COBIT informācijas tehnoloģijas procesu pārvaldībai

Uldis Sukovskis, CISA

Rīgas Tehniskā universitāte

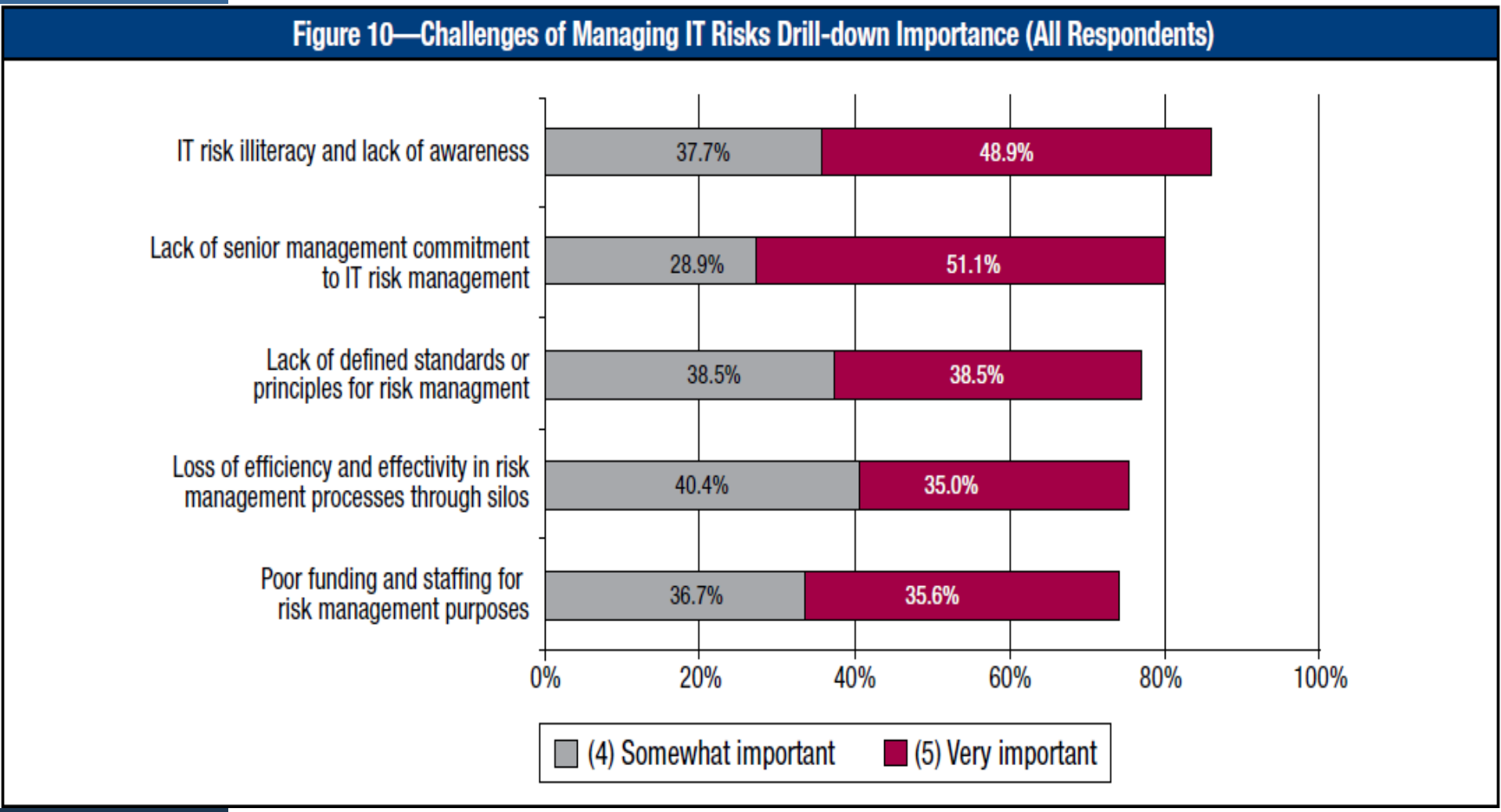
Būtisks risku mazināšanas līdzeklis ir sakārtota, pārraudzīta un mērīta IT procesu pārvaldība un vadība organizācijā

Top Five Issues

Figure 5—Top Seven Business Issues Overall							
Business Issue	Number of Responses	Weighted Score [1]	Importance Ranking				
			1st	2nd	3rd	4th	5th
Regulatory compliance	1,309	4,621	17%	15%	10%	7%	7%
Enterprise-based IT management and IT governance	1,239	4,386	19%	11%	8%	7%	8%
Information security management	1,292	4,083	11%	12%	12%	11%	8%
Disaster recovery/business continuity	1,064	3,139	8%	9%	10%	10%	9%
Challenges of managing IT risks	832	2,471	6%	7%	8%	8%	6%
Vulnerability management	743	2,095	4%	6%	8%	7%	7%
Continuous process improvement and business agility	681	2,002	6%	5%	6%	7%	6%

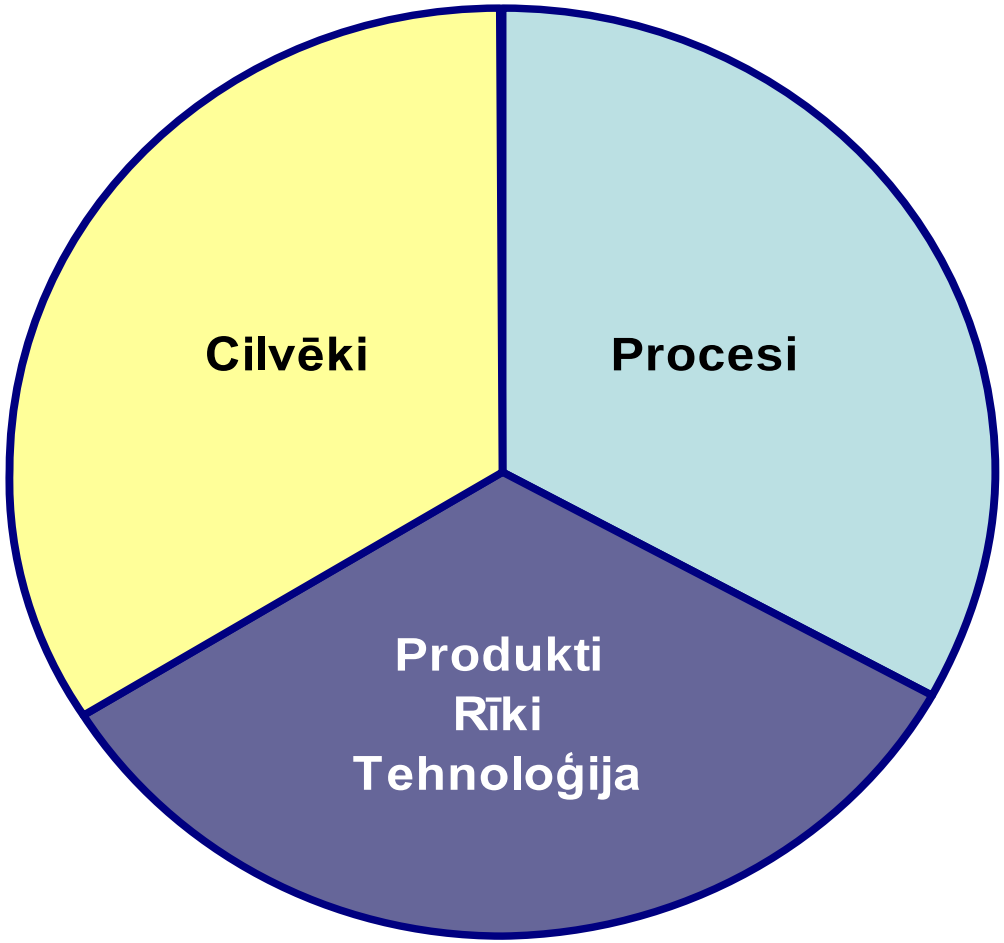
Avots: Top Business/Technology Issues Survey Results, 2011, ISACA

