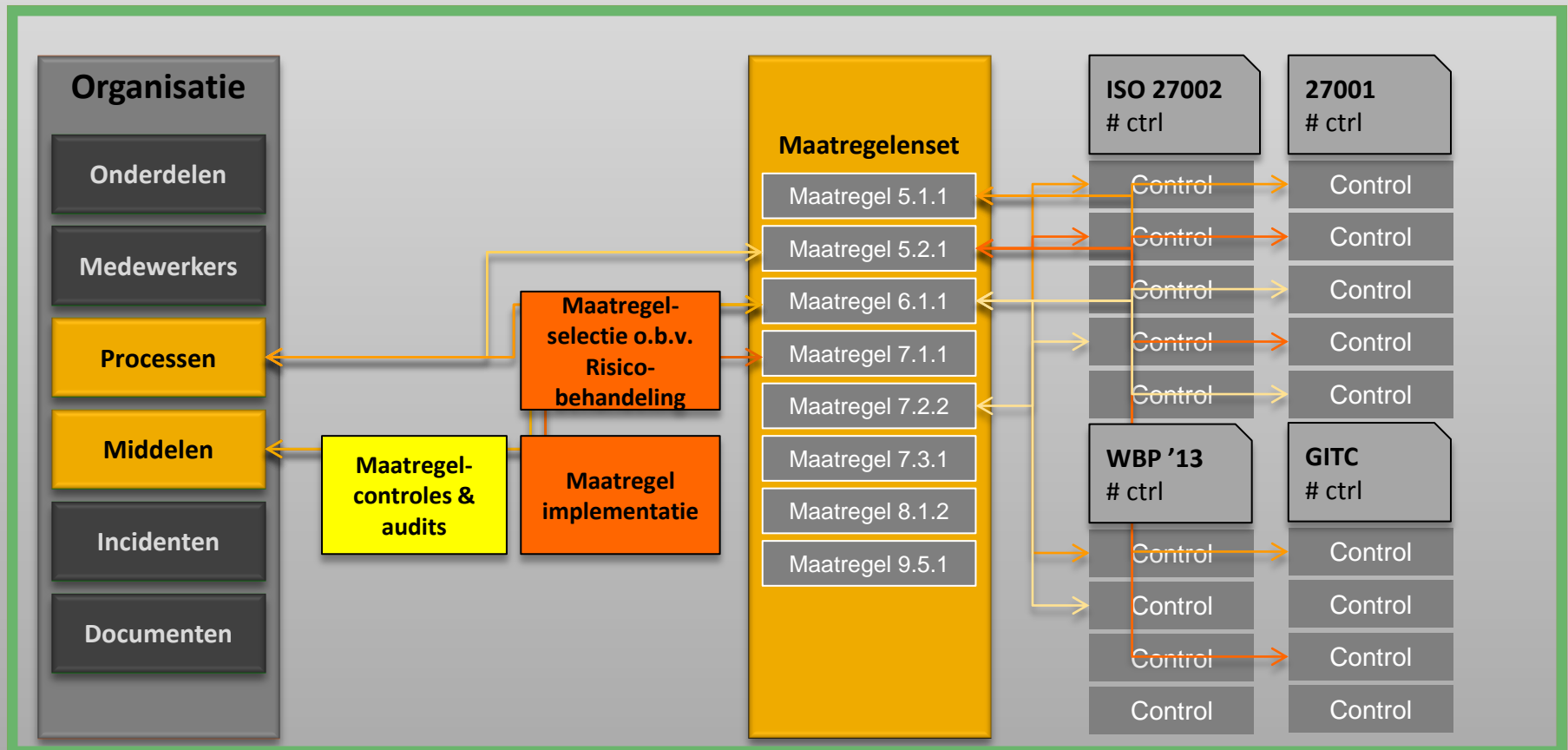
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



