Is Governance relevant?

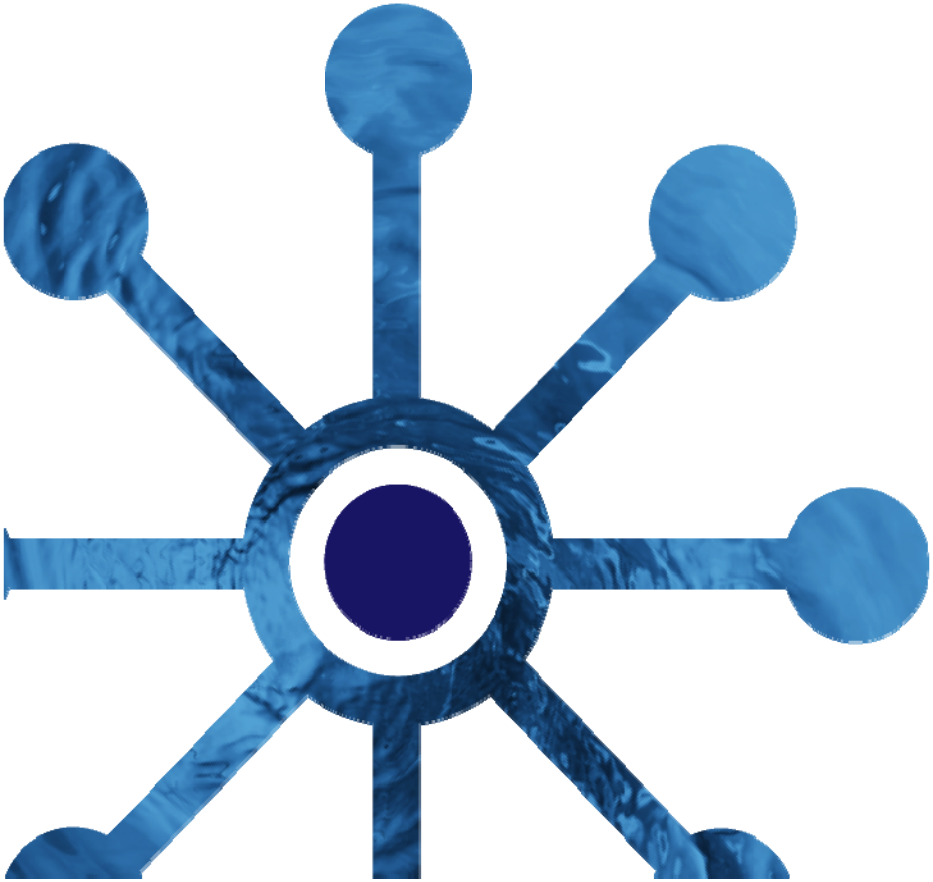
Robert E Stroud CGEIT CRISC

November 2013

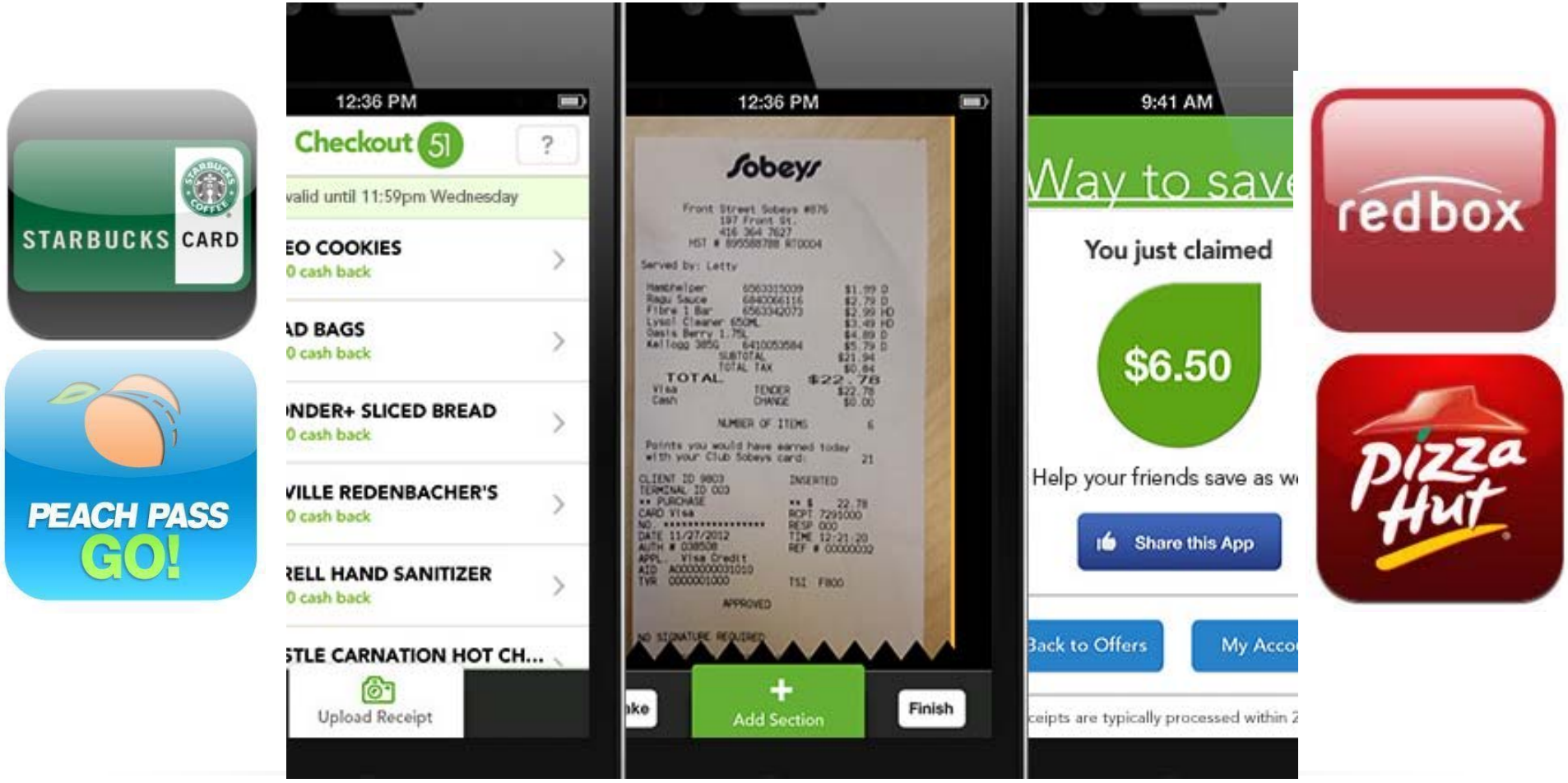
Robert Stroud

- Vice President, Strategy & Innovation
- 15+ years Banking Industry
- Author, speaker, social media luminary & futurist
- IT Governance
  - Past International VP ISACA¥ITGI & member ISACA Strategic Advisory Council
  - Former Chair COBIT Steering Committee
- ITSM
  - Former Treasurer, itSMF International Executive Board Director Audit, Standards and Compliance
  - Member ITIL V3 Advisory Group (IAG) & ITIL v3 Update Board
  - Contributor ITIL Business Perspectives Volume II

The transition has began!
Are you watching or driving?



From coffee to pizza to tolls. . .



ca technologies

Canada National Railway

- Sensing in real-time the position of rolling stock, track switches, level crossings, platforms, signals, and more, to optimize the routing, switching, and prioritization of its rolling stock to reduce travel times and improve profitability.

First Data Corporation

Tesco Homeplus - KOREA

Big Data Hits Real Life: Brick-and-mortar stores are looking for a chance to using software that allows them to watch customers as they shop, and gather da

By STEPHANIE CLIFFORD and QUENTIN HARDY

Published: July 14, 2013 | 410 Comments

3D + Printing = 3D Printing

- 3D Printing is a phrase used to describe the process of creating three dimension objects from digital file using a materials printer, in a manner similar to printing images on paper
- Radically changing the way we deliver goods

3D printing will change you and global economics

U.S. Home | Crime | Terrorism | Economy | Immigration | Disasters | Military | Education | Environment | Pe

Homeland Security bulletin warns 3D-printed guns may be 'impossible' to stop

By Jana Winter / Published May 23, 2013 / FoxNews.com

Print
Email
Share

EXCLUSIVE: A new Department of Homeland Security intelligence bulletin warns it could be "impossible" to stop 3D-printed guns from being made, not to mention getting past security checkpoints.