Challenges of Managing IT Risk



Avots: Top Business/Technology Issues Survey Results, 2011, ISACA

IT nav tikai tehnoloģija



Ko organizācija sagaida no IT servisu nodrošinošās struktūrvienības ?

- Sapratne par uzņēmējdarbības funkcijām
- Ātra reakcija
- Skaidrs un saprotams skaidrojums, ko var izdarīt un ko nevar izdarīt
  - Tehnoloģijas
  - Informācijas sistēmas
- Godīga budžeta sastādīšana
- Vienots kontaktpunkts

IT pakalpojumu organizācija

- Iekšēja
  - Centralizēta
  - Decentralizēta
  - Jaukta
- Ārpakalpojums

IT pakalpojumu centralizācija un decentralizācija

- Centralizācija
  - Stratēģija labākai kontrolei
  - Mazām un vidējām organizācijām
- Centralizēt funkcijas
  - Nepieciešama kvalitāte (konsistence, regularitāte)
  - Izmanto kopīgus resursus
  - Kapitālietilpīgas
- Decentralizācija
  - Fleksibilitātes stratēģija
- Decentralizēt funkcijas
  - Nepieciešama operativitāte
  - Izmanto resursus vienas struktūrvienības ietvaros
  - Darbaspēka intensīvas

IT pakalpojumu organizācija

	Latvija			Eiropa		
	Decentralizēts	Daļēji centralizēts	Centralizēts	Decentralizēts	Daļēji centralizēts	Centralizēts
Programmatūras izstrāde	0%	22%	78%	8%	28%	64%
Tehniskais un lietotāju atbalsts	20%	30%	50%	22%	40%	38%
Tīkla pakalpojumi	10%	10%	80%	10%	26%	64%
IT politika/administrācija	0%	10%	90%	5%	15%	80%

Avots: Global Best Practices™

Ārpakalpojumu izmantošanas iemesli

- Iespēja koncentrēties uz uzņēmējdarbības attīstību
- Vieglāk vadīt strauju attīstību un IT sarežģītību
  - Labākas iespējas izmantot jaunākās tehnoloģijas
  - Lielāka pieredze
- Nav nepieciešams komplektēt un uzturēt augstas kvalitātes profesionālo personālu
  - 95% gadījumu nepieciešams tehniķis, 5% - IT speciālists
  - IT personāla skaita samazināšana
- Skaidras izmaksas
  - Izmaksu samazināšanās
- Zemāks IT pakalpojumu izmantotāju apmierinātības līmenis

Ārpakalpojumu izmantošanas trūkumi

- Organizācijai, kas izmanto ārpakalpojumus, ir nepieciešami
  - Pieredzējuši vadītāji
  - Augsts standartizācijas līmenis
- Elastīguma zudums
  - Ārpakalpojuma piegādātāji piedāvā standarta risinājumus, kas nav speciāli pielāgoti organizācijai un tās kultūrai
- Uzņēmums strauji zaudē IT kompetenci
  - Atkarība no ārpakalpojumu sniedzēja

IT pakalpojumu organizācijas vadlīnijas

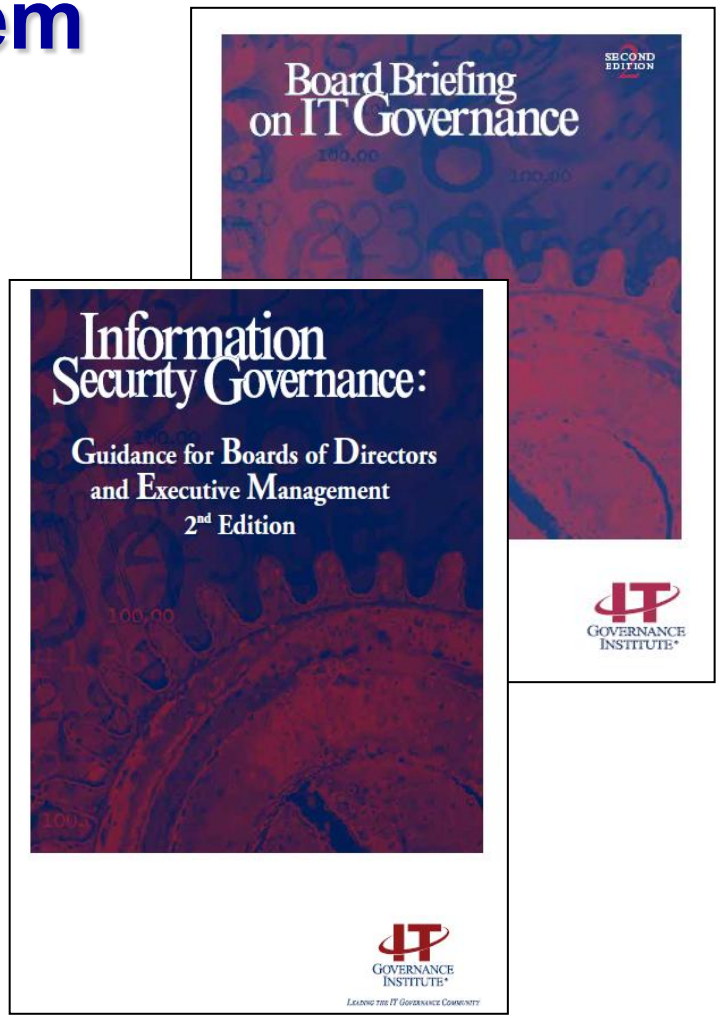
- Sadala IT pakalpojumu sniegšanu skaidri definētos procesos
  - Plānošana
  - Izpilde
  - Kontrole
    - Izmantojot mērījumus
- IT pakalpojumu organizācijas vadlīnijas
  - COBIT
  - ITIL
  - ISO 9001:2000

Kāpēc organizācijas ievieš IT pārvaldības vadlīnijas ?