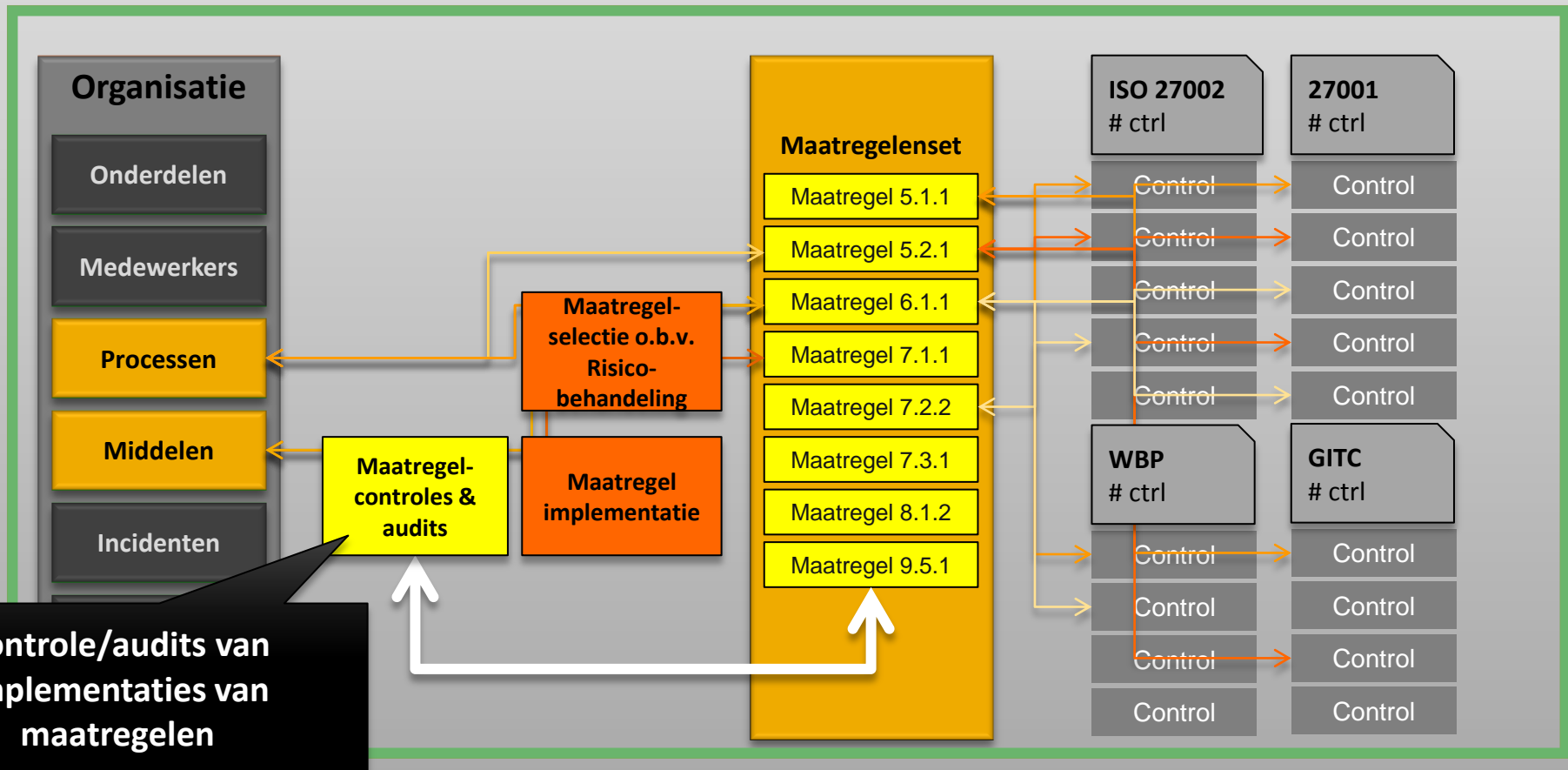
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



