ISACA®
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

C****
COBIT

Erik van Eeden

ISACA®
Serving IT Governance Professionals

ISACA®
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

A recognized global leader in
IT governance, control and assurance

Voorstelronde

Erik van Eeden

Sinds 1982 al werkzaam in de IT en per stap steeds dichter tegen de klantzijde aan. Dit is mijn aansluiting naar Governance.

Het trainingsvak ben ik naast mijn werkzaamheden gaat doen en is inmiddels integraal gecombineerd met consultancy. Dit is ook de reden dat ik werd gevraagd om toe te treden tot het bestuur van ISACA Nederland met als doel om Governance en trainingen met elkaar te verbinden.
Governance is de gewaarwording die ik overal ter wereld in opgang zie. Voor ISACA is het belangrijk om dit uit te stralen en hier een belangrijke rol in te spelen.
Kwaliteit wil ik uitstralen, de middelste twee letters van mijn voornaam geven dit al aan.

In mijn werk als consultant en trainer pak ik graag veel dingen aan en wil ik mensen en bedrijven graag verder helpen. Het netwerk om mij heen geeft mij veel mogelijkheden.

Privé ben ik trotse opa, door joggen blijf ik lichamelijk en geestelijk in balans.

Binnen het bestuur ben ik het aanspreekpunt voor trainingen, waarbij we op zoek zijn naar meer netwerk en draagvlak. Graag kom ik met u in contact via trainingen@isaca.nl.

De bestuursleden van ISACA Nederland zijn veelzijdig en enthousiast. Ik ben ervan overtuigd dat we met elkaar een goede uitwerking gaan geven aan de nieuwe strategie.

APMG accredited

APMG International

THIS IS TO CERTIFY THAT

Erik van Eeden

Erik van Eeden
Roodenburgerstraat 8
2313HK Leiden
The Netherlands

IS A

COBIT® 5
Approved Trainer
Foundation

16 March 2018

COBIT® 5
AN ISACA® FRAMEWORK


APMG International

THIS IS TO CERTIFY THAT

Erik van Eeden

IS A

COBIT® 5
Approved Trainer
Assessor

MEETING STANDARDS
APMG/QMS/Approved Trainer and Facilitator Certification as stated in the APMG Quality Management System.

EFFECTIVE DATE
08 May 2015

EXPIRY DATE
16 March 2018

REGISTRATION NUMBER
COBITTNL/190

CERTIFICATE NUMBER
03096363-01-8MXG

Nick Houlton
Chief Operating Officer

00018688


APMG International

THIS IS TO CERTIFY THAT

Erik van Eeden

IS A

COBIT® 5
Approved Trainer
Implementation

MEETING STANDARDS
APMG/QMS/Approved Trainer and Facilitator Certification as stated in the APMG Quality Management System.

EFFECTIVE DATE
08 May 2015

EXPIRY DATE
16 March 2018

REGISTRATION NUMBER
COBITTNL/190

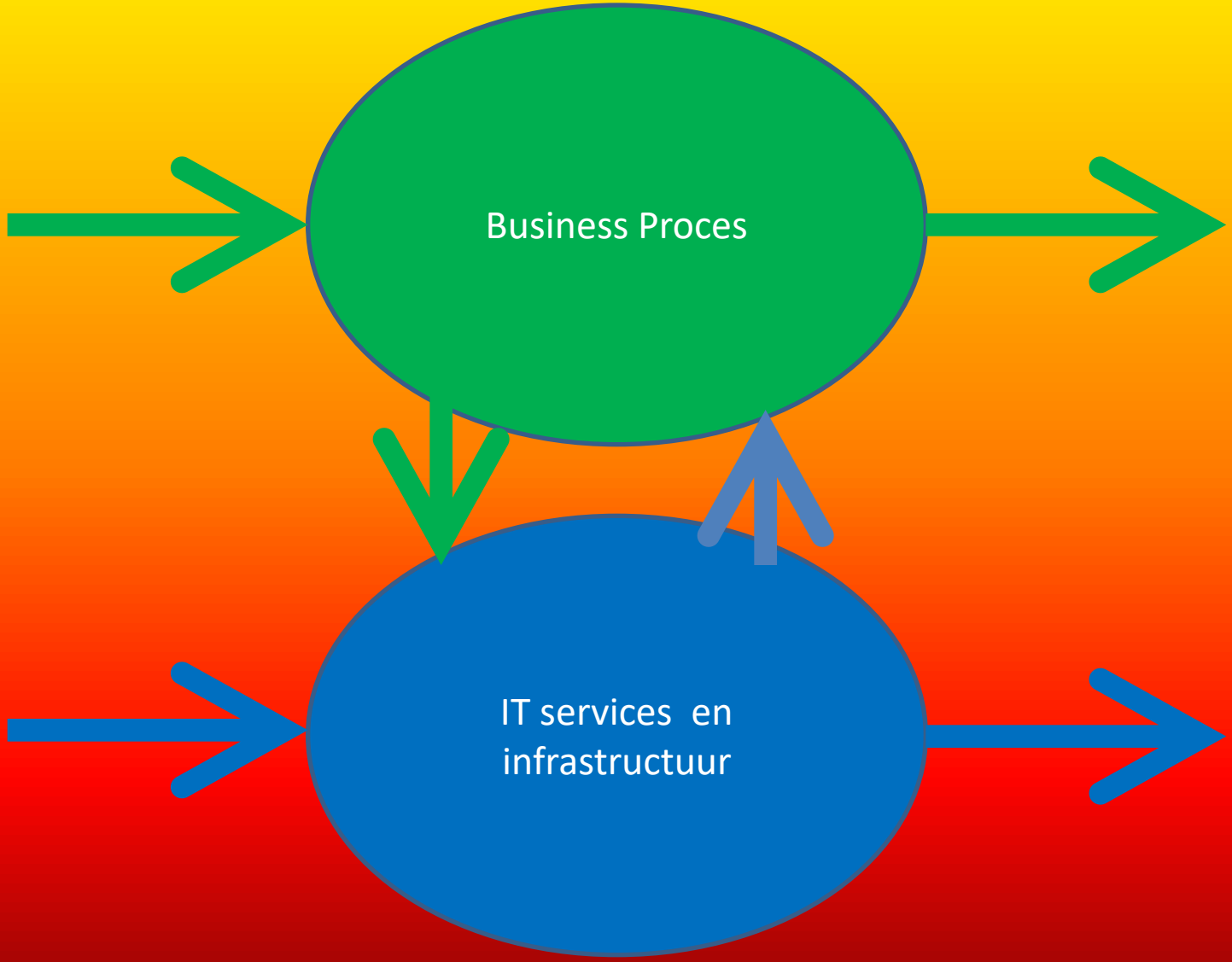
CERTIFICATE NUMBER
03096362-01-GQ3X

Nick Houlton
Chief Operating Officer

APMG accredited Cobit Independent Trainer

COBIT5

- COBIT5 =


Business Proces
IT services en
infrastructuur

Organizations Concern

Auditor's Concerns

- Inadequate view of IT functioning
- Operational failures of IT
- Increase in number security incidents
- High dependency of Businesses on IT
- Too many IT Standards & Frameworks
- Lack of knowledge of critical systems
- IT not meeting compliance

CIO's Priorities

- Delivering projects to meet business growth
- Demonstrating value to business
- Tightening security and privacy controls
- Improving business continuity readiness
- Improving quality of IT service delivery
- Applying metrics to IS organization and services
- Demonstration of Compliance
- Too many Audits (Internal / External)

GEIT


BUSINESS OUTCOMES OF GOVERNANCE OF ENTERPRISE IT (GEIT)
42%
IMPROVED MANAGEMENT OF IT-RELATED RISK
40%
IMPROVED COMMUNICATION AND RELATIONSHIPS BETWEEN BUSINESS AND IT
38%
LOWER IT COSTS
37%
IMPROVED IT DELIVERY OF BUSINESS OBJECTIVES
28%
IMPROVED BUSINESS COMPETITIVENESS