- Izveidot iekšējās kontroles sistēmu
- Uzraudzīt un kontrolēt IT investīcijas
- Labāka izmaksu kontrole
- Potenciālas atšķirības no konkurentiem
- Autoritatīva direktīva
- Labāka komunikācija organizācijas iekšienē
- Pašnovērtēšanas mehānisma izveide
  - Mērījumu izmantošana

Ievads IT pārvaldībā un drošībā uzņēmumu vadītājiem

- Īss labākās prakses kopsavilkums
- Strukturētas galvenās IT pārvaldes un drošības jomas:
  - IT un uzņēmuma stratēģiju saskaņa
  - Risku pārvaldība
  - Resursu pārvaldība
  - u.c.

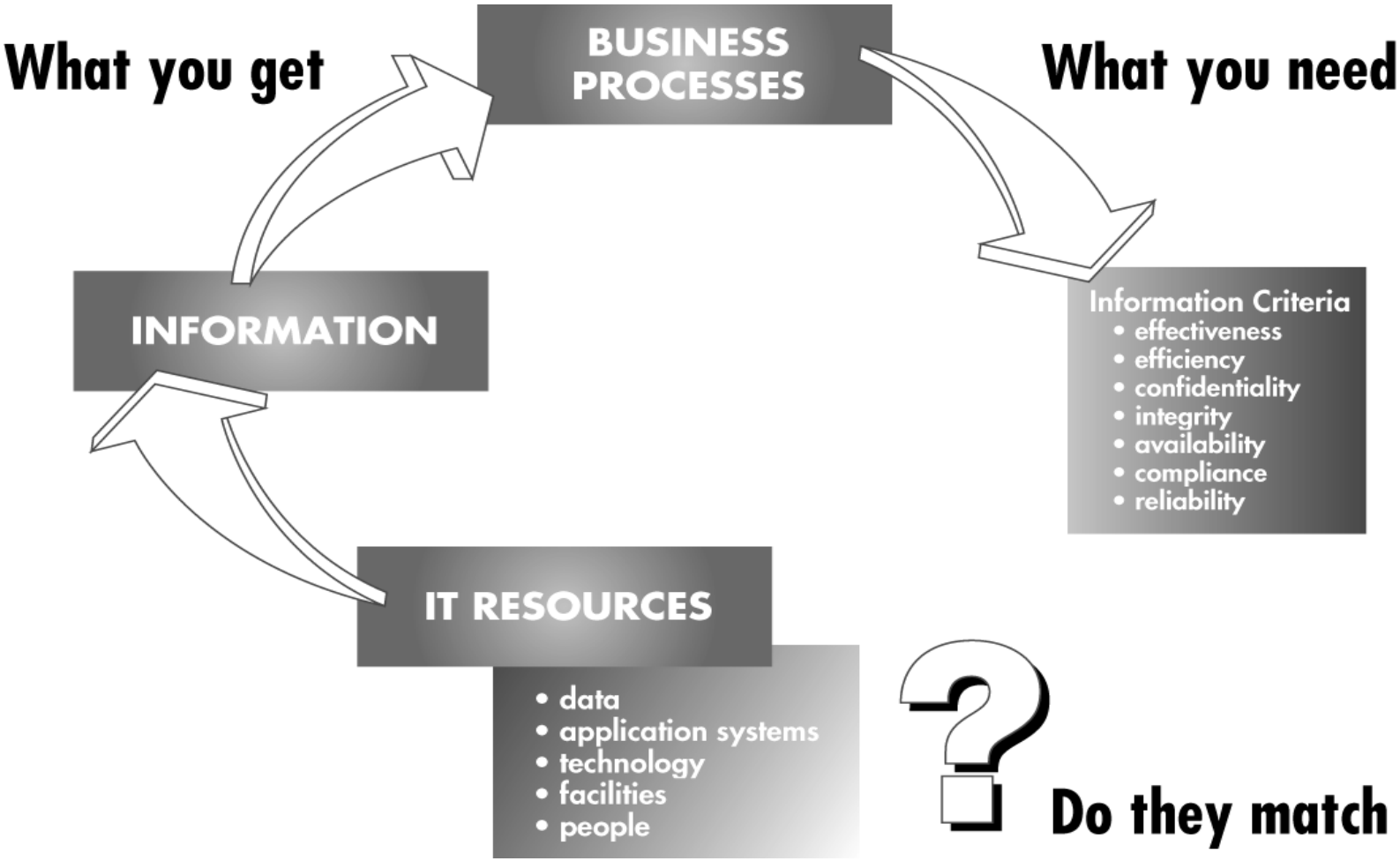


- Pieejami bezmaksas www.itgi.org un www.isaca.org

Kas ir COBIT?

A Business Framework for the Governance and Management of Enterprise IT

CobiT principi



No COBIT 4.1

COBIT

Control **Ob**jectives for **I**nformation and related **T**echnology

- Sāka izstrādāt ISACA 1992.g., pirmā versija 1996.g.
- 2005. gadā izdod COBIT 4.0 un 2007. gadā COBIT 4.1
- Pašlaik izstrādes stadijā ir COBIT 5.0

- Balstīts uz labāko praksi un IT standartiem
- Starptautiski atzītas IT pārvaldības vadlīnijas, kuras iesaka ISACA
  - Saista IT procesus ar organizācijas darbības mērķiem
  - Apraksta metrikas un kritērijus IT procesu vērtēšanai
  - Ietver IT procesu pārvaldības un audita vadlīnijas

www.itgi.org

IT GOVERNANCE INSTITUTE®

www.isaca.org

ISACA®
Trust in, and value from, information systems

COBIT 5 balstīts uz labākās prakses ietvariem un standartiem

- Association for Project Management (APM); *APM Introduction to Programme Management, Latimer, Trend and Co.,* UK, 2007
- British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, UK, 2007
- European Commission, *The Commission Enterprise IT Architecture Framework (CEAF), Belgium, 2006*
- HM Government, Best Management Practice Portfolio, *PRINCE2®, UK, 2009*
- HM Government, Best Management Practice Portfolio, *Information Technology Infrastructure Library (ITIL®), 2011*
- International Organization for Standardization (ISO), 9001:2008 Quality Management Standard, Switzerland, 2008
- ISO/International Electrotechnical Commission (IEC), 20000:2006 IT Service Management Standard, Switzerland, 2006
- ISO/IEC, 27005:2008, Information Security Risk Management Standard, Switzerland, 2008
- ISO/IEC, 38500:2008, Corporate Governance of Information Technology Standard, Switzerland, 2008
- Project Management Institute, Project Management Body of Knowledge (PMBOK2®*), USA, 2008*