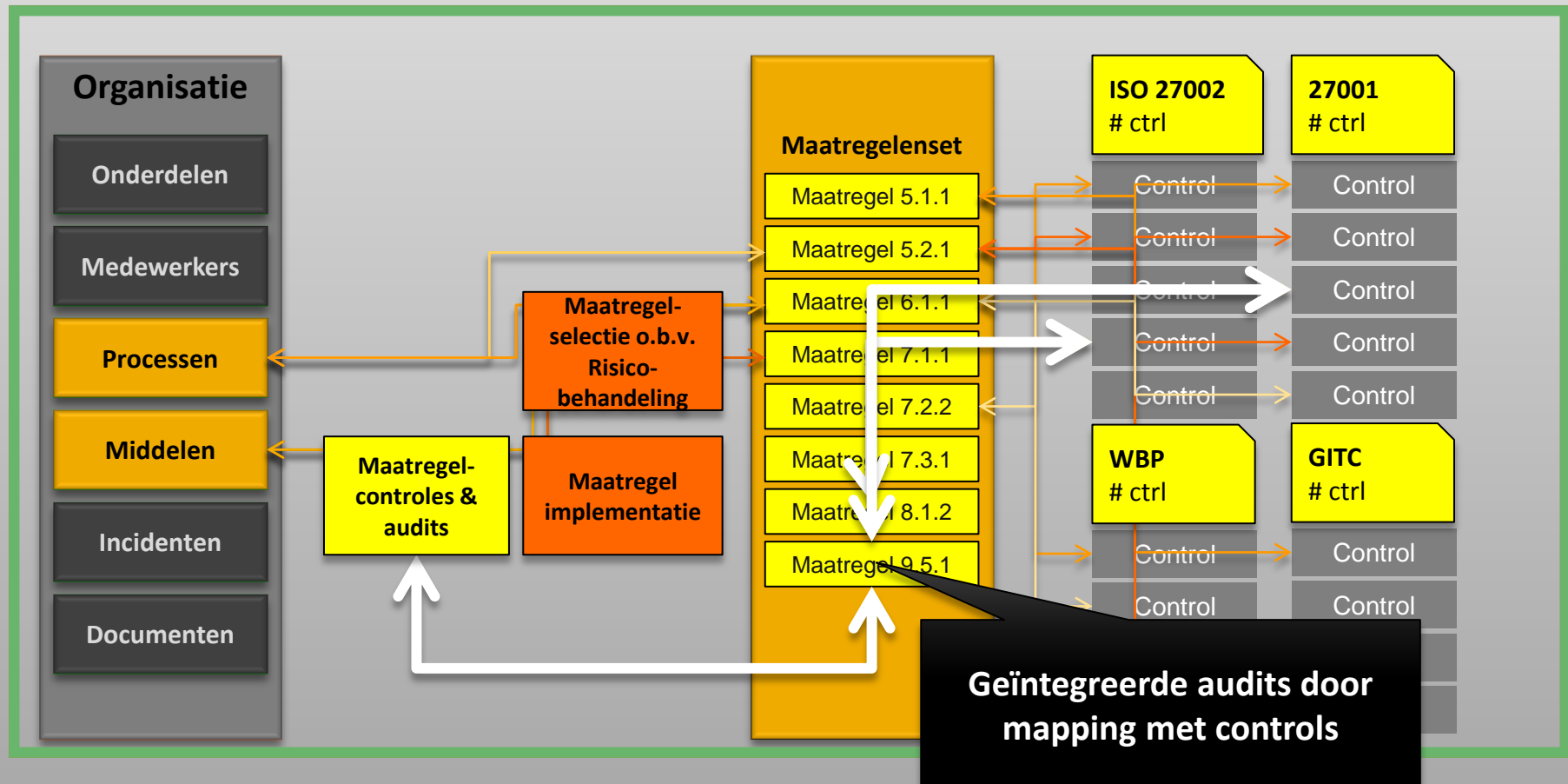
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