COBIT® beantwoord belangrijke bedrijfsvragen

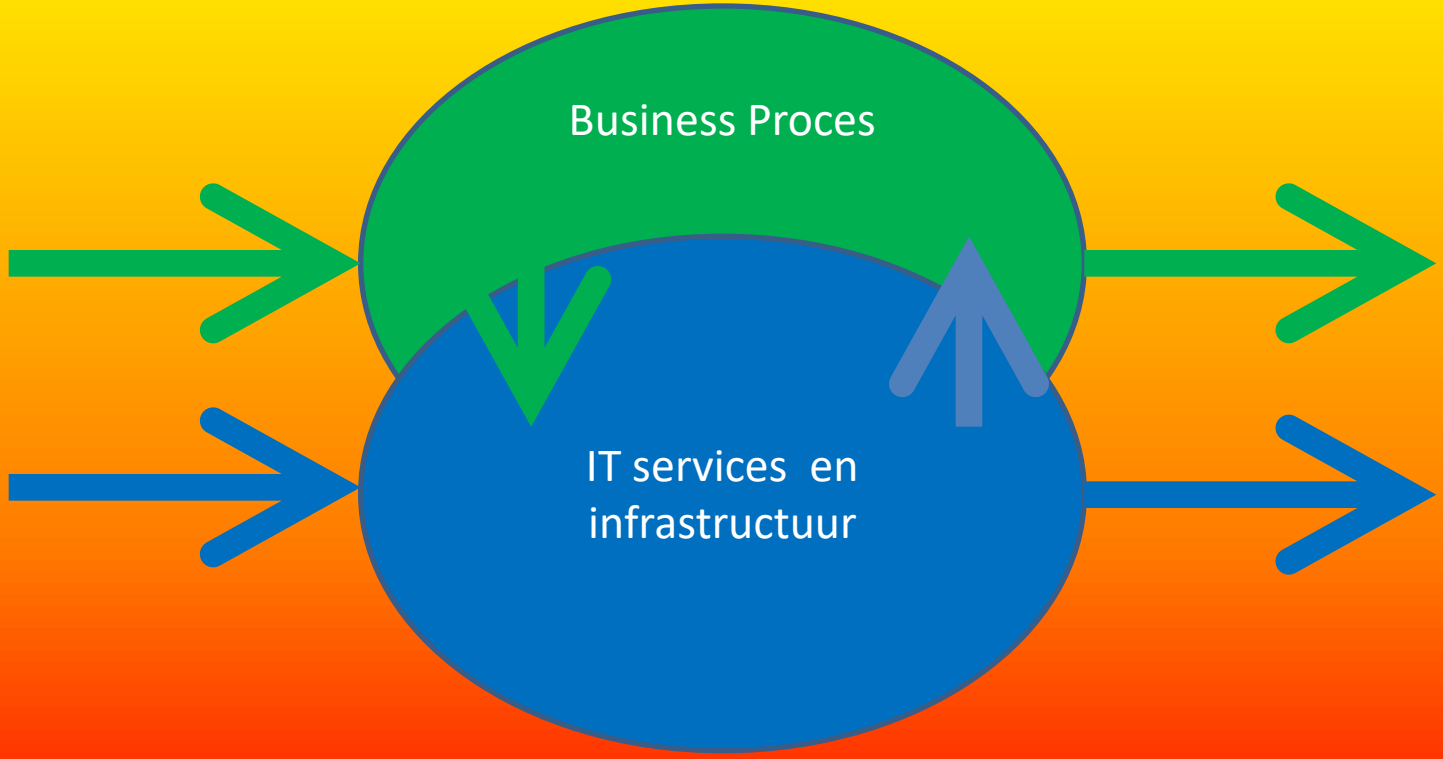
Is mijn informatie technologie organisatie de juiste dingen aan het doen?

Doen we de dingen op de juiste manier?

Krijgen we de dingen voor elkaar?

Zien we de resultaten wel goed?

* Based on the "Four Ares" as described by John Thorp in his book *The Information Paradox,* written jointly with Fujitsu, first published in 1998 and revised in 2003



Leunen op IT

COBIT® Business voordelen

- COBIT® geeft inzicht aan executive management om governance uit te voeren over de IT in het bedrijf

- Effectievere wegen om de IT de bedrijfsdoelen te laten ondersteunen
- Meer transparantie en voorspelbare IT kosten over de hele life-cycle
- Meer informatie over IT die betrouwbaar en op tijd is
- Hogere kwaliteit uit IT services en meer succesvolle projecten
- Effectiever management van IT-gerelateerde risico's

Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.
- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT**

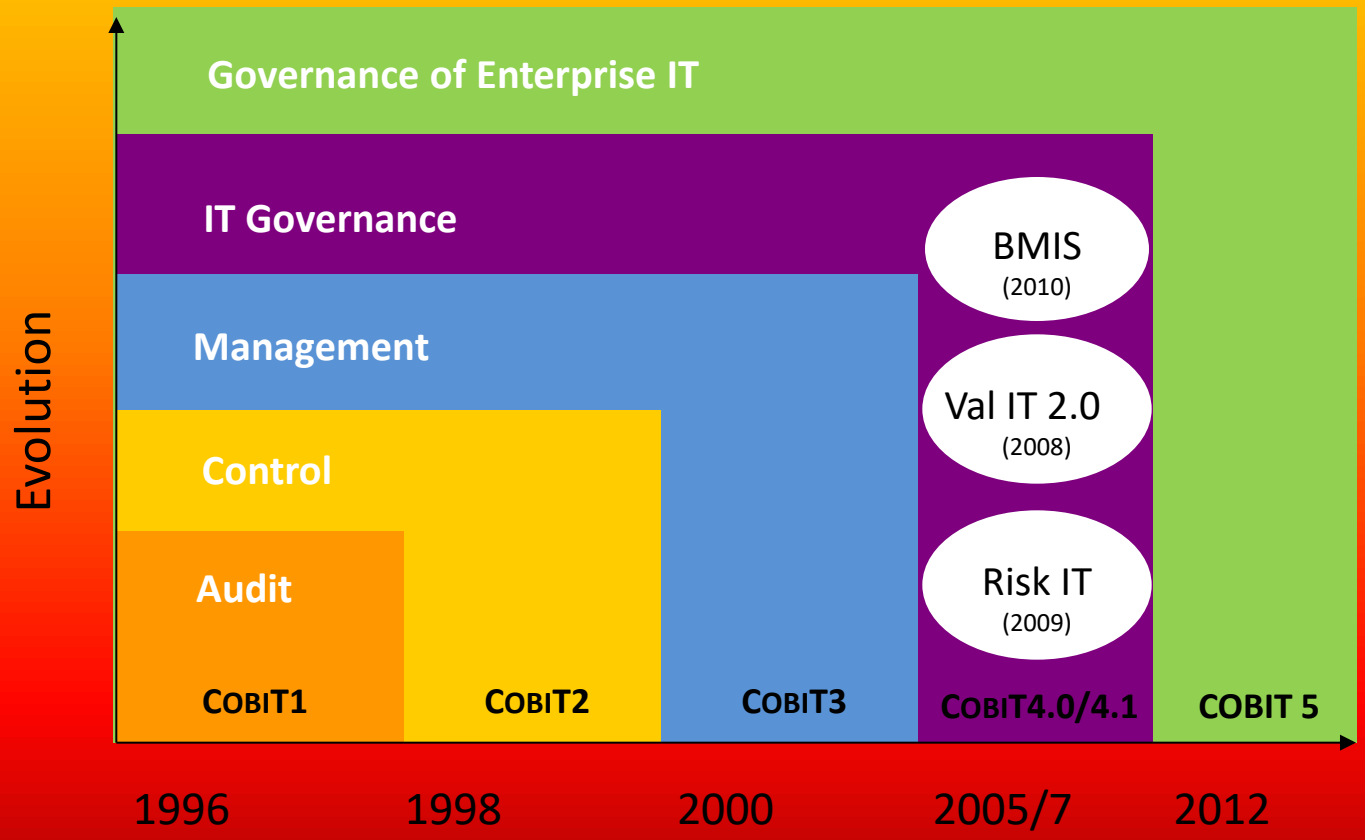
How many controls are enough?