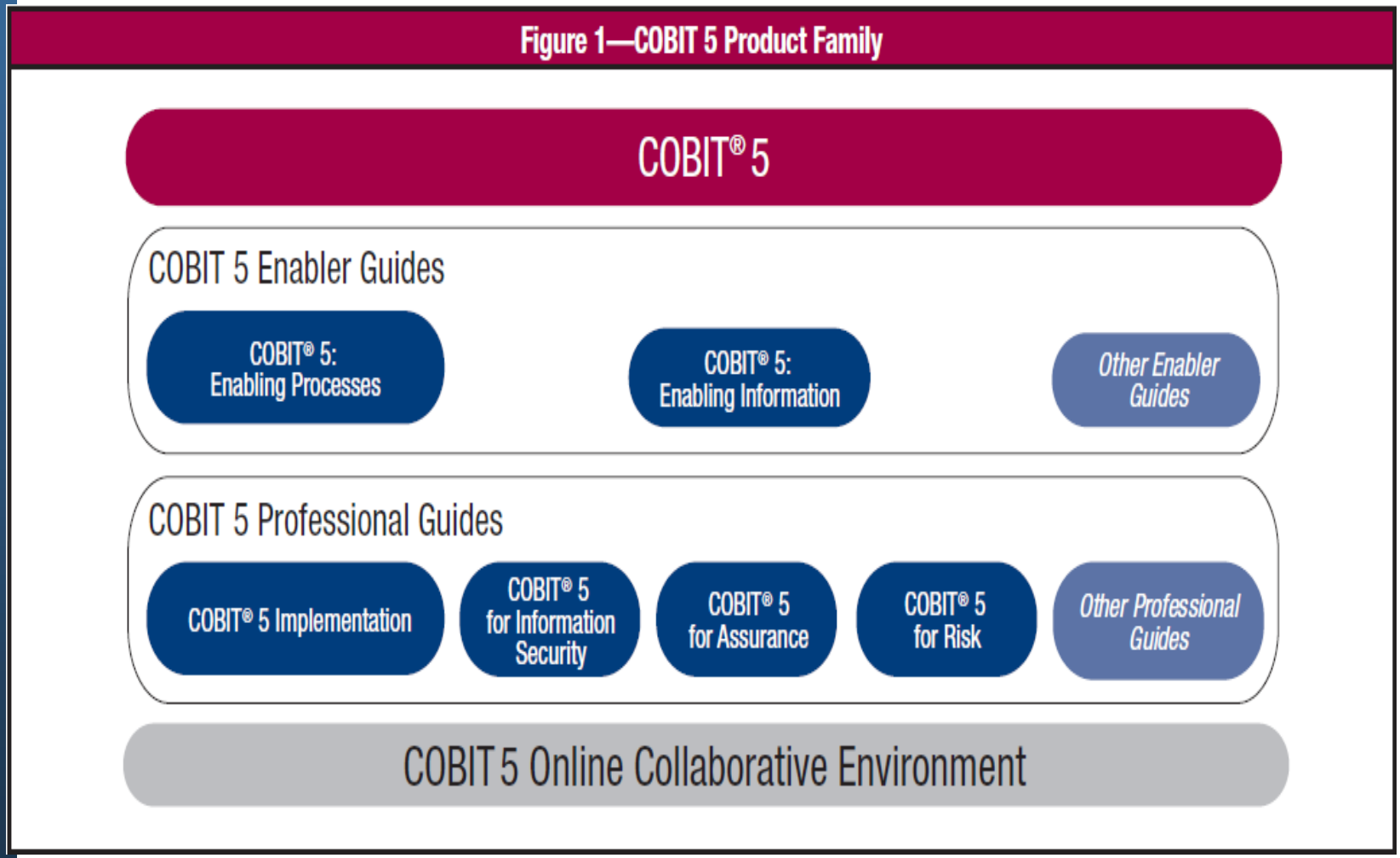
COBIT 4.1 apraksti

- COBIT 4.1 grāmatas

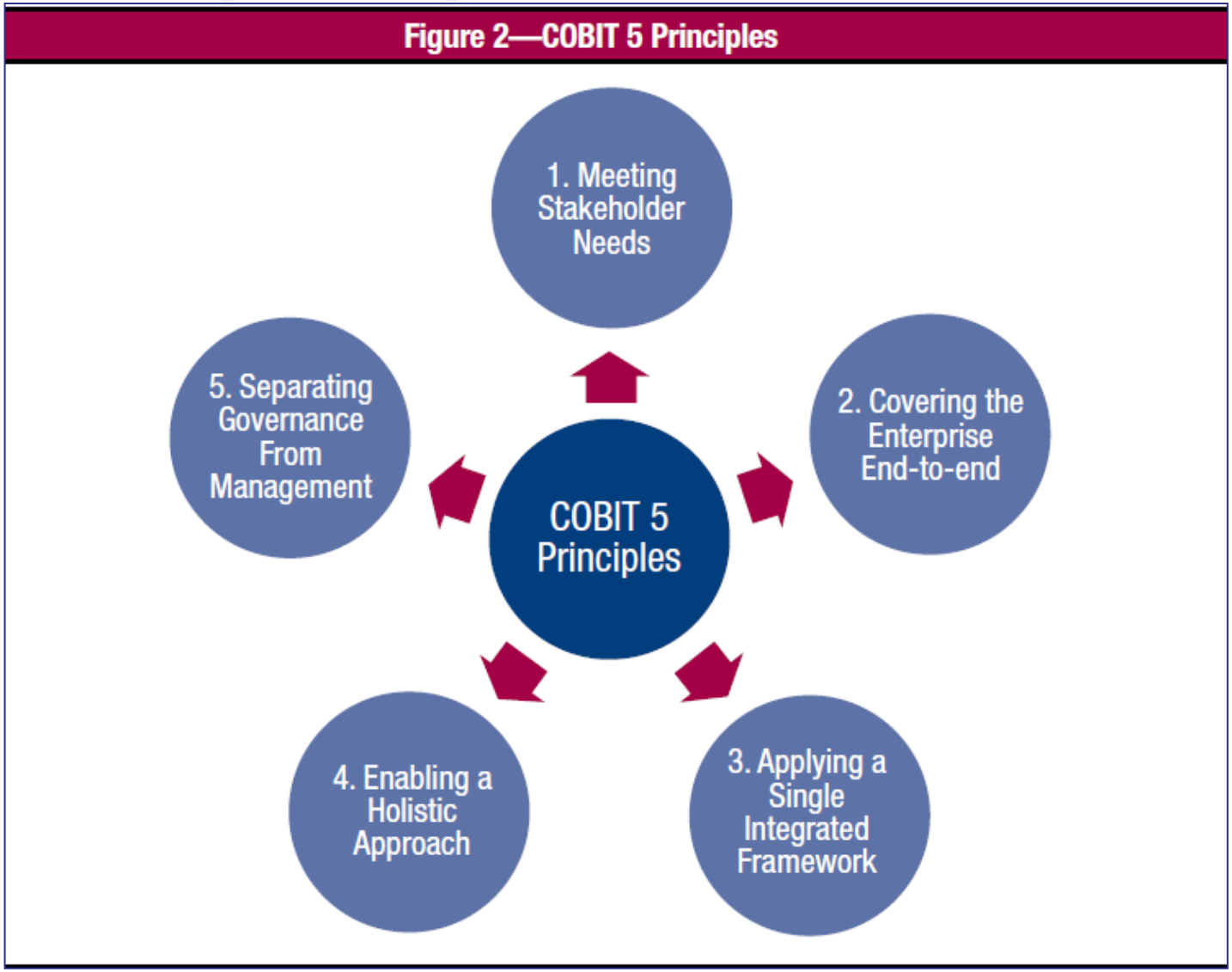
- u.c.