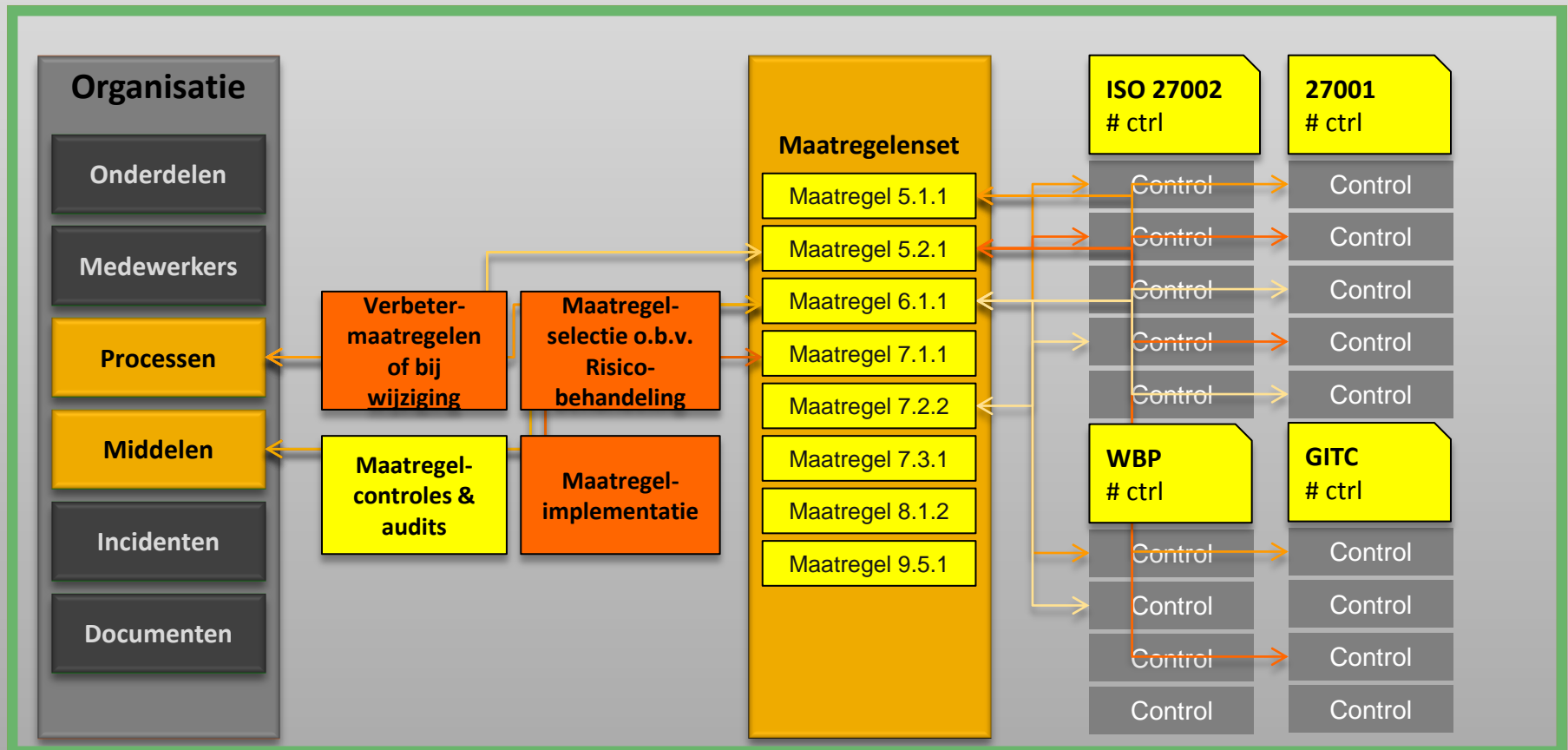
Interne beheersing op basis van risicomanagement benadering