- 3D printing will make it possible to print (build) anything
- Allow printing ¥ manufacturing locally
- How will governance ¥ compliance be managed

http://www.foxnews.com/us/2013/05/23/govt-memo-warns-3d-printed-guns-may-be-impossible-to-stop/

3D Printing of human parts

- Using “stem” cell technology we will soon be able to “print” (create) replacement parts for people
- Governance will be crucial

Integration of big data, analytics and real time information

- Drive you to the office or station and safely park
- Safer than a human
- Can you give up control

Robotics from factory to knowledge worker!

The transition has began!

41

Average # of apps per device

25

Number of mobile apps CIO's expect to deploy in the next 2 years

1 Trillion

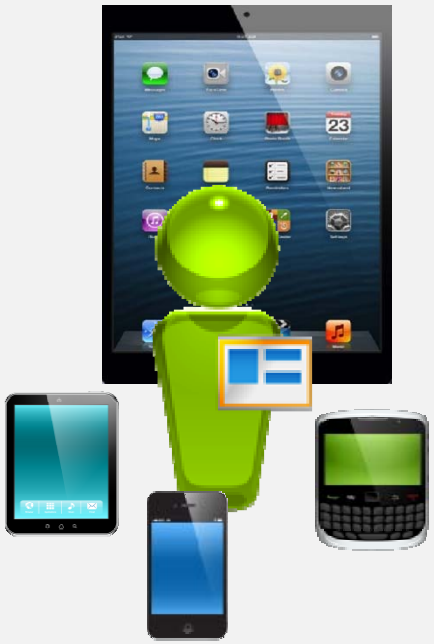
Approx Number of transactions processed through API's

ca technologies

Key inhibitors - from being, well 'just human', to slow execution

3.3

Average # of connected devices per knowledge worker by 2014



20+ Million

# of Jailbreaks using just one tool

$167,000

One employees telecom expense bill

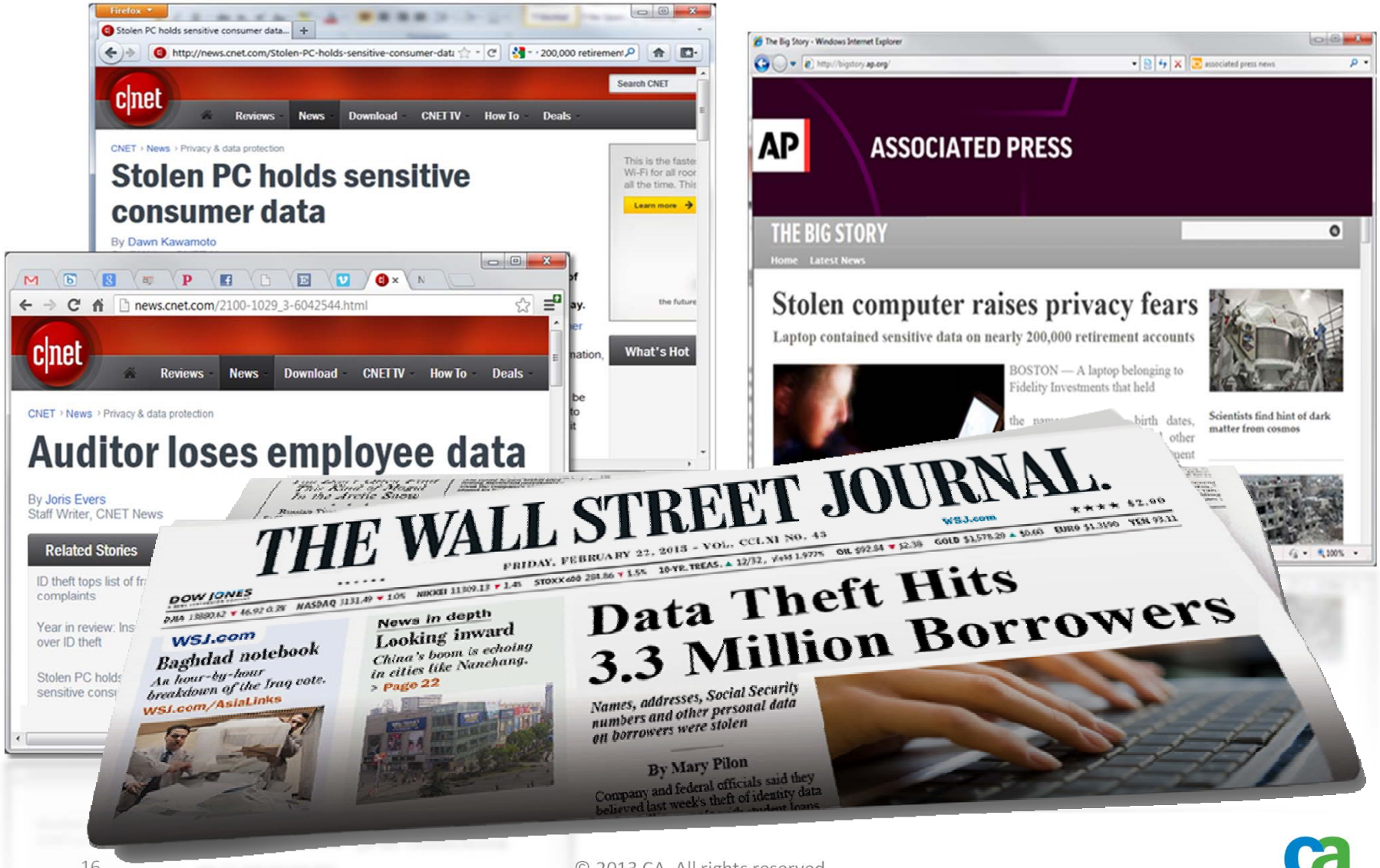
66%

software dev projects challenged or fail

…but apps can have a life of days, even minutes!

ca technologies

We have to balance innovation & risk



We are in changing times – are you ready?