Overview COBIT5

- 5 Principles
- 7 Enablers
- Process Reference Model
- Life Cycle model voor Implementation
- Process Assessment Model
- Dimensies

Er zijn aparte Implementation trainingen en Assessor trainingen

The Evolution of COBIT 5

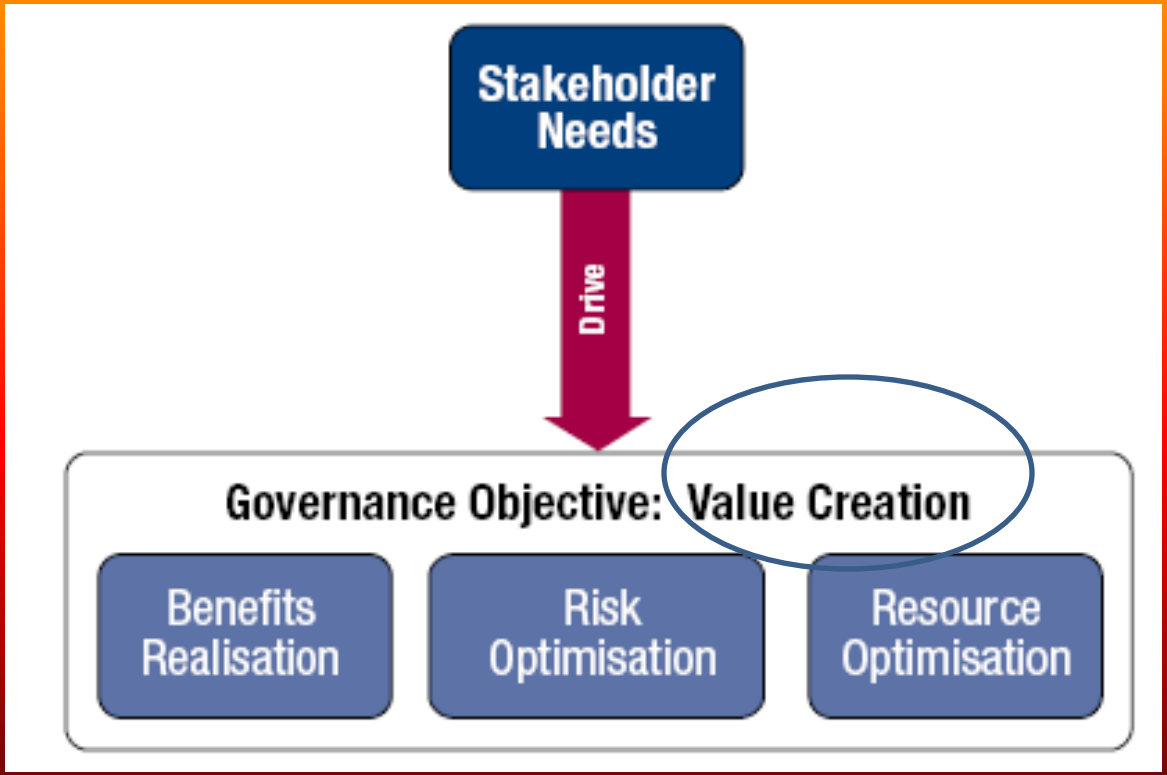


© 2012 ISACA. All Rights Reserved.

Meeting Stakeholder Needs

Principle 1. Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders



BRR

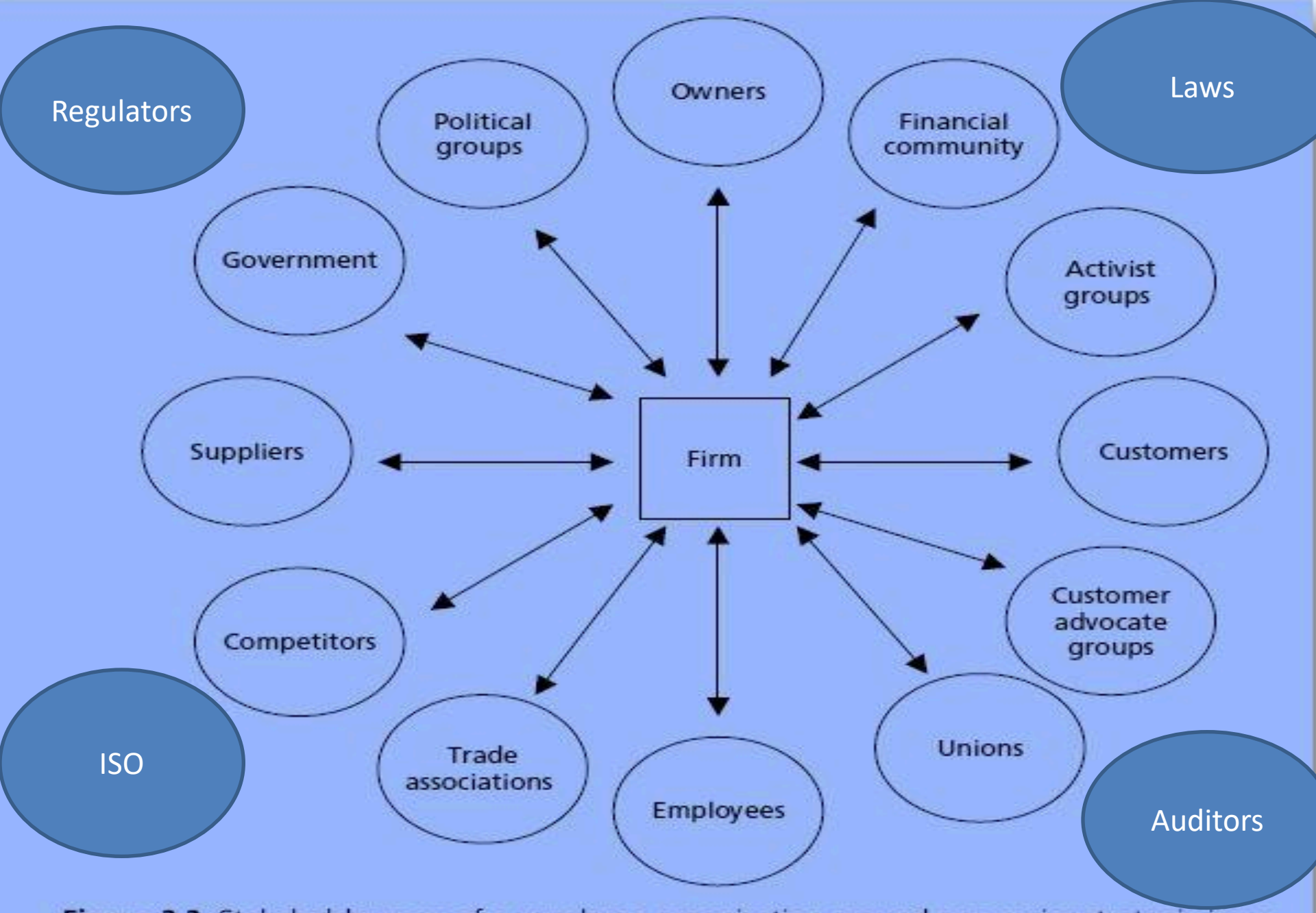


Figure 2.2 Stakeholder map of a very large organization around one major strategic issue

Source: Freeman (1984: 55).

