

COBIT4.1 and VALIT Updates!

Robert E Stroud
International Vice President ISACA
ITSM & IT Governance Evangelist
CA, Inc.

Robert.Stroud@ca.com



TRUE or FALSE



1. Apples, not caffeine, are more efficient at waking you up in the morning.
2. Forty people are sent to the hospital for dog bites every minute.
3. The toothbrush was invented in 1498.
4. 40,000 Americans are injured by toilets each year.
5. If coloring weren't added to Coca-Cola, it would be green.



Robert.Stroud@ca.com



Robert Stroud



- 26 years in Industry experience
- 15+ years banking industry
- ISACA\ITGI International VP
- Chair COBIT® Steering Committee
- Contributor to COBIT® Version 4 & 4.1
- USA itSMF Board of Directors
- Chair Certification Committee
- Member ITIL® Version 3 (V3) Advisory Group
- Mentor and Reviewer of ITIL® V3



Robert.Stroud@ca.com



IT Governance Institute

IT Governance Institute is a non-profit research think-tank associated with ISACA®.

Media Supporters Info Request Site Map Contact Us

IT
GOVERNANCE
INSTITUTE®

Leading the IT Governance Community

About ITGI About IT Governance Resource Center Case Studies / Best Practices Search

Wednesday, 8 November 2006

The IT Governance Institute (ITGI) exists to assist enterprise leaders in their responsibility to ensure that IT is aligned with the business and delivers value, its performance is measured, its resources properly allocated and its risks mitigated.

IT Governance Institute
3701 Algonquin Road
Suite 1010
Rolling Meadows, IL
60008 USA

Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org

© 2006 IT Governance Institute (ITGI) All rights reserved.

Second Edition of Sarbanes-Oxley Publication Available

ITGI has released an updated edition of its well-received publication, *IT Control Objectives for Sarbanes-Oxley*. The first edition, published in 2004, has been downloaded more than 250,000 times. Companies around the world have used it as a tool for evaluating IT controls in support of Sarbanes-Oxley compliance. Experts from many organizations, including the top 10 accounting and professional firms, provided input and direction for the update.

[IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition](#) (PDF, 890K)

ITGI Issues Val IT—New IT Value Framework

Val IT provides the means to measure, monitor and optimize the realization of business value from investment in IT. It complements CobIT from a business and financial perspective and will help all those with an interest in value delivery from IT. This initial series consists of three volumes, available for free download:

- ▶ [Enterprise Value: Governance of IT Investments, The Val IT Framework](#) (PDF, 355K)
- ▶ [Enterprise Value: Governance of IT Investments, The Business Case](#) (PDF, 296K)
- ▶ [Enterprise Value: Governance of IT Investments, The ING Case Study](#) (PDF, 385K)

ITGI has released CobIT 4.0

The newest version of its globally recognized and adopted IT governance framework.
[Learn more...](#)

COBIT
GOVERNANCE, CONTROL
and ASSET for INFORMATION
and RELATED TECHNOLOGY

Control Objectives
for Information and
related Technology

Now in German!
[Introduction to COBIT](#)

MEET OUR SUPPORTERS

- ▶ Support ITGI's creation of groundbreaking research!

NEWS

New Case Studies

- ▶ [Prudential Financial Asia](#)
COBIT is a powerful management tool that helps achieve goals.
- ▶ [Harley-Davidson](#)
COBIT revs up management and staff interest in controls.

CobIT In Use

- ▶ [A new look at the use of CobIT](#) within the Swiss public sector. (Available in [English](#), [French](#), [German](#) or [Italian](#).)

ITGI Responds

- ▶ A response was delivered to the U.S. Securities and Exchange Commission's (SEC) request for comments on its *Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting*. [View Response](#) (PDF, 80K)
- ▶ Comments and recommendations on lessons learned from applying the



Trademark Notice



COBIT[®] and ValIT[™] are registered trademarks of ISACA/ITGI - Information Systems Audit and Control Association / IT Governance Institute[®]

DISCLAIMER

CA nor its speaker warrant or guarantee the concepts or the accuracy of information provided herein.

©All rights reserved

Robert.Stroud@ca.com



Agenda



- IT Governance
- COBIT
- VALIT
- Q&A



Robert.Stroud@ca.com



IT Governance



Robert.Stroud@ca.com

© 2007. Information Systems Audit and Control Association. All rights reserved.