Twenty-five Percent Of Companies Will Have A Chief Digital Officer In Two Years

CIO.com, 2013

CIOs May Become Irrelevant, Replaced By The CMO and The CDO

Who's Who of FSI, 2013

The CIO Will Be Diminished And Likely Eliminated At Many Companies

Information Week, 2012

IT is transitioning

Capabilities of the new CIO

Portfolio Management

- Demand Management
- Investment Management
- Resource and Capacity Planning

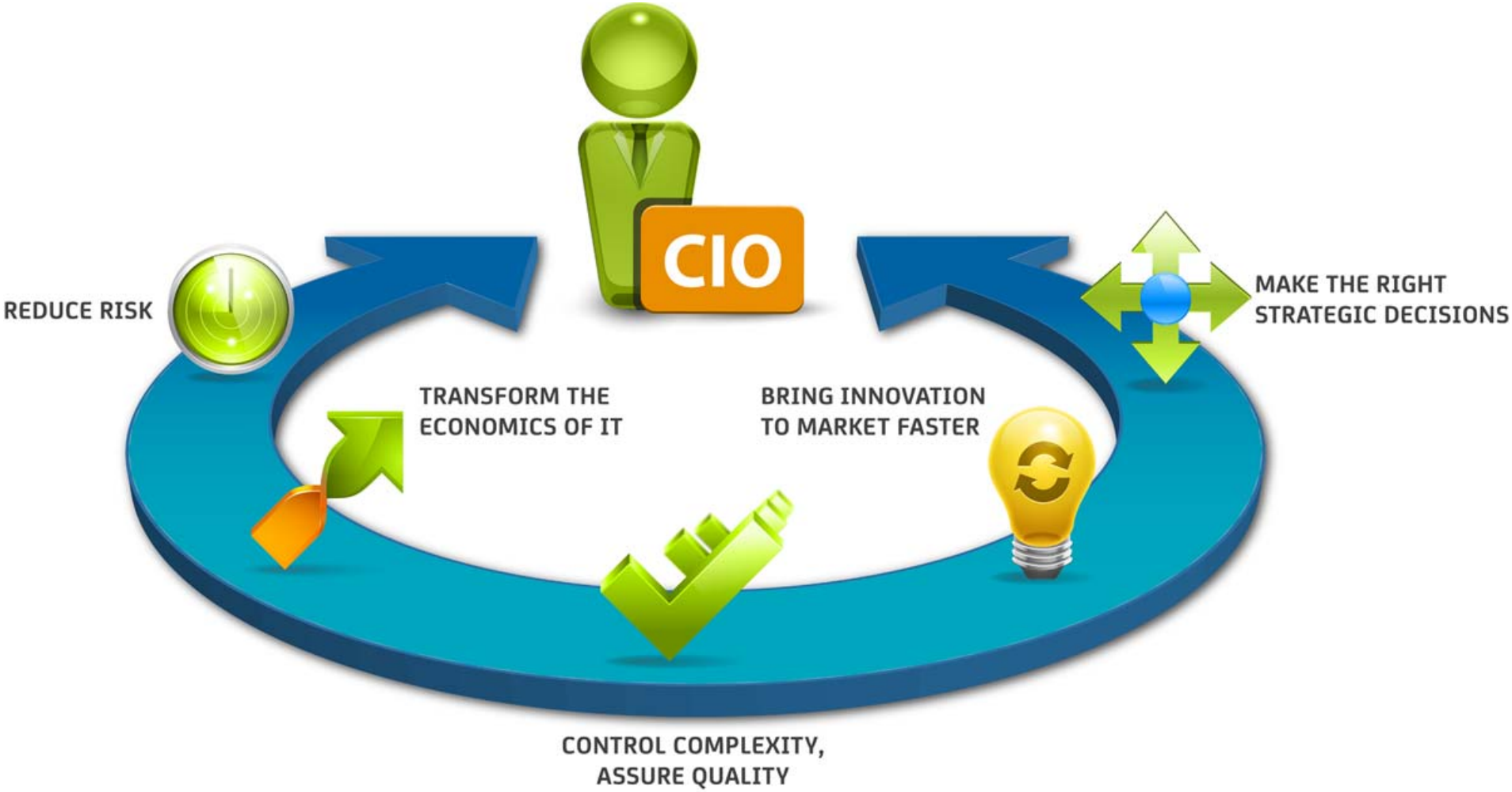
Financial Management

- Budgeting and Forecasting
- Cost Management
- Detailed Financial Analysis

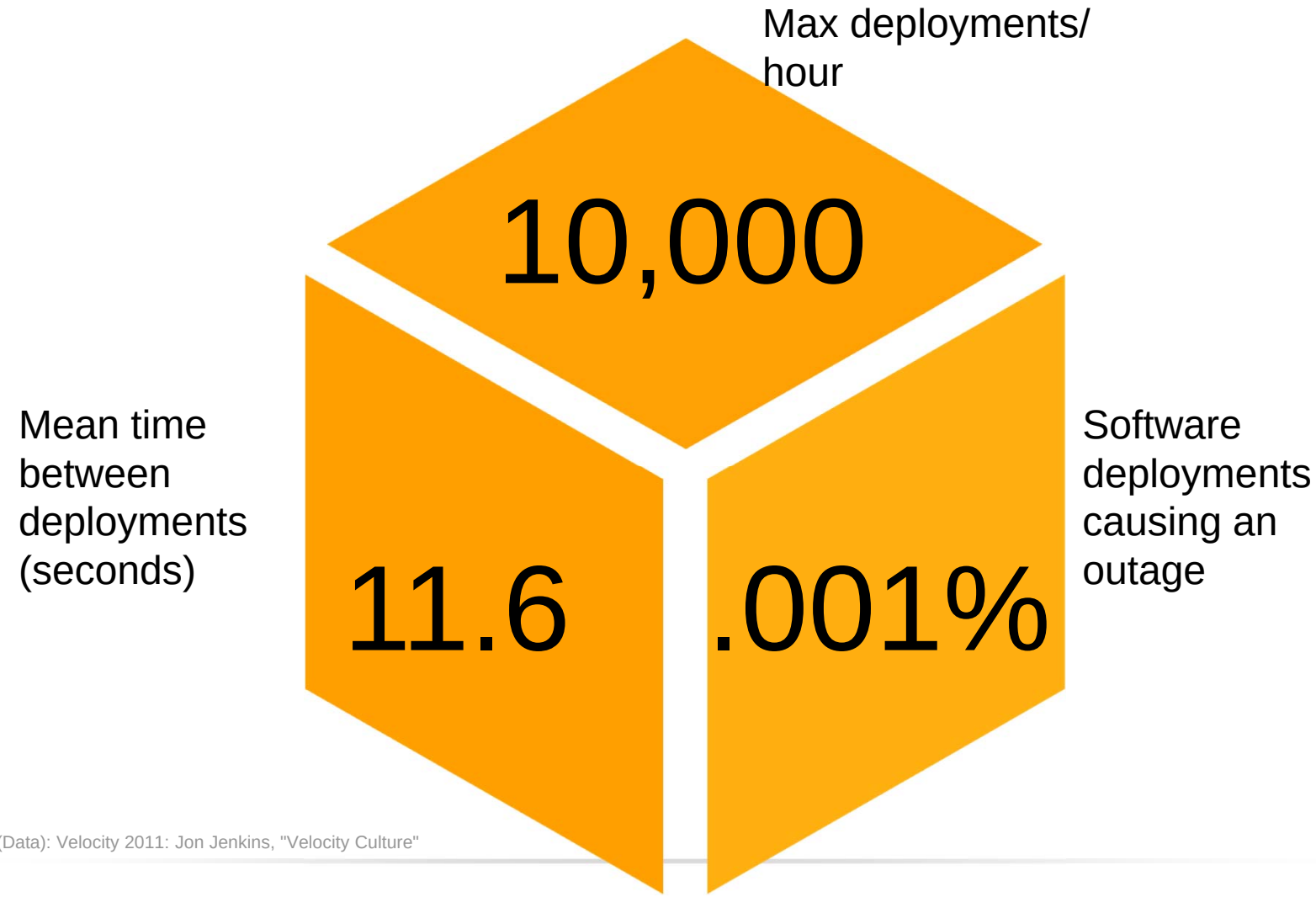
Relationship Management

- Performance and Benchmarking
- Contract Management
- Vendor Management

Balance Risk and Transform for Business Value



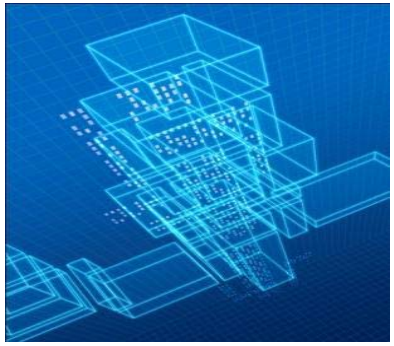
Amazon AWS are delivering up to 10K deployments per hour with .001% causing an outage



Source (Data): Velocity 2011: Jon Jenkins, "Velocity Culture"

We need to drive the change or we will be changed!