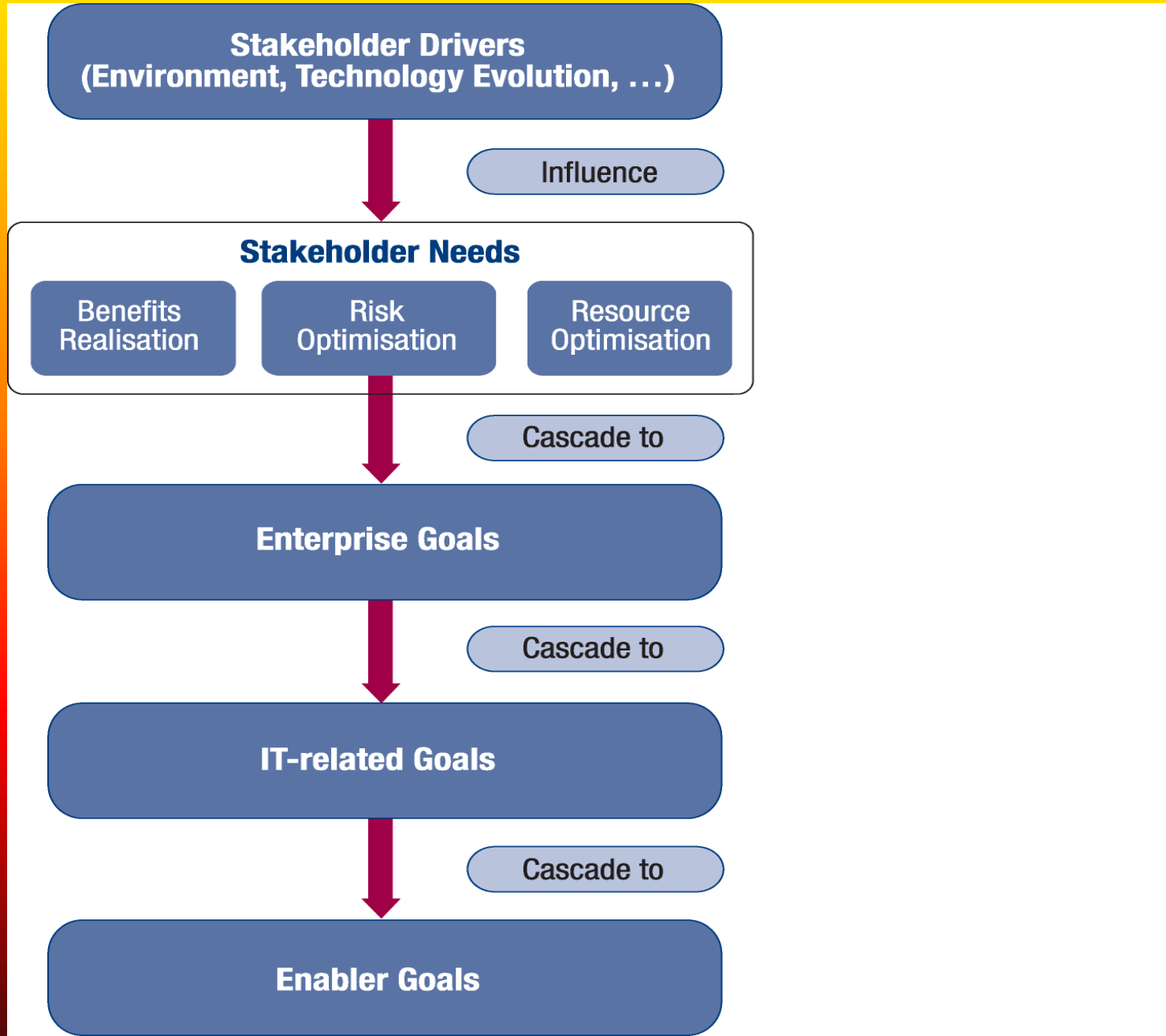
Waar begint COBIT5 ?

- EERST moet een bedrijf zijn doelen gesteld hebben
- Hoe bemoeit COBIT zich niet mee
- SWOT, COSO, BSC, ERM, DMW, JFW
- Stakeholder analyse !
- → Doelen
- En dan … Governance, supported by COBIT5

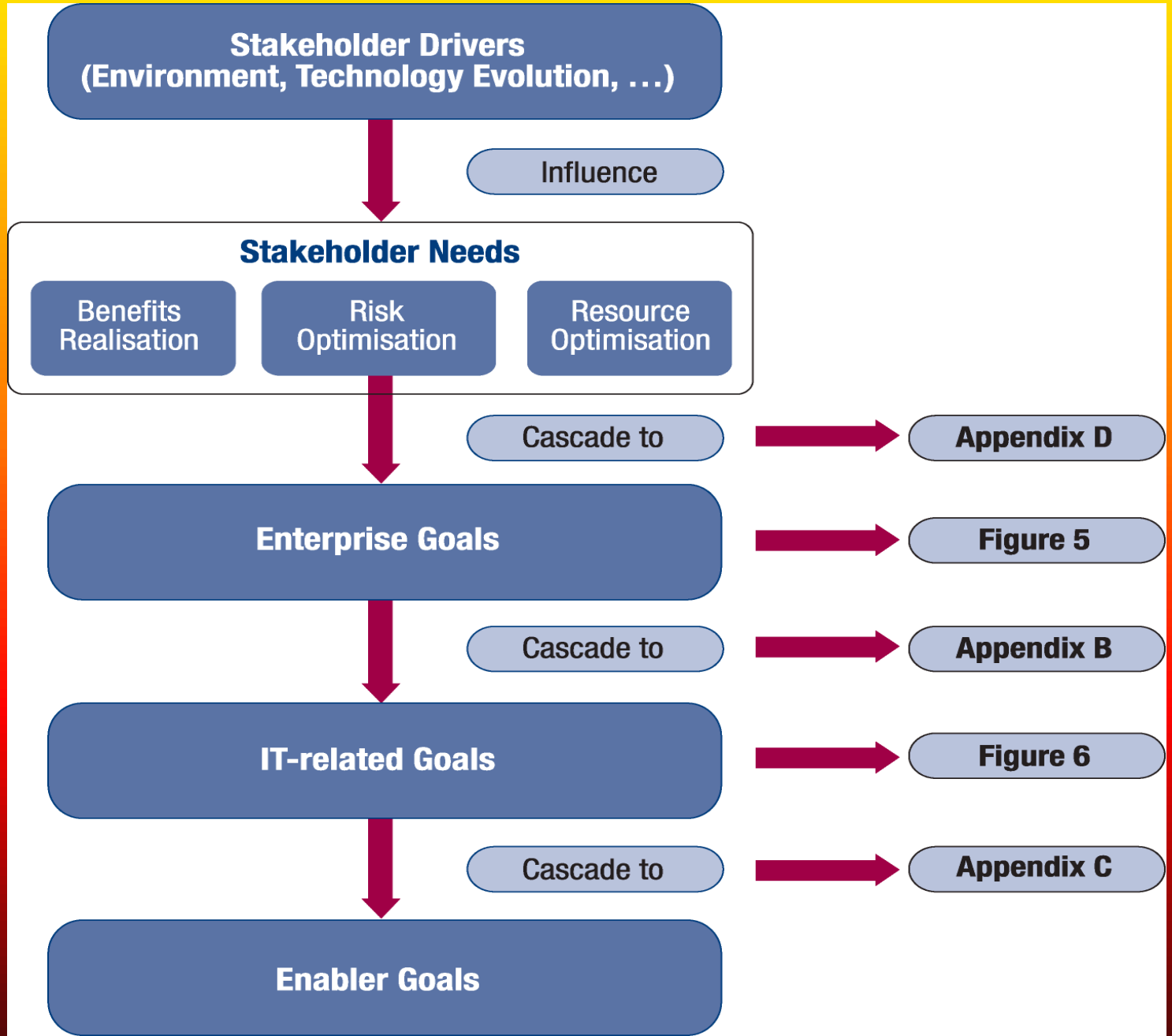
Daar begint COBIT5 !

- Uw bedrijf heeft zijn doelen gesteld en wil ze goed in beeld houden
- Doelen zijn altijd in beweging…
- Regelmatige Stakeholder analyse !
- Vertaling van Stakeholder needs naar Doelen naar IT gerelateerde doelen en naar Enabling doelen en weer terug en dat is Governance, supported by COBIT5 !