- COBIT interneta versija

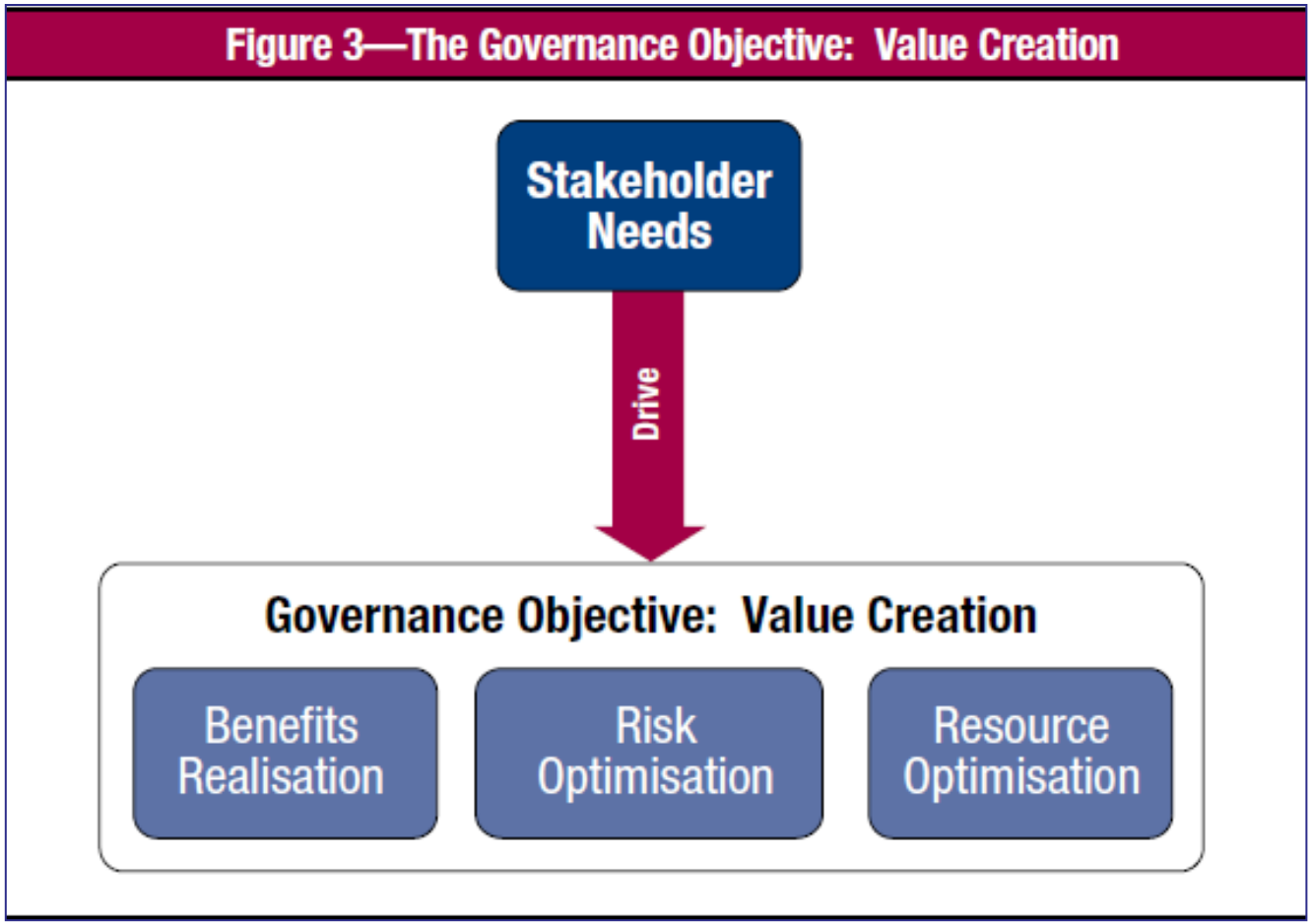
CobiT 5 apraksti



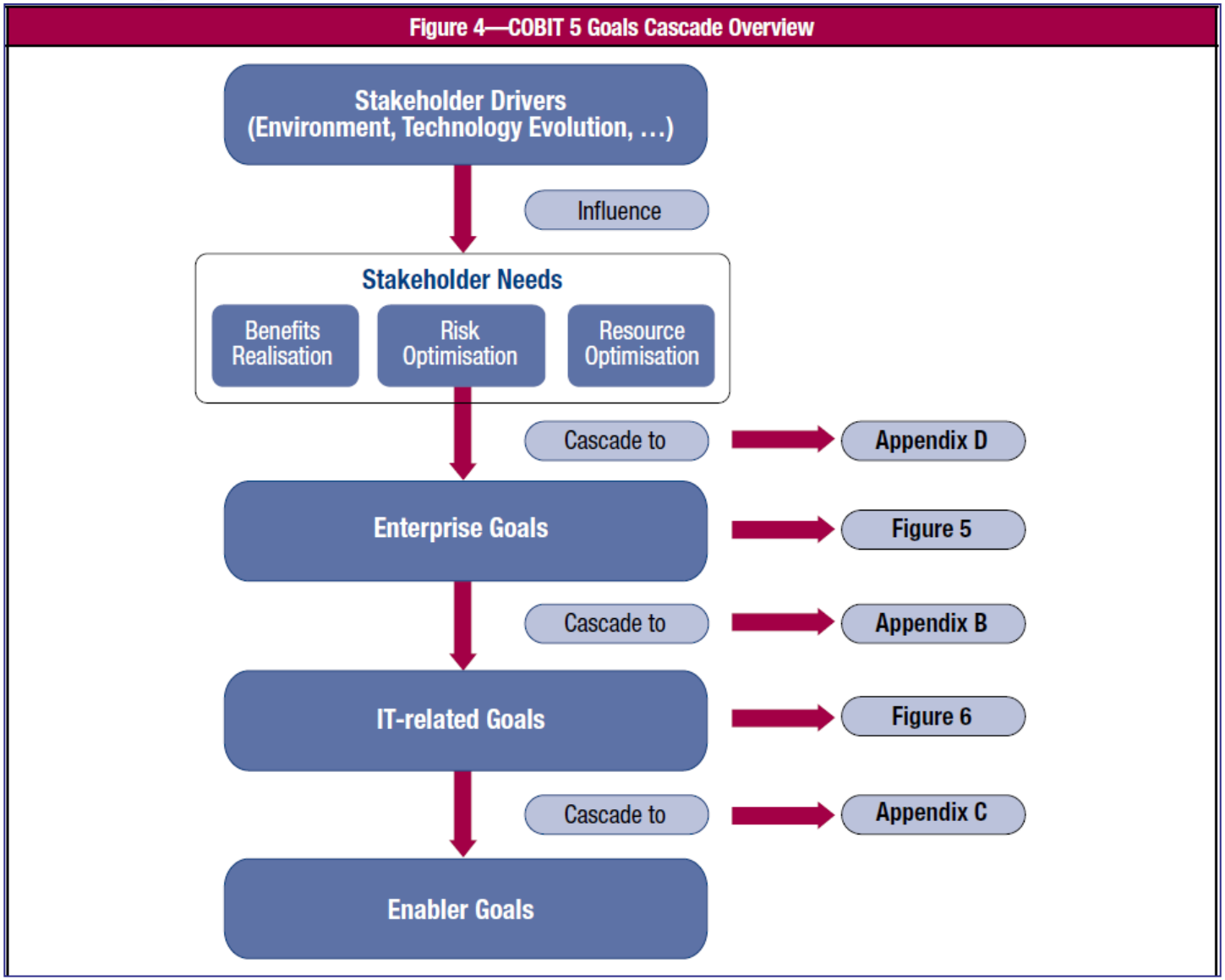
CobiT principi



Meeting Stakeholder Needs



Mērķu kaskadēšana



Pārvaldība un vadība

- **Pārvaldība**
- **Governance** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved, setting direction through prioritisation and decision making, and monitoring performance and compliance against agreed-on direction and objectives.

- **Vadība**
- **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

Dažādu līmeņu mērķi

Figure 5—COBIT 5 Enterprise Goals

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

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