Using cloud services delivers measurable benefits



have deployed a SaaS app.

discrete services

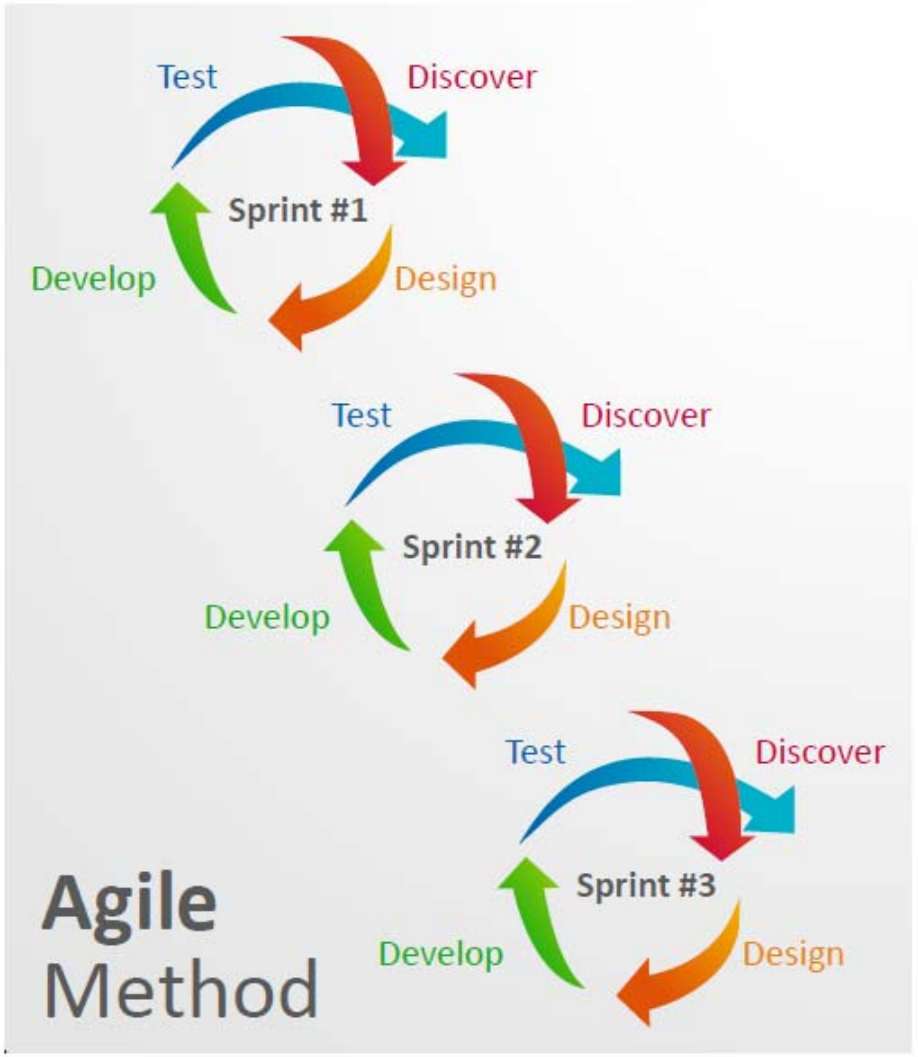
to SaaS increases revenue

cloud for 3 years or more

performance, scalability and resiliency

Source: global research of 450 IT leaders conducted by Luth Research and Vandson Bourne, commissioned by CA Technologies.

Waterfall to agile – how do we govern?



30 – 50% faster time to market

80 – 100% improvement in quality

20 – 30% reduction in cost

Effectively balance risk with outcomes

We need to leverage effective governance more than ever!

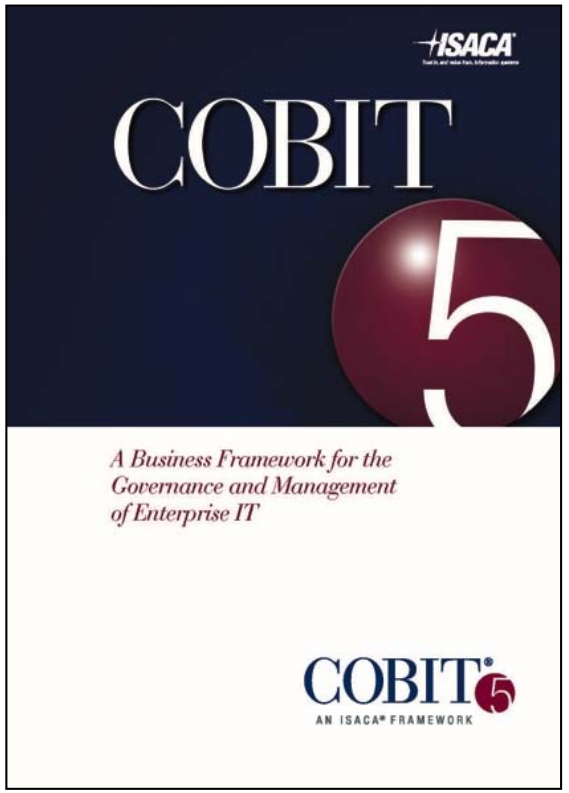
COBIT, ITIL, PmBok, ISO 27000 delivering value in a large global bank

- Rapidly growing globally focused on growth emerging markets
- Technology central to the solution and growth
- Changing demographics mobility
- Framework for measuring value and assuring value to the market

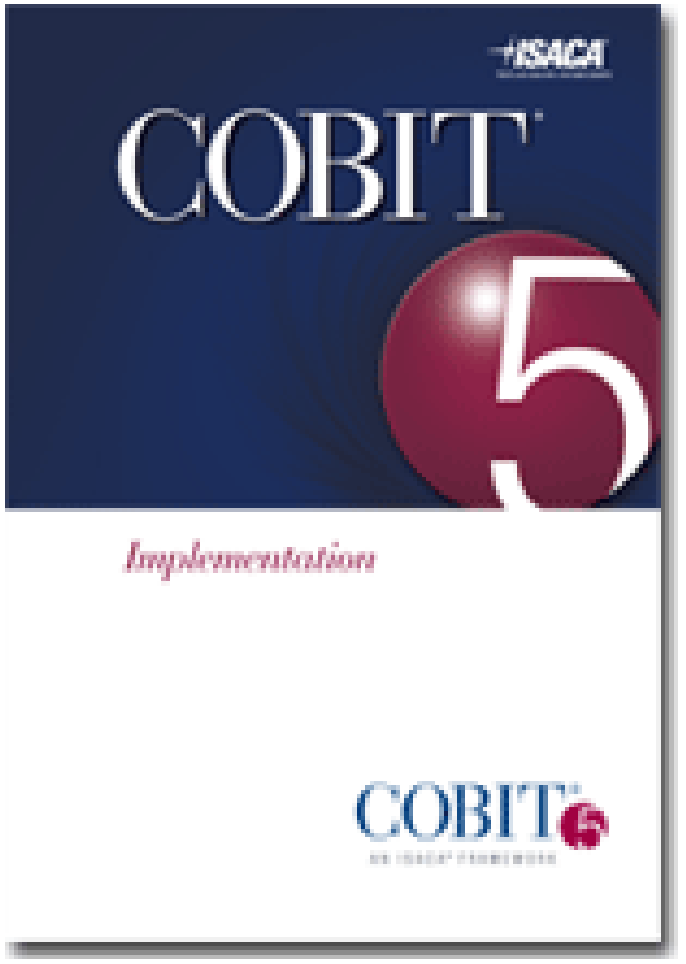
28

COBIT 5 – A business framework for the governance and management of enterprise IT