Compliance raamwerk



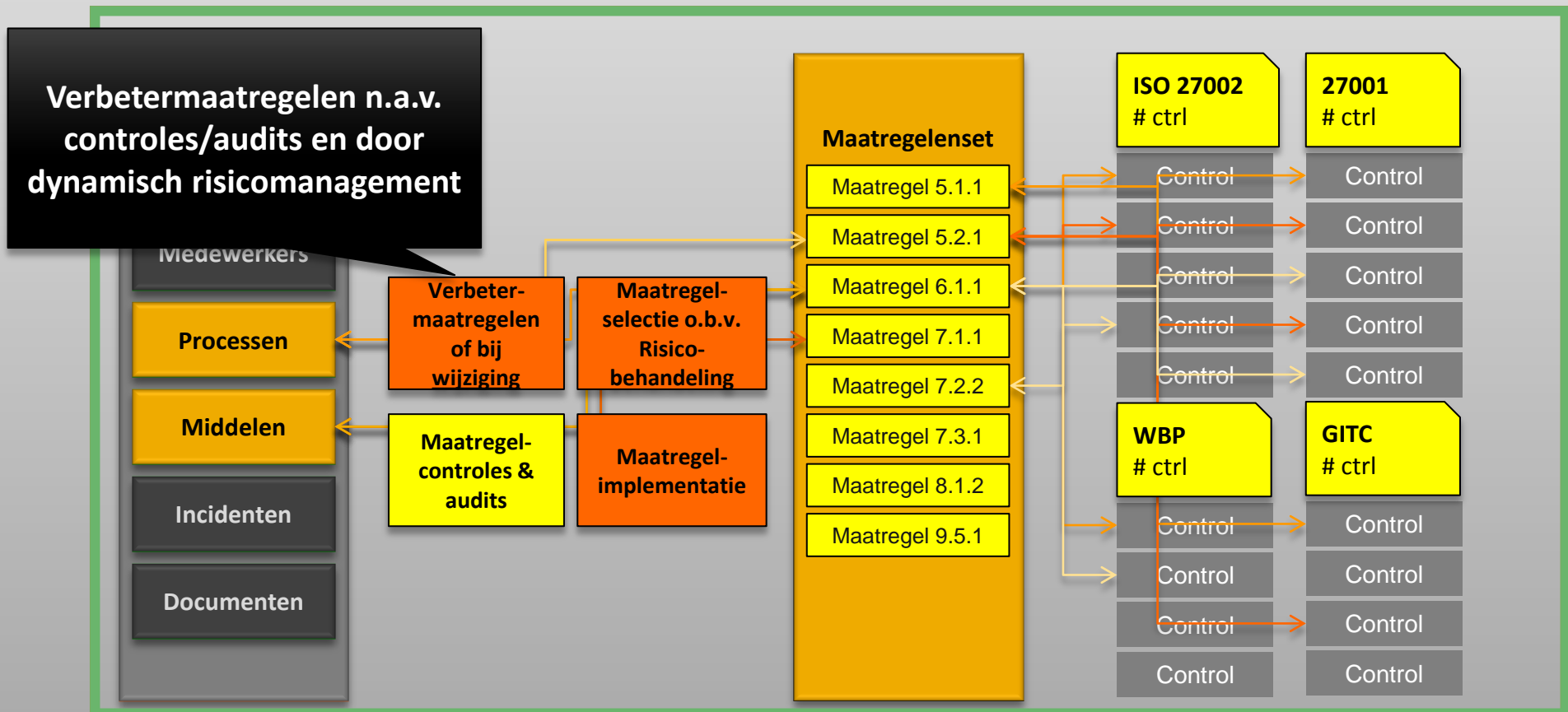
Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