Mērķu sasniegšana ir jāmēra

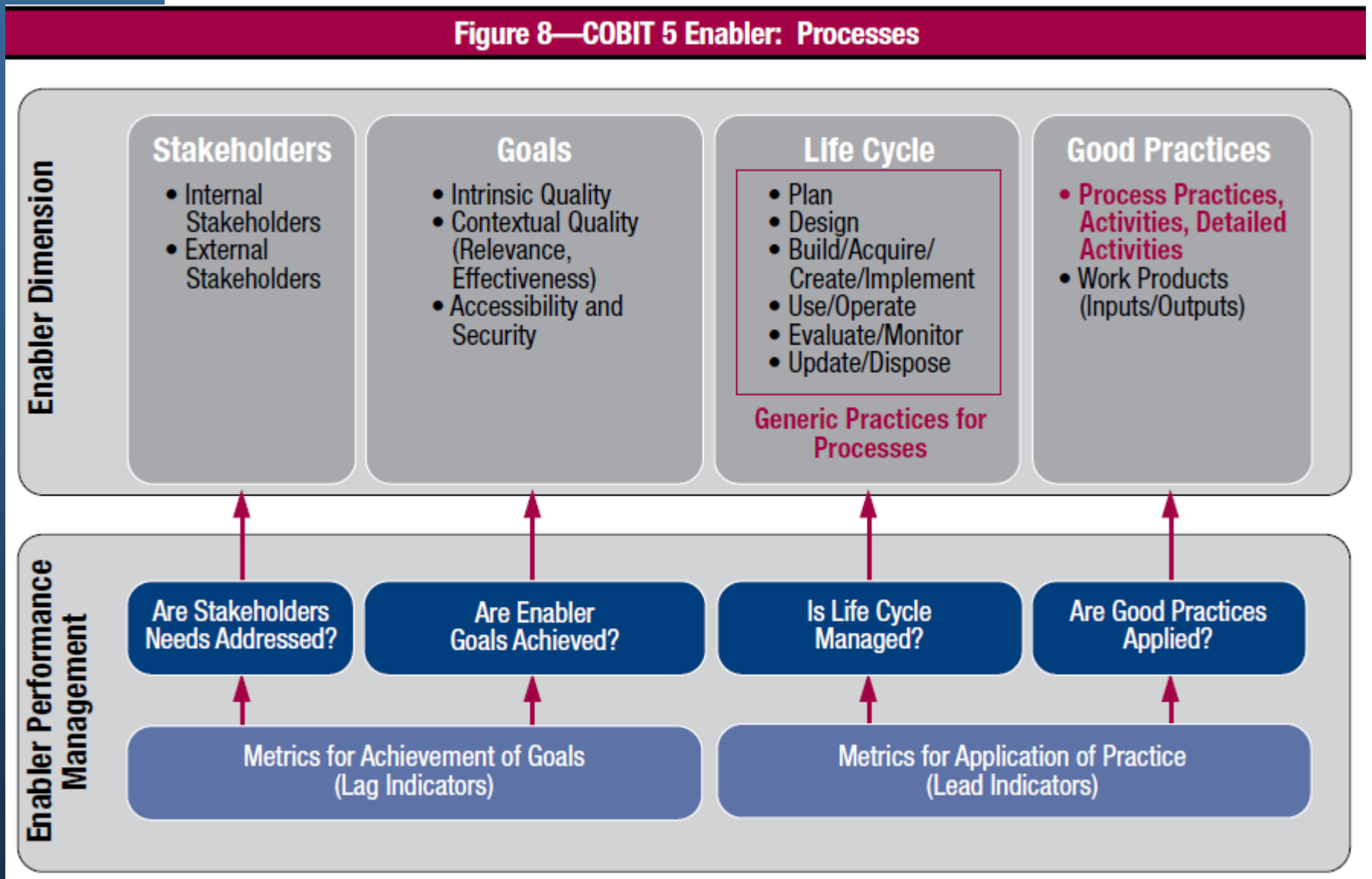
Figure 6—Enterprise Goal Sample Metrics

BSC Dimension	Enterprise Goal	Metric
Financial	1. Stakeholder value of business investments	• Percent of investments where value delivered meets stakeholder expectations • Percent of products and services where expected benefits are realised • Percent of investments where claimed benefits are met or exceeded
	2. Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Ratio of products and services per life cycle phase • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage
	3. Managed business risk (safeguarding of assets)	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents

Figure 7—IT-related Goal Sample Metrics

BSC Dimension	IT-related Goal	Metric
Financial	01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
	02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
	03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions

Enabling Processes – nodrošinošie procesi



Parvaldības un vadības aktivitātes

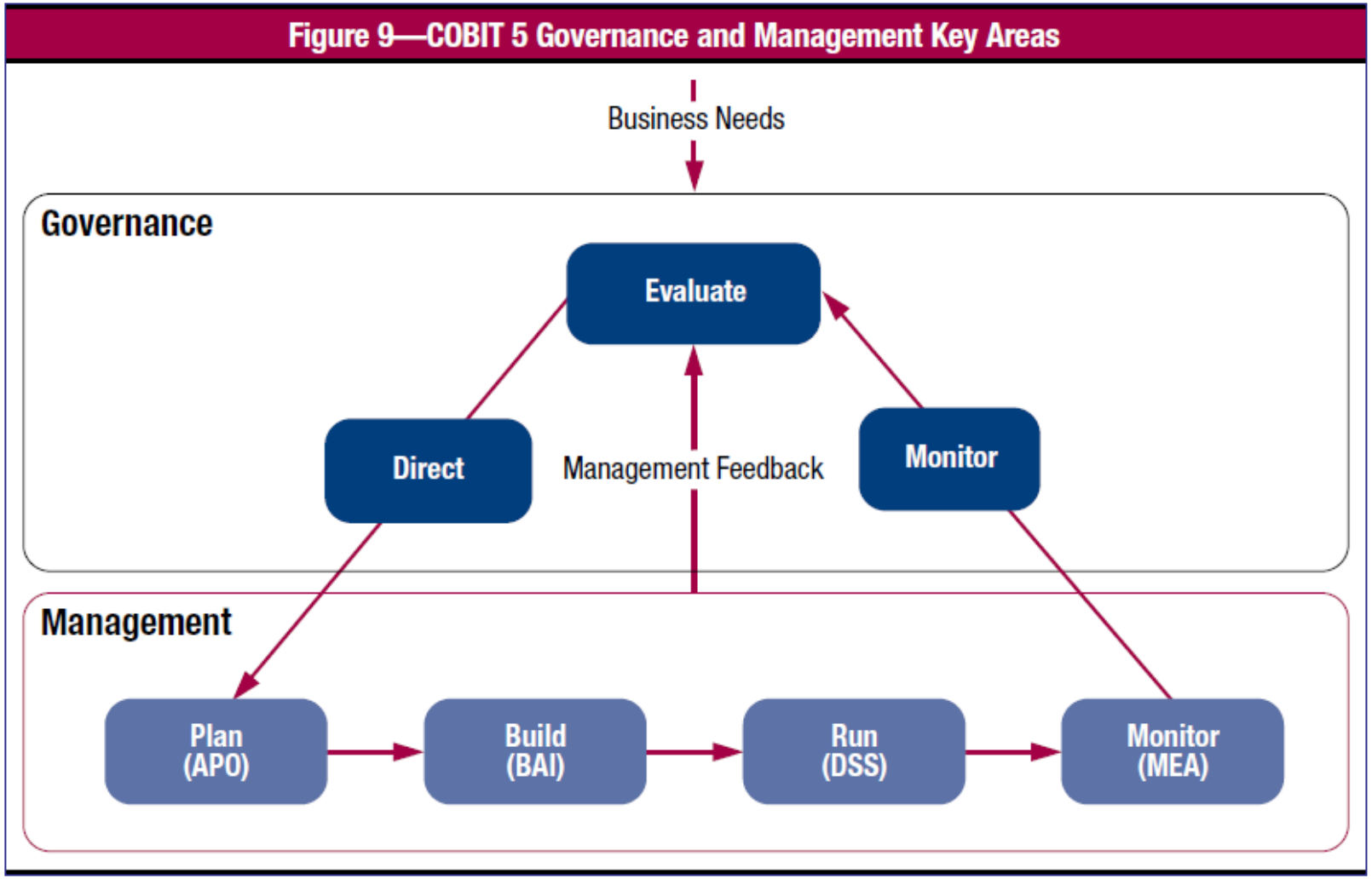
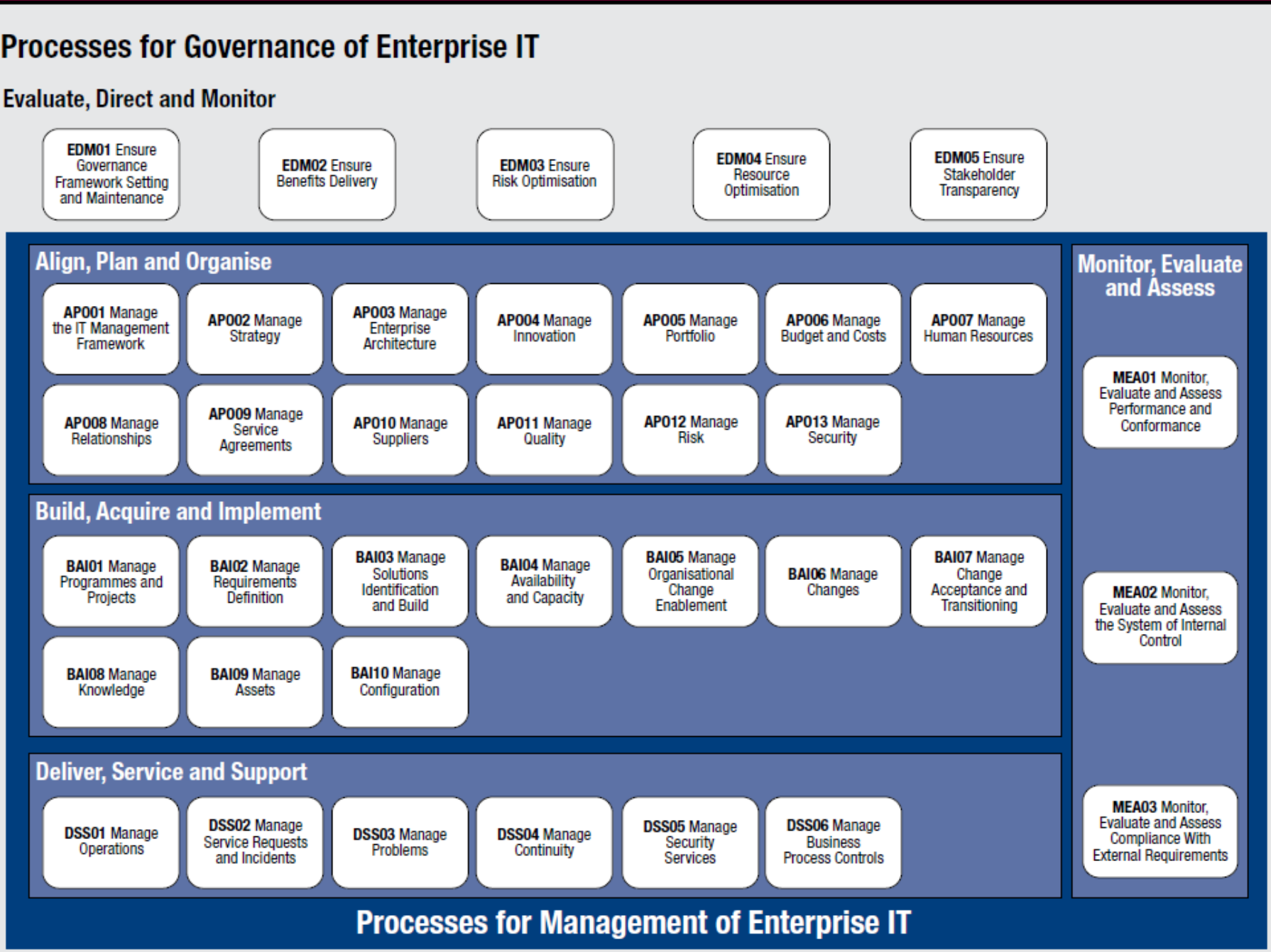