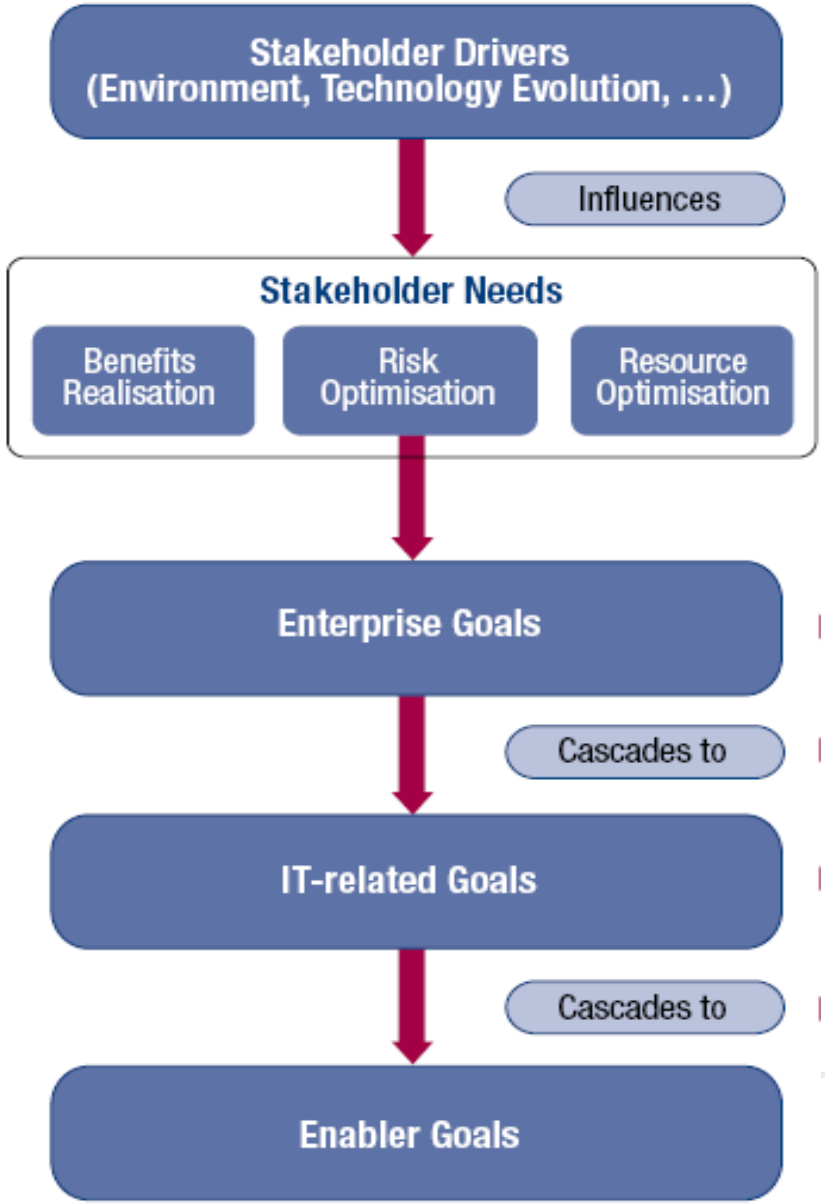
- EU adopts COBIT for agricultural paying agencies
- COBIT adopted by Paraguayan Superintendent of Banks
- COBIT adopted in Argentina and Uruguay
- Lebanese banks endorse COBIT
- Auditor General of Quebec adopts COBIT
- US National Institute of Standards and Technology references COBIT
- US House of Representatives adopts COBIT/Office of Inspector General implements and uses COBIT
- Australian National Audit Office uses COBIT in IT audits
- Philippine Commission on Audit (COA) adopts COBIT
- US Department of Defense, Office of Inspector General, adopts COBIT



Implementing effective GRC leveraging COBIT 5



Meeting Stakeholder Needs



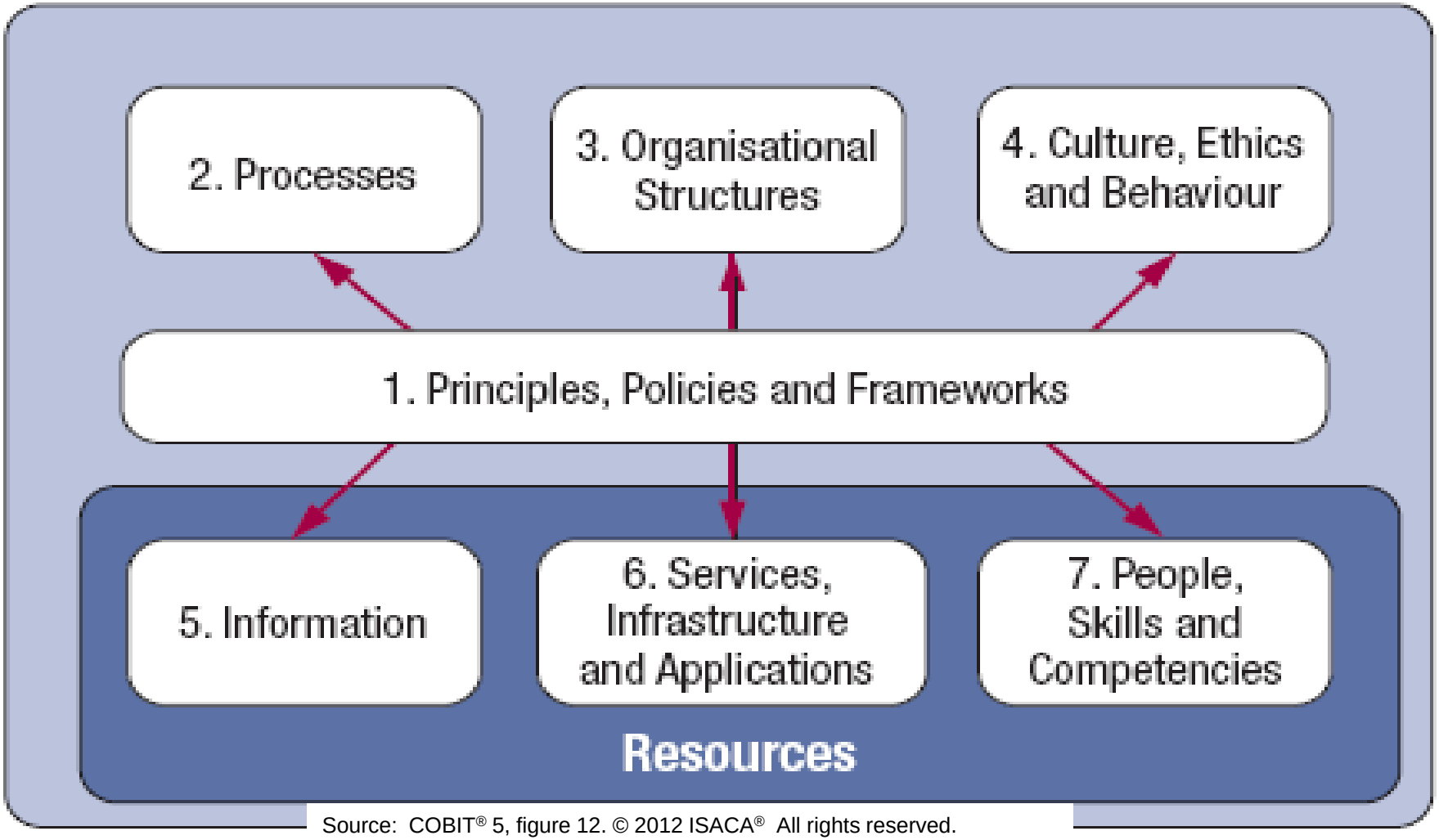
Stakeholder Value to Business Objectives

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		

Source: COBIT® 5, figure 5. © 2012 ISACA® All rights reserved.