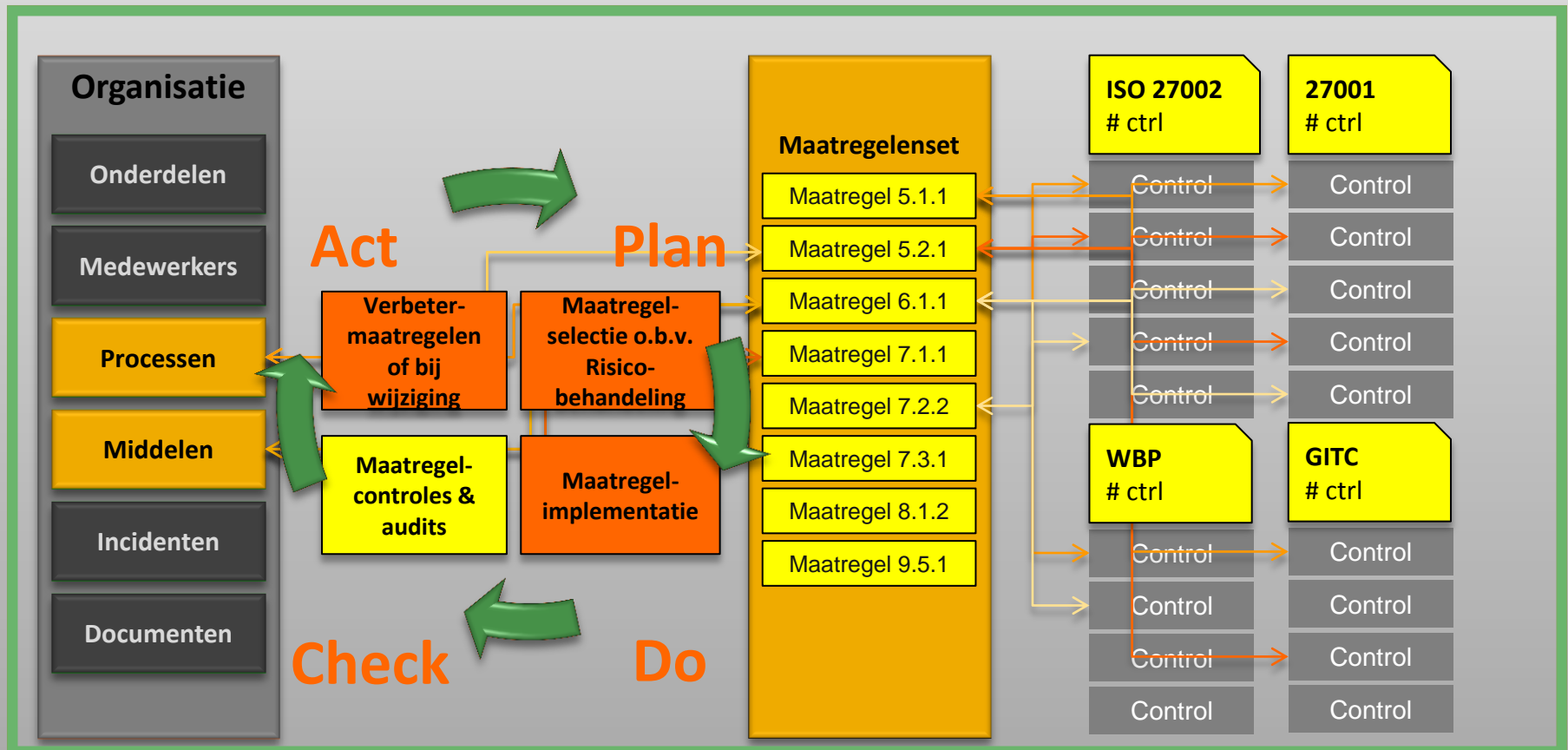
Interne beheersing op basis van risicomanagement benadering