COBIT5 Goals Cascade



COBIT5 Goals Cascade +



Start met de BSC categorie in stap 1

Balanced Scorecard	Enterprise Goals	IT Related Goal (ITRG)	COBIT Process
Financial			
Customer			
Internal			
Learning			

Customer	
	6. Customer-oriented service culture
	7. Business service continuity and availability
	8. Agile responses to a changing business environment
	9. Information-based strategic decision making
	10. Optimisation of service delivery costs

© 2012 ISACA. All rights reserved.

Stap 1 Appendix D Stakeholder Needs en BSC dimensies

STAKEHOLDER NEEDS	1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?	■	■				■	■						■			■	■
How do I manage performance of IT?		■			■				■	■	■	■		■			
How can I best exploit new technology for new strategic opportunities?	■	■						■					■			■	■
How do I best build and structure my IT department?								■		■	■	■		■	■	■	
How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers?			■	■						■							
What are the (control) requirements for information?				■					■						■		
Did I address all IT-related risk?			■				■		■						■		
Am I running an efficient and resilient IT operation?					■		■										

Cascade stap 1 Figure5: BSC dimensies en Enterprise Goals plotten op BRR

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Stap 2 – Selecteer Enterprise Goal, IT related Goals en Processen

Customer	
	6. Customer-oriented service culture
	7. Business service continuity and availability
	ITRG 07 Delivery of IT services in line with business requirements
	ITRG 08 Adequate use of applications, information and technology solutions
	ITRG 01 Alignment of IT and business strategy
	ITRG 04 Managed IT-related business risk
	ITRG 10 Security of information, processing infrastructure and applications
	ITRG 14 Availability of reliable and useful information for decision making

PROCESSES	PRIMARY IMPORTANCE OR IMPACT
APO09 Manage Service Agreements	P
APO13 Manage Security	P
BAI04 Manage Availability and Capacity	P
BAI08 Manage Knowledge	P
BAI10 Manage Configuration	P
DSS03 Manage Problems	P
DSS04 Manage Continuity	P

© 2012 ISACA. All rights reserved.

Enterprise Goals To IT Related Goals

There are also 17 generic IT related goals as shown in Figure 6 (shown below) that are also categorised into the Balanced Score Card (BSC) categories. The relationship of enterprise goals to IT related Goals are shown in Appendix B Figure 22 page 50

Figure 6—IT-related Goals

IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Stap 2 Appendix B Enterprise Goals naar IT Related Goals in BSC dimensies

		IT-related Goal	Enterprise Goal: Financial					Customer					Internal					Learning and Growth	
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
	07	Delivery of IT services in line with business	P	P	S	S		P	S	P	S		P	S	S			S	S

Stap 2 – het laatste deel: de processen

Customer	
	6. Customer-oriented service culture
	7. Business service continuity and availability
	ITRG 07 Delivery of IT services in line with business requirements
	ITRG 08 Adequate use of applications, information and technology solutions
	ITRG 01 Alignment of IT and business strategy
	ITRG 04 Managed IT-related business risk
	ITRG 10 Security of information, processing infrastructure and applications
	ITRG 14 Availability of reliable and useful information for decision making

PROCESSES	PRIMARY IMPORTANCE OR IMPACT
APO09 Manage Service Agreements	P
APO13 Manage Security	P
BAI04 Manage Availability and Capacity	P
BAI08 Manage Knowledge	P
BAI10 Manage Configuration	P
DSS03 Manage Problems	P
DSS04 Manage Continuity	P

© 2012 ISACA. All rights reserved.

Stap 2 Appendix C IT Related Goals naar processen

		IT-related Goal															
		Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process	**Financial**						**Customer**		**Internal**							**Learning and Growth**	
BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S

Build, Acquire and Implement

Step .3

Example APO09 – Examine Metrics

Process ID	APO09
Process Name	Manage Service Agreements
Process Description	Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.
Process Purpose	Ensure that IT services and service levels meet current and future enterprise needs.

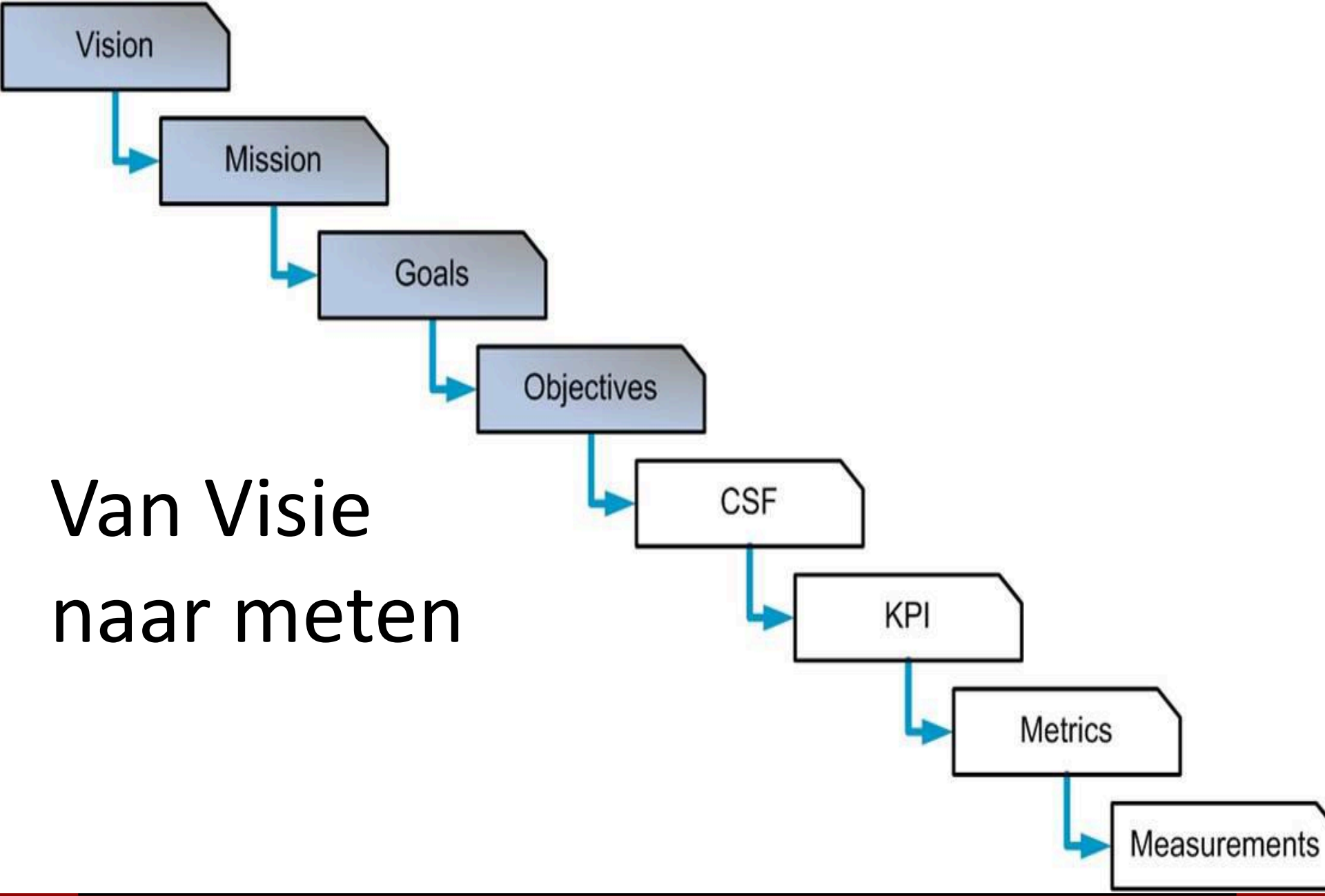
Outcomes (OS)

Number	Description
APO09-O1	IT services are identified, defined and catalogued according to enterprise nee
APO09-O2	Service agreements reflect enterprise needs and the capabilities of IT.
APO09-O3	IT services perform as stipulated in service agreements.