32

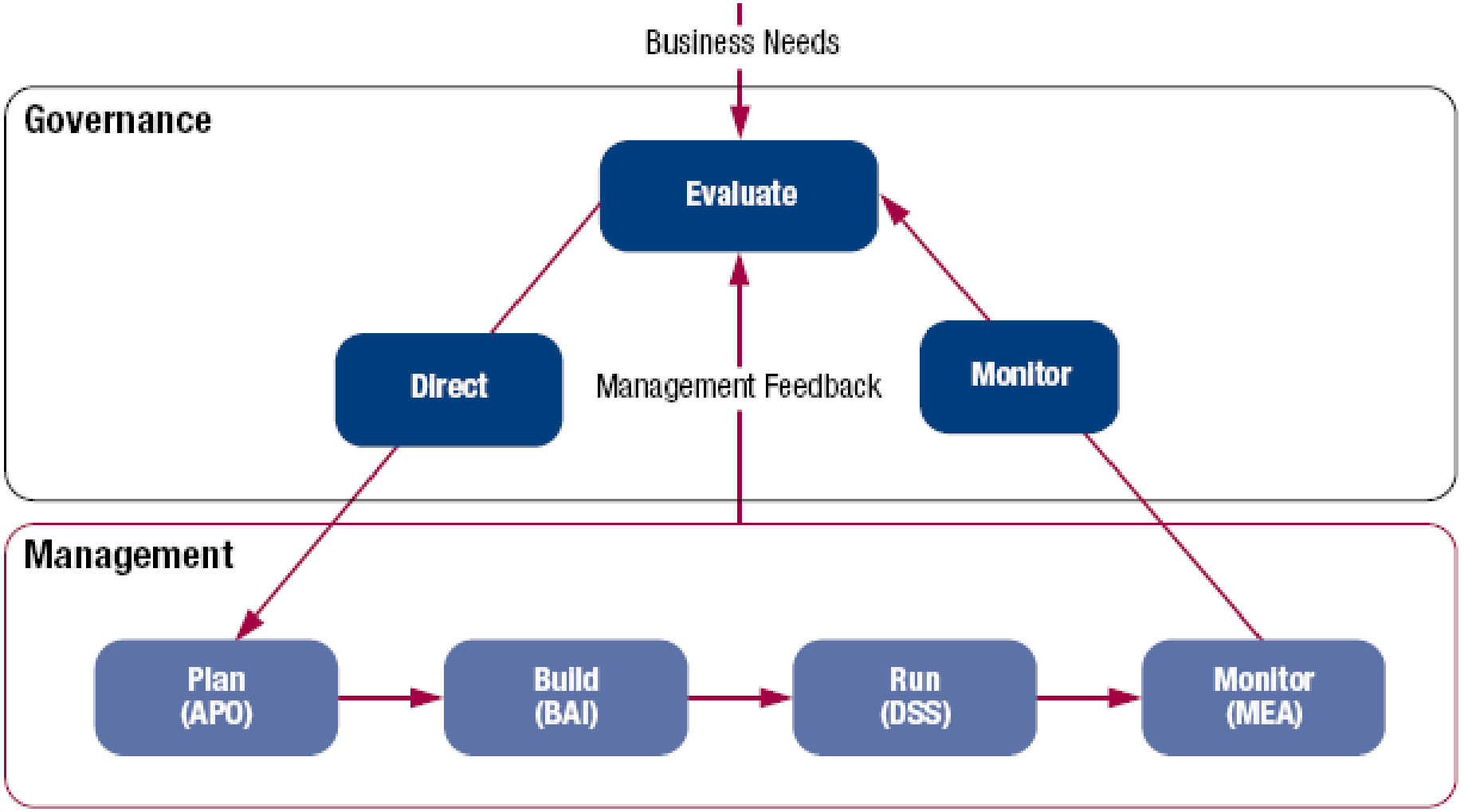
Balanced approach



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

33

Governance and Management are different



Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.

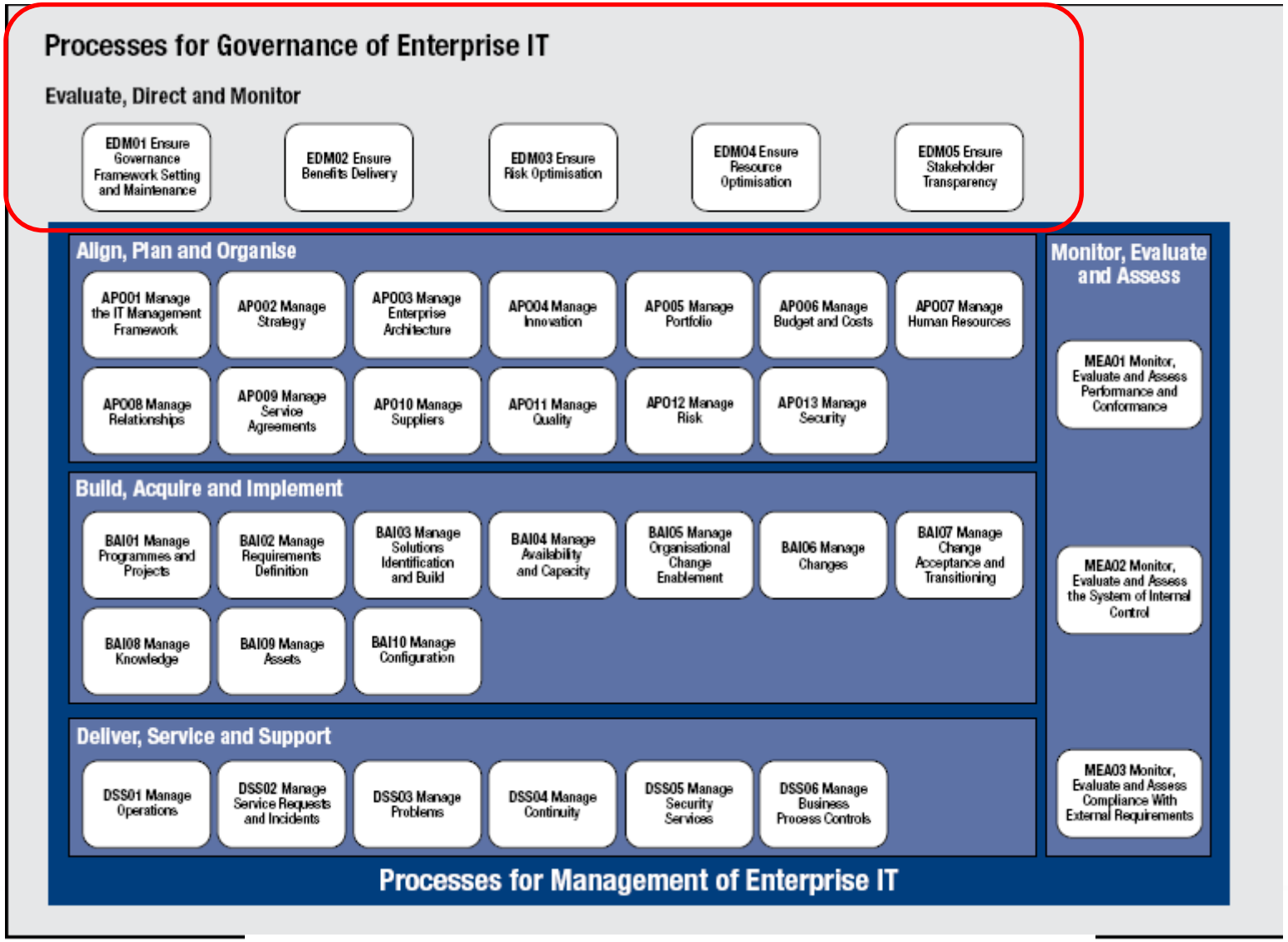
34

Governance and management ARE DIFFERENT!

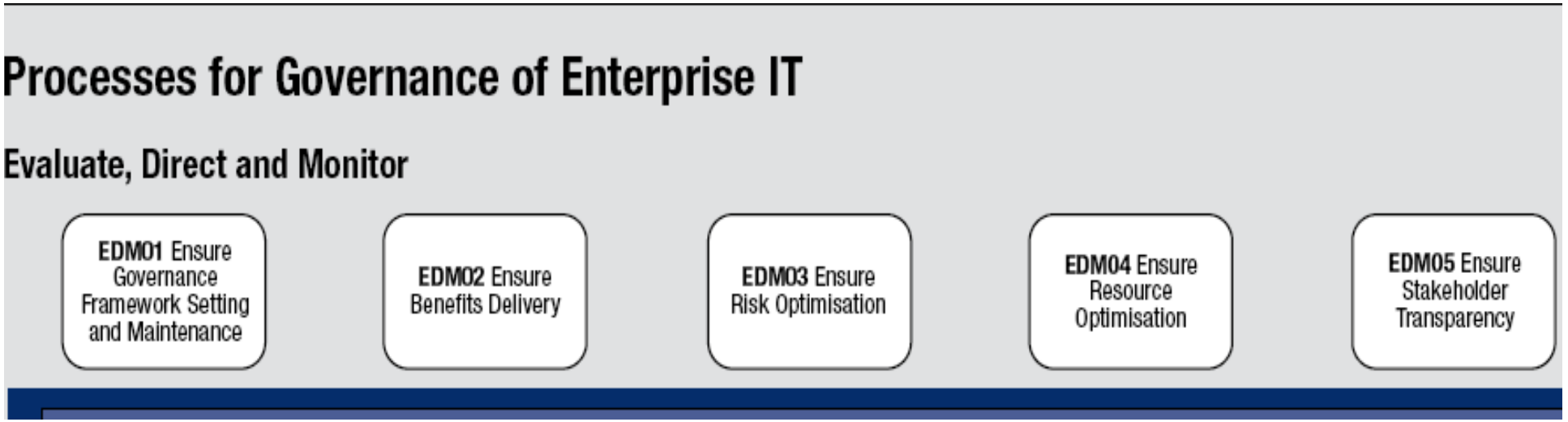
- Governance ensures stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives are achieved; setting direction through prioritisation, decision making; and monitoring performance and compliance against agreed-on direction and objectives (EDM).
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

35

Governance in COBIT 5 (cont.)