Compliance raamwerk



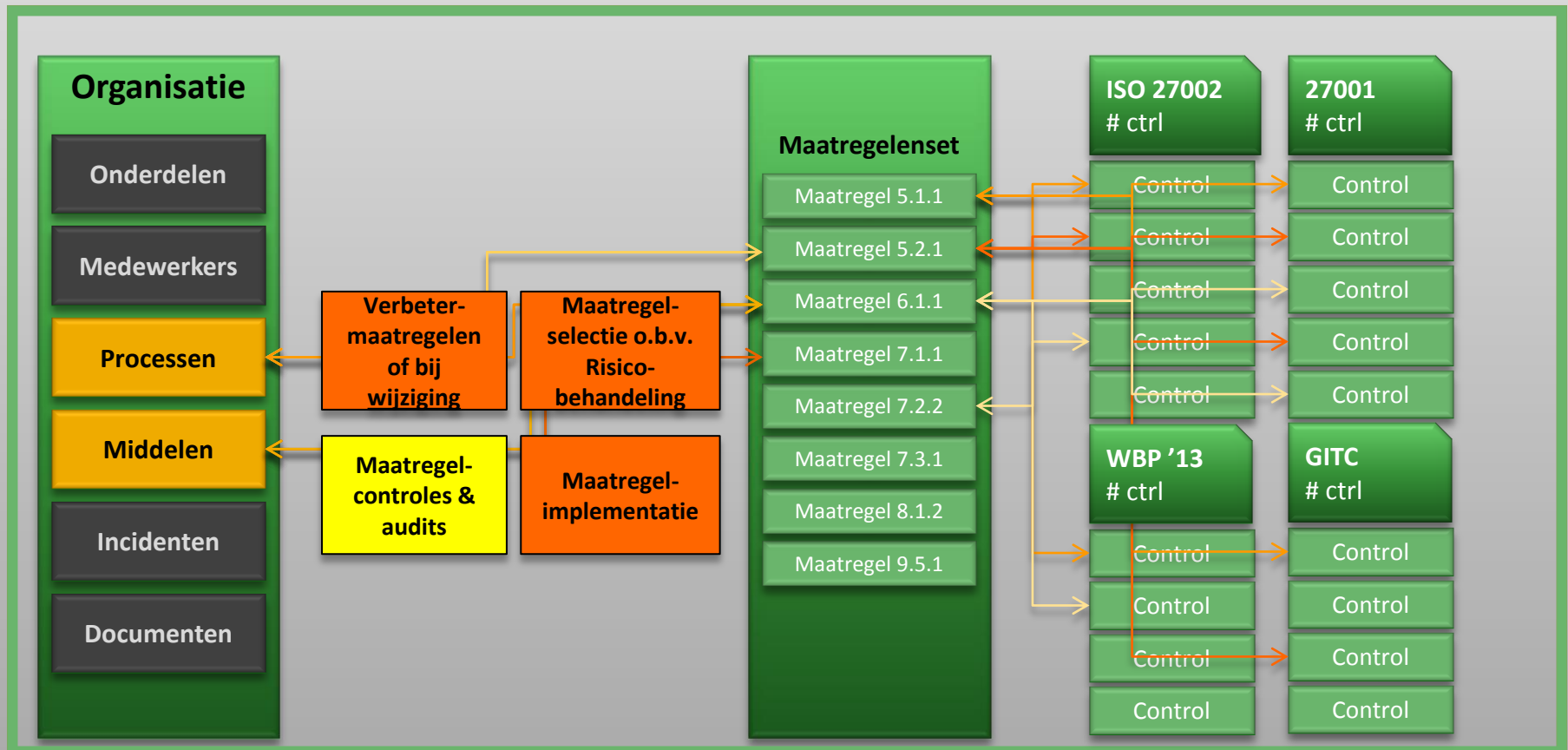
Interne beheersing op basis van risicomanagement benadering