RELATED METRICS
The number of business processes with unidentified service agreements
% of live IT services covered by service Agreements
% of Customers satisfied that service delivery meets agreed-on levels
Number & severity of service breaches
% of services being monitored to service levels
% of service targets being met

© 2012 ISACA. All rights reserved.

Van Visie naar meten

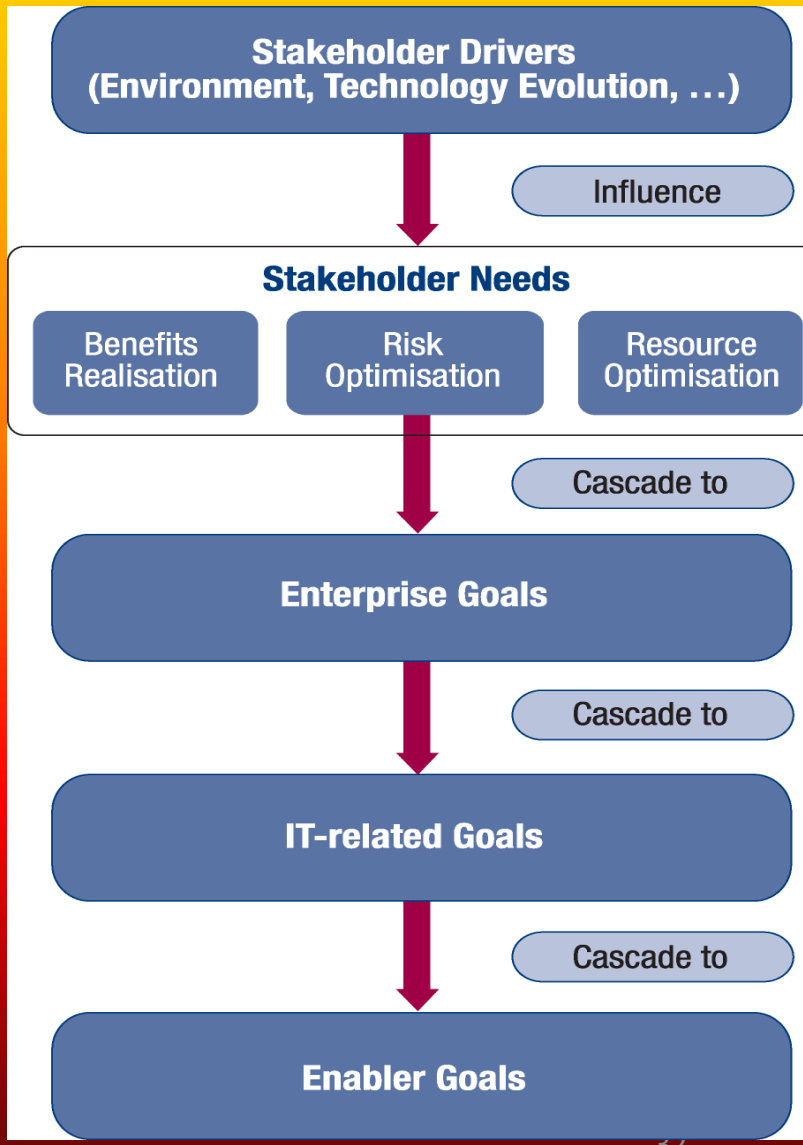


© Crown copyright 2011. Reproduced under license from Axelos.
Figure 4.1 Continual Service Improvement, page 50

Een voorbeeld van Governance en doelen

Questions?

Heeft u vragen (tot zover) over het omzetten van uw bedrijfsdoelen naar ….. processen ?

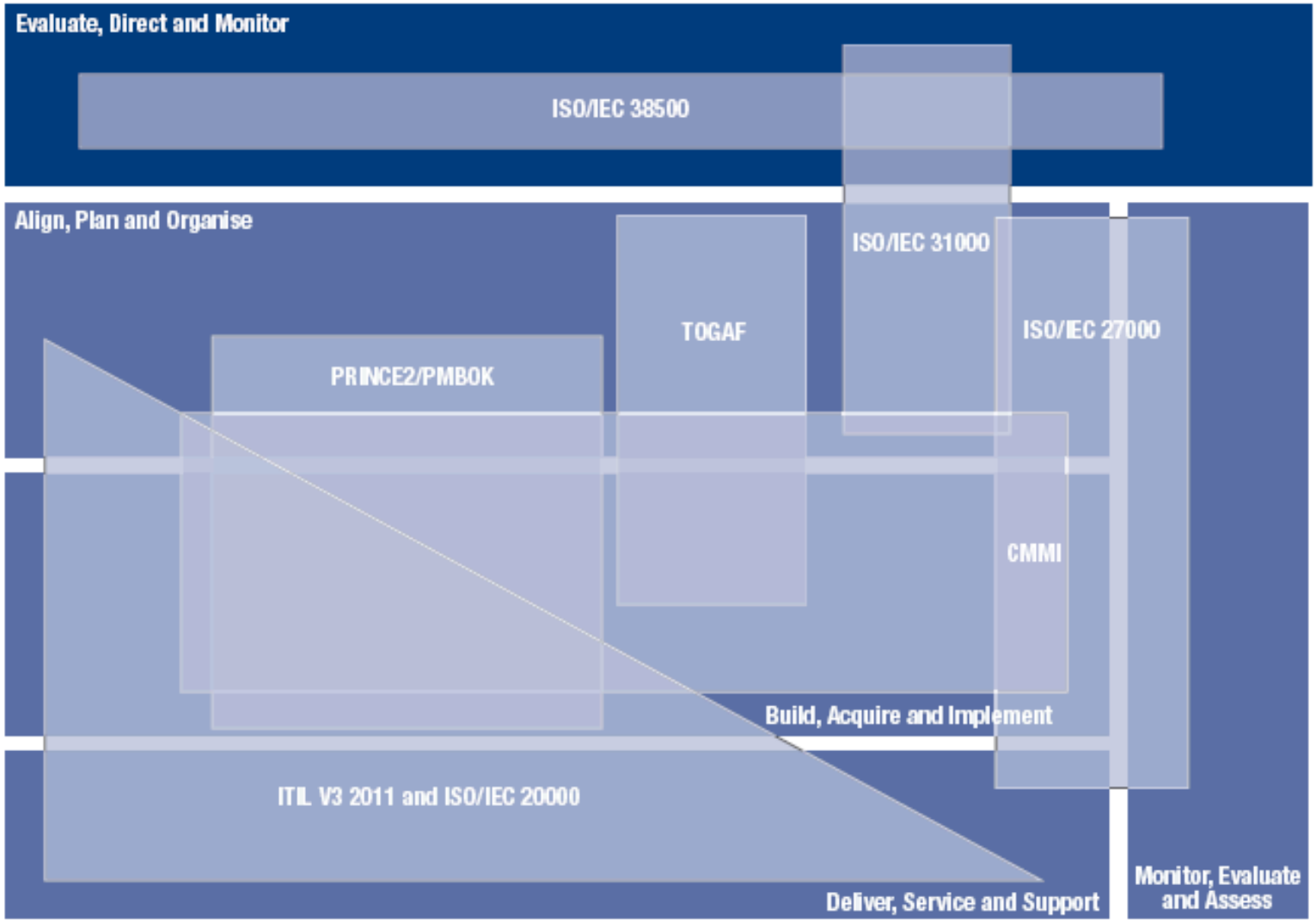


© 2012 ISACA. All Rights Reserved.