COBIT 5: Enabling Processes (cont.)



- 01 Ensure governance framework setting and maintenance.
- 02 Ensure benefits delivery.
- 03 Ensure risk optimisation.
- 04 Ensure resource optimisation.
- 05 Ensure stakeholder transparency.

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.

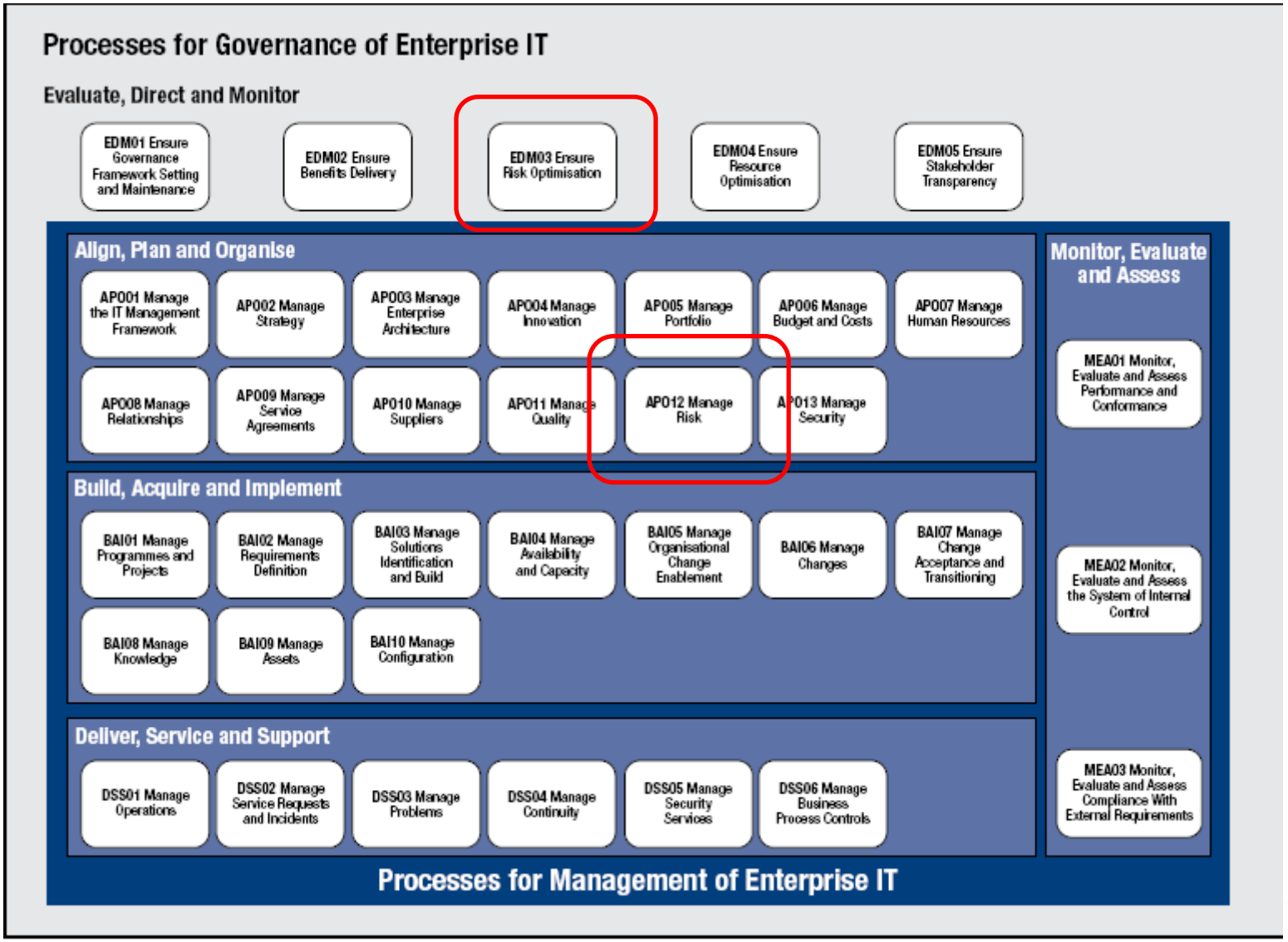
Risk Management in COBIT 5

- The GOVERNANCE domain contains five governance processes, one of which focuses on stakeholder risk-related objectives: **EDM03 Ensure risk optimisation.**
  - **Process Description**
    - Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.
  - **Process Purpose Statement**
    - Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.

Risk Management in COBIT 5 (cont.)

- The MANAGEMENT Align, Plan and Organise domain contains a risk-related process: **APO12 Manage risk.**
  - **Process Description**
    - Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.
  - **Process Purpose Statement**
    - Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

Risk Management in COBIT 5 (cont.)



Risk Management in COBIT 5 (cont.)

- All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities
  - EDM03 Ensure risk optimisation ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated.
  - APO12 Manage risk provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise.
  - All other processes include practices and activities that are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer/accept).

Risk Management in COBIT 5 (cont.)

- In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process. **These include risk-related roles.**

APO12 RACI Chart

Align, Plan and Organise	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
Key Management Practice																										
APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Source: *COBIT® 5: Enabling Processes*, page 108.