Figure 10—COBIT 5 Process Reference Model



Katram procesam dots

- Procesa identifikācija
- Procesa apraksts
- IT mērķu apraksts un metrikas to mērīšanai
- *RACI chart* – iesaistīto personu atbildību sadalījums
  - R(esponsible) — galvenais izpildītājs
  - A(ccountable) —atbildīgais par veiksmīgu izpildi (zemākais līmenis)
  - C(onsulted) — nodrošina ieejas informāciju u.c. resursus
  - I(nformed) —saņem informāciju un procesa aktivitāšu rezultātus
- Detalizēts procesa “prakšu” (uzdevumu) apraksts
  - nosaukums un apraksts
  - ieejas un izejas
  - veicamās aktivitātes – tālāka detalizācijaProcess activities, further detailing the practices
- Atsauces uz citiem standartiem un vadlīnijām

Piemērs: Konfigurācijas vadība

BAI10 Manage Configuration	Domain: Build, Acquire and Implement

Process Description
Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.

Process Purpose Statement
Provide sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.

The process supports the achievement of a set of primary IT-related goals:

IT-related Goal	Related Metrics
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor

Process Goals and Metrics

Process Goal	Related Metrics
1. Configuration repository is accurate, complete and up to date.	• Number of deviations between the configuration repository and live configuration • Number of discrepancies relating to incomplete or missing configuration information

Piemērs: Konfigurācijas vadība

BAI10 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI10.01 Establish and maintain a configuration model.						C											C	C	C	I	A	R	R			
BAI10.02 Establish and maintain a configuration repository and baseline.																			C	R	A	R	R			
BAI10.03 Maintain and control configuration items.																		A	C	R	R	R	C			
BAI10.04 Produce status and configuration reports.						I											I	I	C	C	A	R	I			
BAI10.05 Verify and review integrity of the configuration repository.						I											R		R	R	A		R			

Piemērs: Konfigurācijas vadība

BAI10 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI10.01 Establish and maintain a configuration model. Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items (CIs) and the relationships amongst them. Include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service.	BAI07.06	Release plan	Scope of configuration management model	Internal
			Logical configuration model	Internal

Activities

1. Define and agree on the scope and level of detail for configuration management (i.e., which services, assets and infrastructure configurable items to include).
2. Establish and maintain a logical model for configuration management, including information on configuration item types, configuration item attributes, relationship types, relationship attributes and status codes.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI10.02 Establish and maintain a configuration repository and baseline. Establish and maintain a configuration management repository and create controlled configuration baselines.	BAI09.05	Register of software licences	Configuration repository	BAI09.01 DSS02.01
			Configuration baseline	BAI03.11

Activities

1. Identify and classify configuration items and populate the repository.
2. Create, review and formally agree on configuration baselines of a service, application or infrastructure.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI10.03 Maintain and control configuration items. Maintain an up-to-date repository of configuration items by populating with changes.	BAI06.03	Change request status reports	Updated repository with configuration items	DSS02.01

Process Capability Model – Procesa spēju/spējīguma modelis

- Raksturo procesa īstenošanas pilnīguma un kvalitātes pakāpi
- **0 Incomplete process —** The process is not implemented or fails to achieve its process purpose
- **1 Performed process —** The implemented process achieves its process purpose
- **2 Managed process —** The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained
- **3 Established process —** The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes
- **4 Predictable process —** The previously described established process now operates within defined limits to achieve its process outcomes
- **5 Optimising process —** The previously described predictable process is continuously improved to meet relevant current and projected business goals
- Izmantotas idejas no Maturity Model (brieduma modeļa) 5 pakāpēm

Brieduma līmeņi – izmanto iepriekšējās COBIT versijās CMM u.c.

0 Non-existent. Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined. Procedures have been standardised and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Ieviešanas process

- Izskatīt COBIT procesus, izvēloties piemērotākos savas organizācijas darbības uzlabošanai
- Analizēt riskus, kas traucē sasniegt izvēlētos mērķus
- Izvēlēties indikatorus un noteikt mērījumu kārtību
- Izvēlēties monitoringa procedūras, kas kontrolētu izvirzīto mērķu sasniegšanu
- Ieviest procesus un uzraudzīt to izpildi

IT pārvaldības vadlīniju ieviešana

- Iniciatīva nāk no IT departamenta
- Ieviešana virzienā no augšas uz leju
  - Uzņēmuma vadības iepazīstināšana ar vadlīnijām
    - Atgriezeniskās saites nodrošināšana
  - Vidējā līmeņa vadītāju iepazīstināšana ar vadlīnijām
  - “Reklāmas kampaņa” uzņēmumā
- IT pārvaldības vadlīniju ieviešana kā projekts
  - Plānošana
  - Izpilde
  - Kontrole
  - Nepieciešama nepārtraukta uzturēšana