COBIT 5 Principles

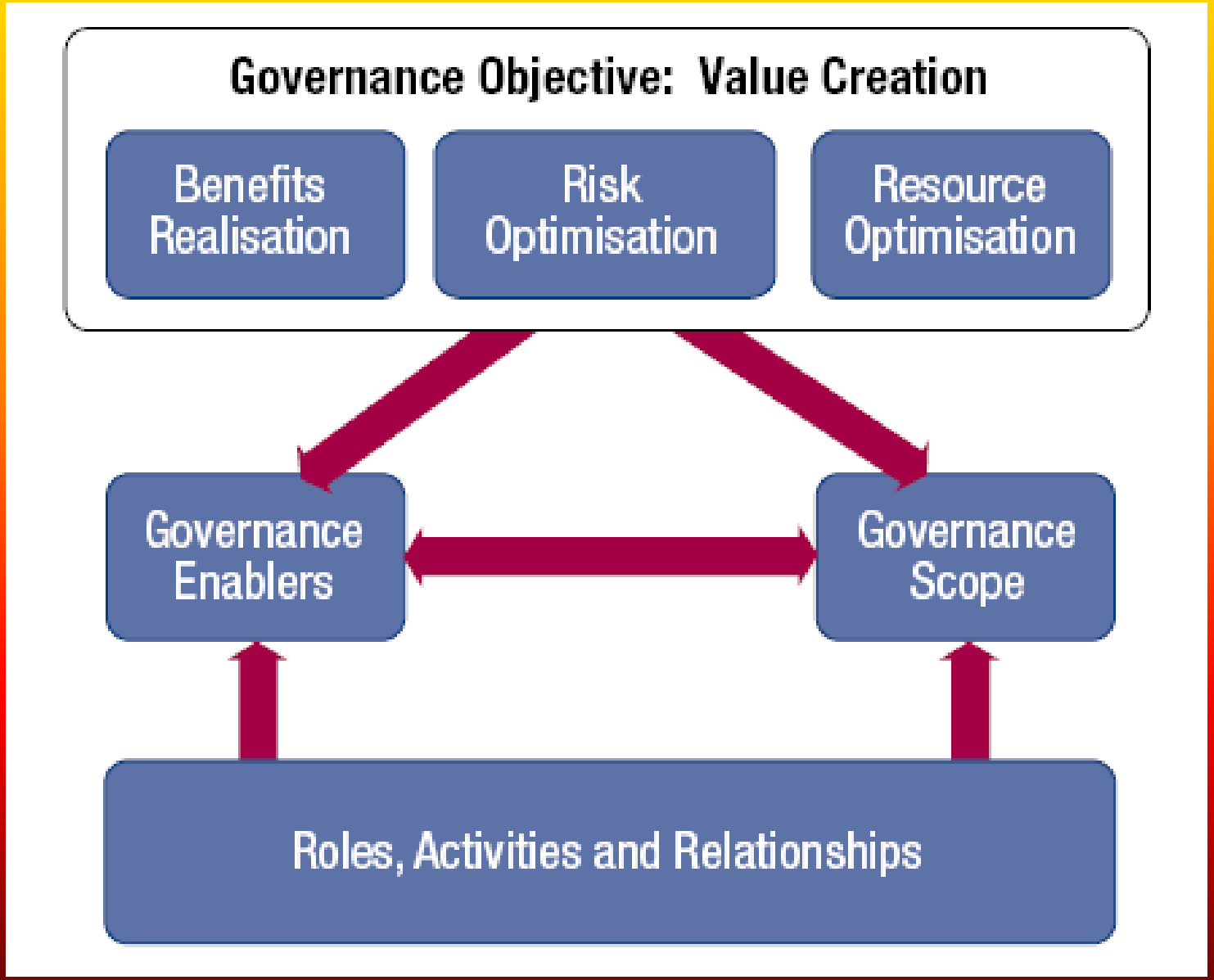
© 2012 ISACA All rights reserved.

COBIT 5 Mapping Summary



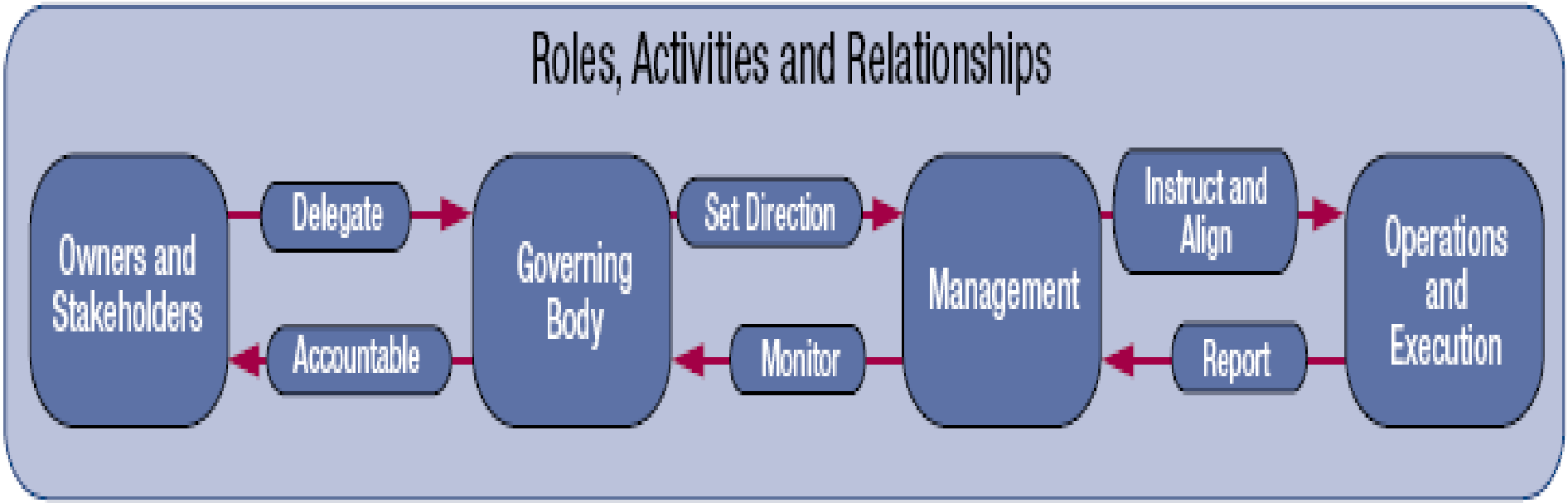
© 2012 ISACA. All rights reserved.