Compliance raamwerk



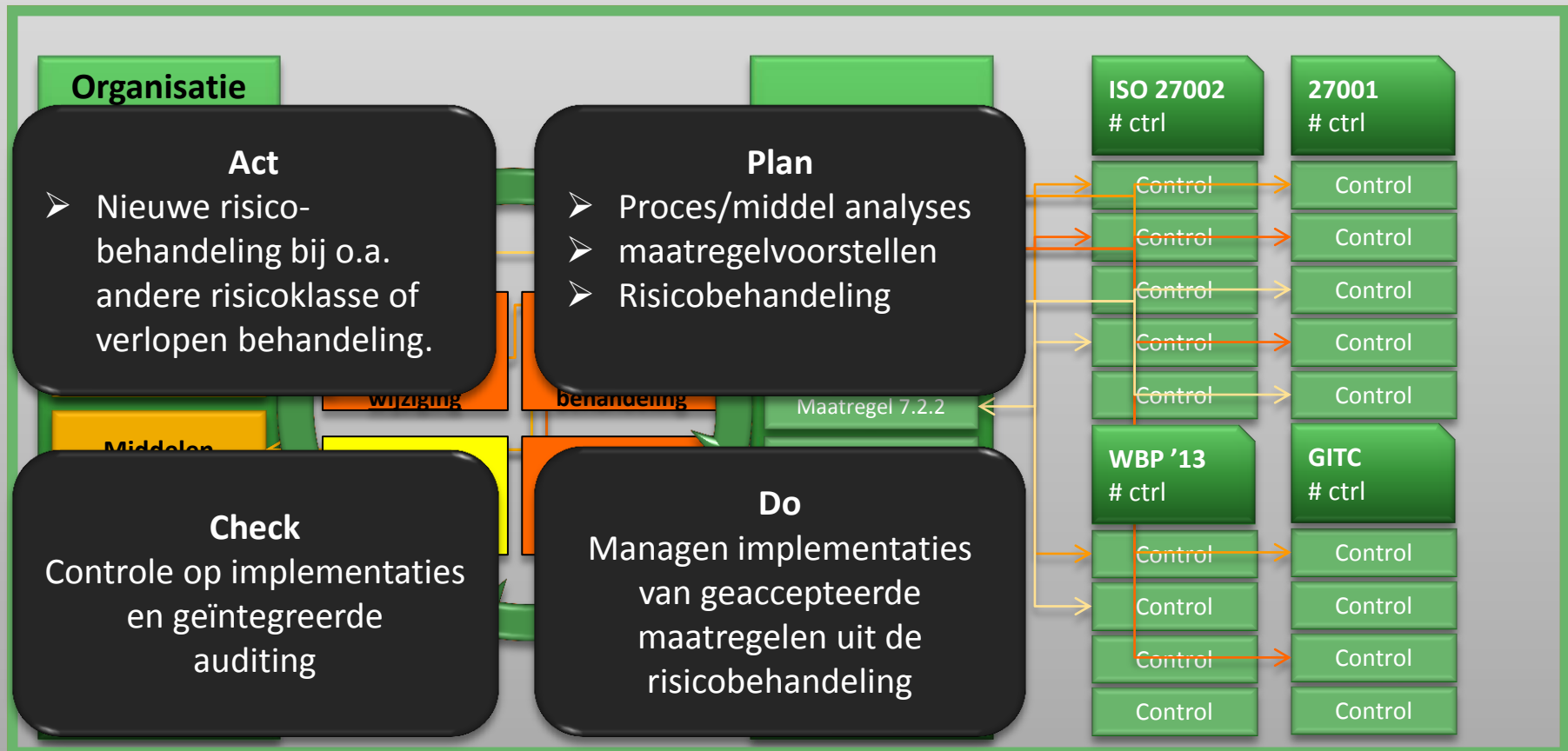
Interne beheersing op basis van risicomanagement benadering

Compliance raamwerk



Interne beheersing op basis van
risicomanagement benadering

Compliance raamwerk



- **Voordelen**

- Geïntegreerd dynamisch risicomanagement
- Eenvoudige beheersing van wet- en regelgeving & normen (Compliance raamwerk: Map once, comply to many)
- Procesmatige structuur, PDCA en stapsgewijze workflows
- Geïntegreerde auditing
- Rapportages (geschikt voor certificering)
- Content: grote hoeveelheid beschikbare normen/maatregelen, dreigingen, hulpvragen etc. (Plug & Play Governance)
- Geen Big Bang implementatie
- Mogelijkheid om “klein” te beginnen

Plan
middel- / proces analyses

- BIA's
- DA's

Plan
risicobehandeling

- Per middel
- Per proces

Maatregelcyclus

Van Plan naar
implementatie (Do)
voor verdere
Governance en
Compliance (Check en
Act)

- **Meer zien?**
 - Een DEMO is mogelijk op onze stand: B117



- Meer informatie? Demo/presentatie: info@complions.nl