ca technologies

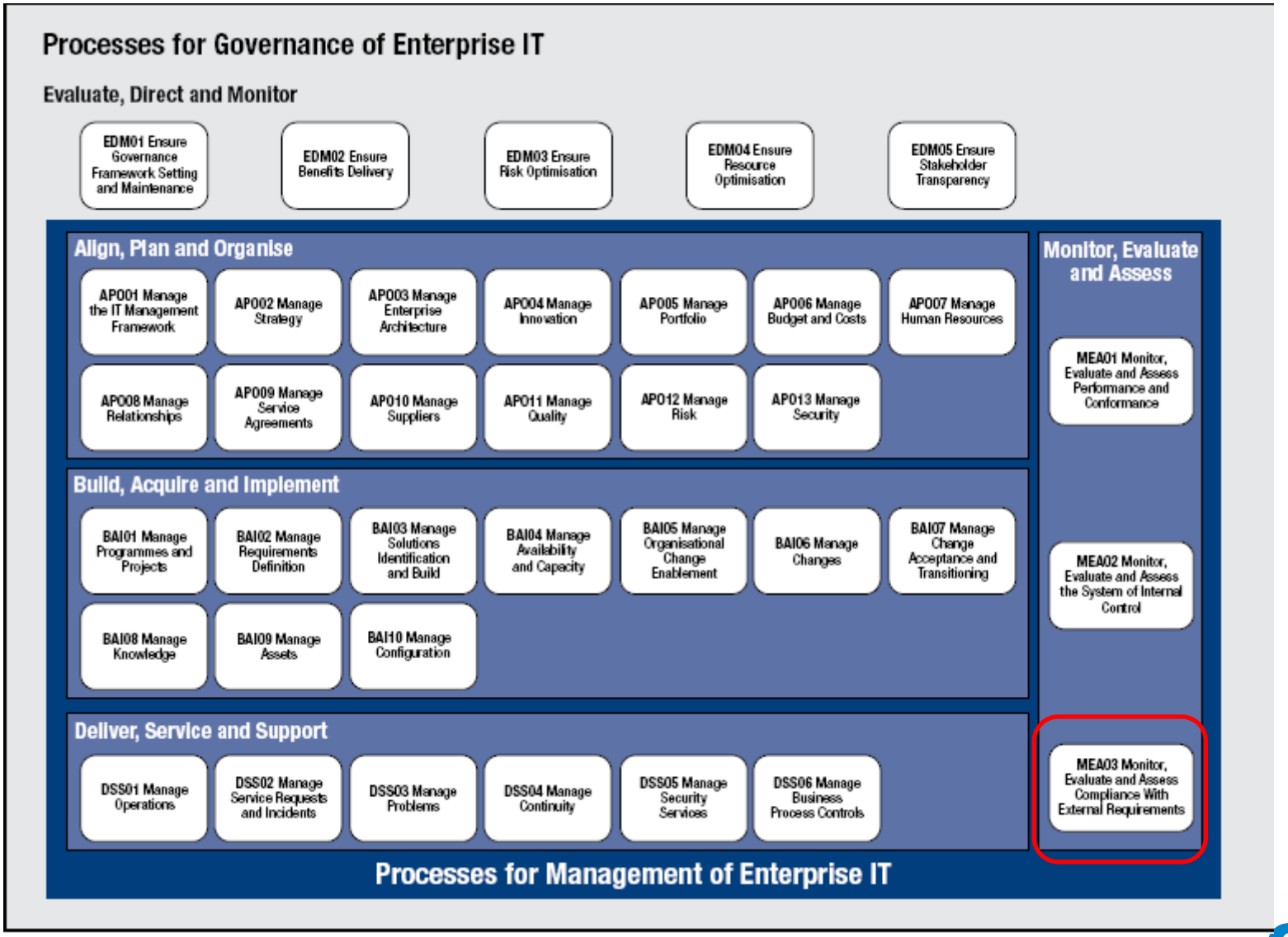
Compliance in COBIT 5

- The MANAGEMENT Monitor, Evaluate and Assess domain contains a compliance focused process:

  MEA03 Monitor, evaluate and assess compliance with external requirements.

- **Process Description**
  - Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.
- **Process Purpose Statement**
  - Ensure that the enterprise is compliant with all applicable external requirements.

Compliance in COBIT 5 (cont.)



Compliance in COBIT 5 (cont.)

- Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03).
- In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures.

Compliance in COBIT 5 (cont.)

- In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process.

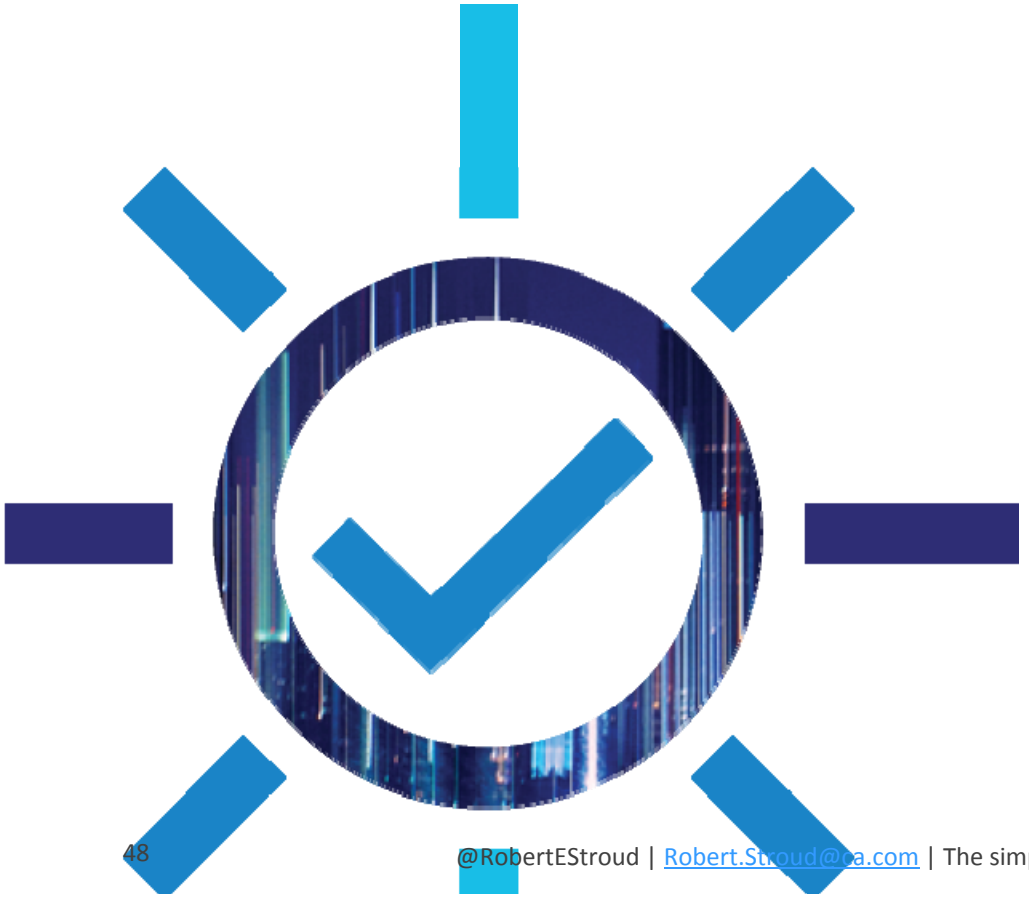
  These include a compliance-related role.

Compliance in COBIT 5 (cont.)

MEA03 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
MEA03.01 Identify external compliance requirements.					A	R										R	R	R								R
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C

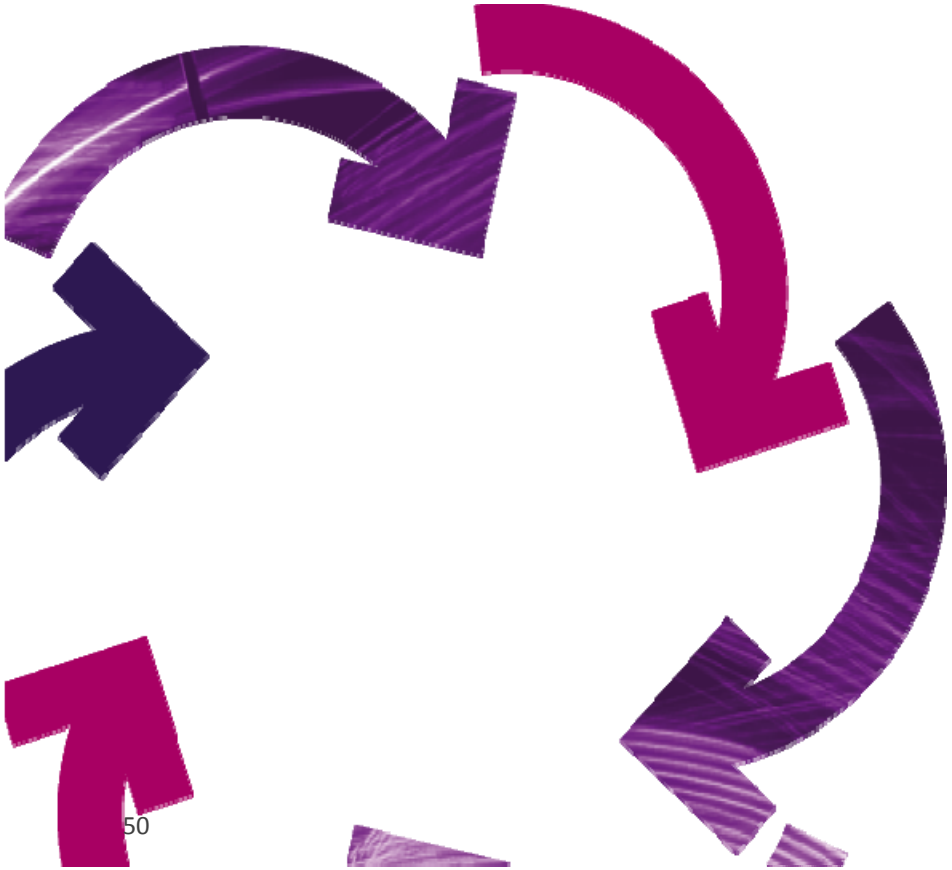
Recommendations and action plan!



Summary

- The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities:
  - Governance activities related to GEIT (5 processes)
  - Risk management process—and supporting guidance for risk management across the GEIT space
  - Compliance—a specific focus on compliance activities within the framework and how they fit within the complete enterprise picture
- Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements—silos of activity!

Thank you!



Governance is relevant!

Robert E Stroud

VP Strategy & Innovation

CA Technologies

Robert.Stroud@ca.com

@RobertEStroud

November 2013