Key components of a governance system



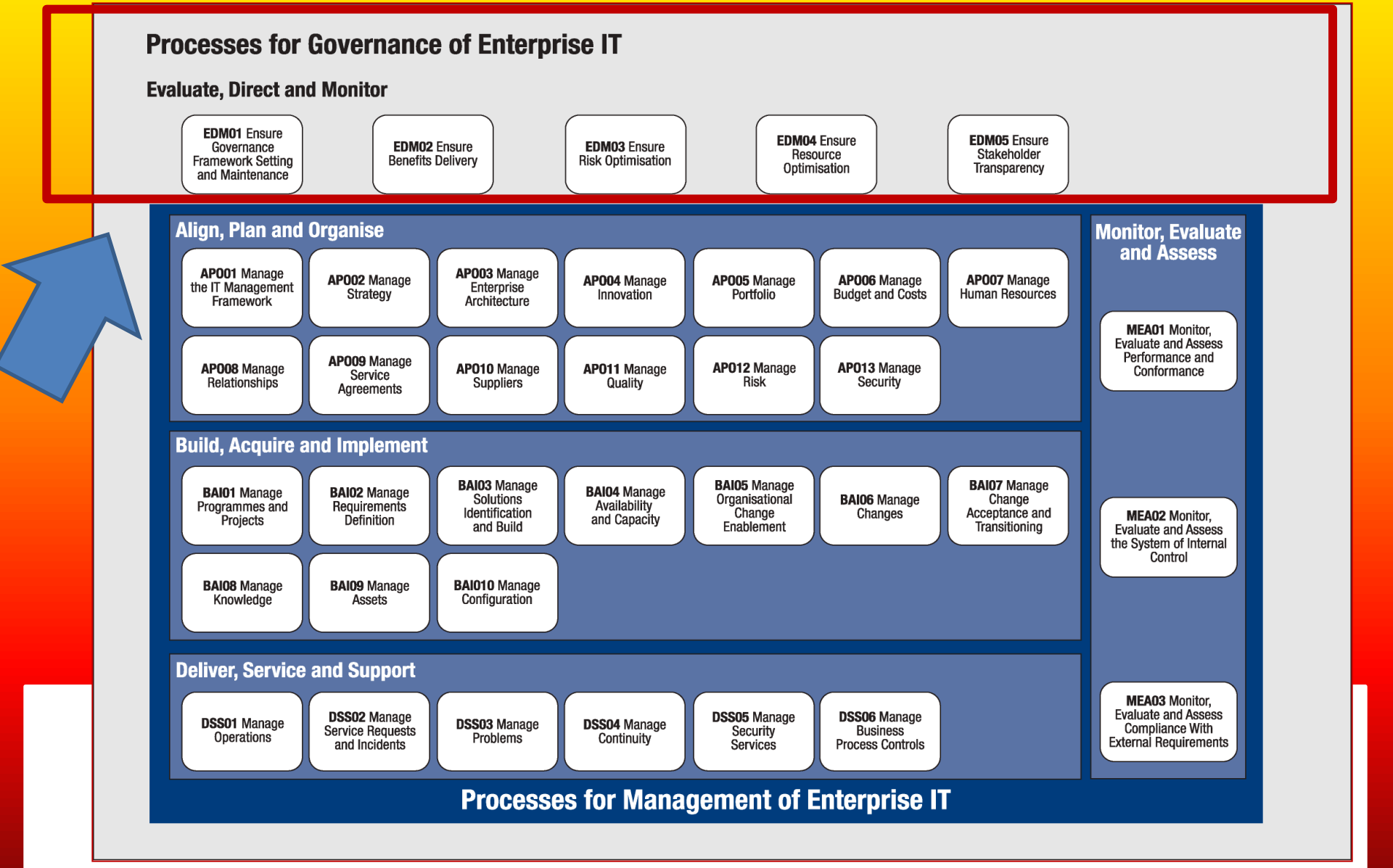
© 2012 ISACA. All Rights Reserved.

Governing Body



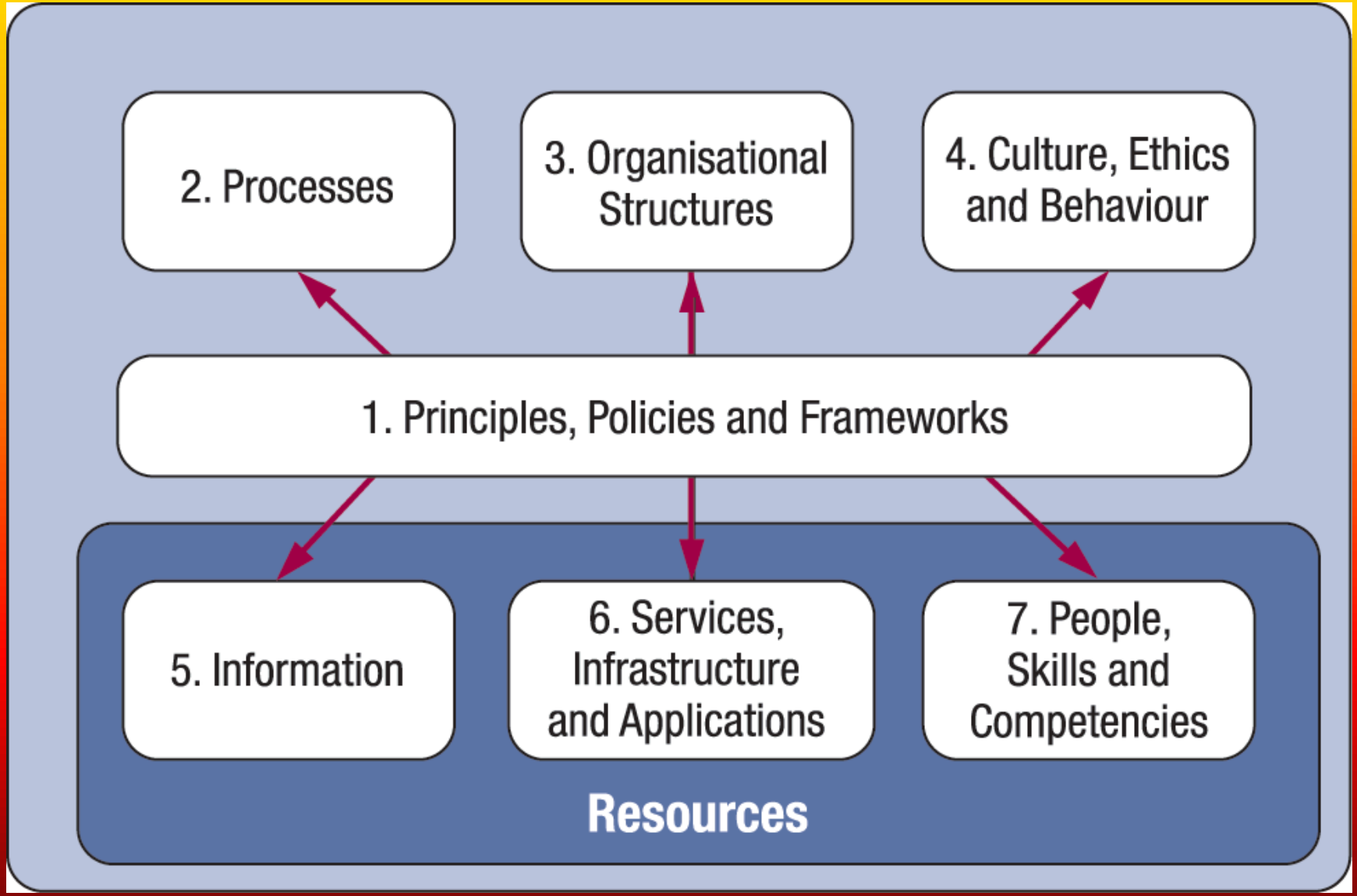
control is important especially when you don't have it!

COBIT 5 Process Reference Model



© 2012 ISACA. All Rights Reserved.

The COBIT5 Enterprise Enablers



© 2012 ISACA. All Rights Reserved.

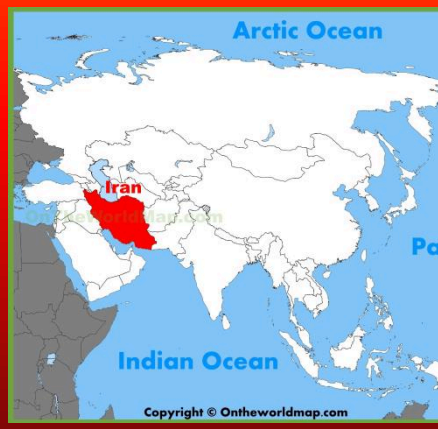
COBIT 5 Implementation Life Cycle

- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

© 2012 ISACA. All Rights Reserved.

My view on Governance
Of Enterprise IT with COBIT5

- Manage before you can Govern
- Controls are needed
- Stakeholders must be involved
- IT helps the enterprise
- Organizations are helped to find out what they really want



Questions?


MANAGEMENT
GOVERNANCE
ORGANISATIONS
MULTIPLE
IDENTIFIED
INITIATIVES
COMPETITIVE
INFORMATION
VALUE
POSSIBLE
IMPACT
SHIFT
QUESTIONS
CHANGE
SYSTEMATICALLY
ENTERPRISE
BUSINESS
TRIGGERS
CASE
ABILITY
LOW
DAMAGE
COMPLIANCE
IMPLEMENTATION
EVENTS
GEIT
ADDRESS
AUDIT
PRACTICE
RELATED
RESOURCES
FAILURE
RISK
TRIGGER
RAPIDLY
SECURITY
ORGANISATION
BUILT
TECHNOLOGY

afterthought

"All Models are wrong, but some are useful"

George Box

Thank you !

Erik van Eeden