Trends in Information Technology

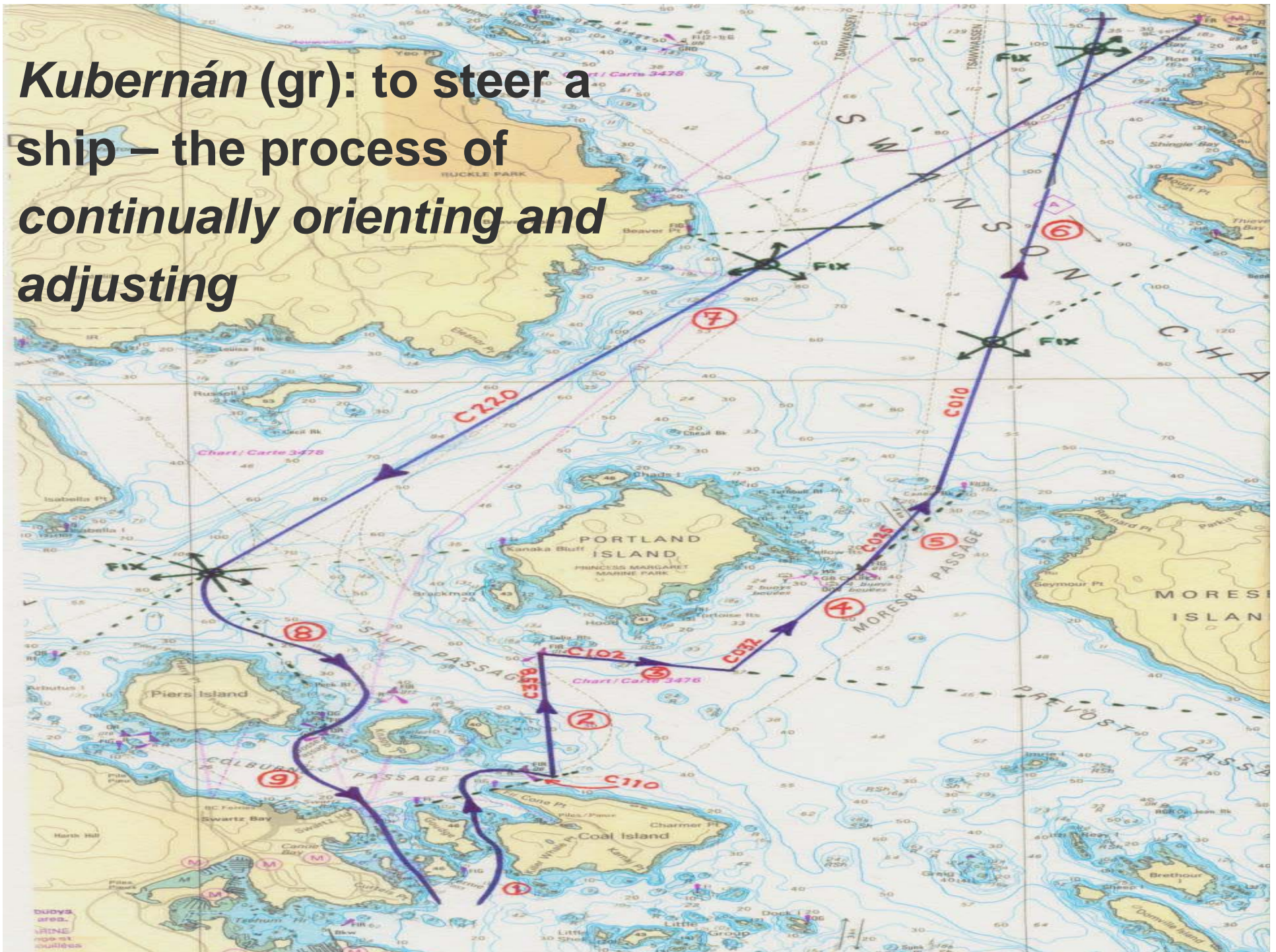


- Business decision makers demanding IT transparency
 - Spending accountability
 - Mapping IT initiatives to business initiatives
 - A better way of allocating IT costs to Business Units
- Increased recognition of IT's criticality to the business
 - Increased responsiveness
 - Consistent service-level delivery
- Insource/outsource analysis for all IT services
 - Service cost benchmarking
- Changing industry regulations
 - Business Software Alliance (BSA)
 - Environmental Protection Agency (EPA)
 - Legal compliance
- Increased utility computing offerings from vendors
- Adoption of Best Practices

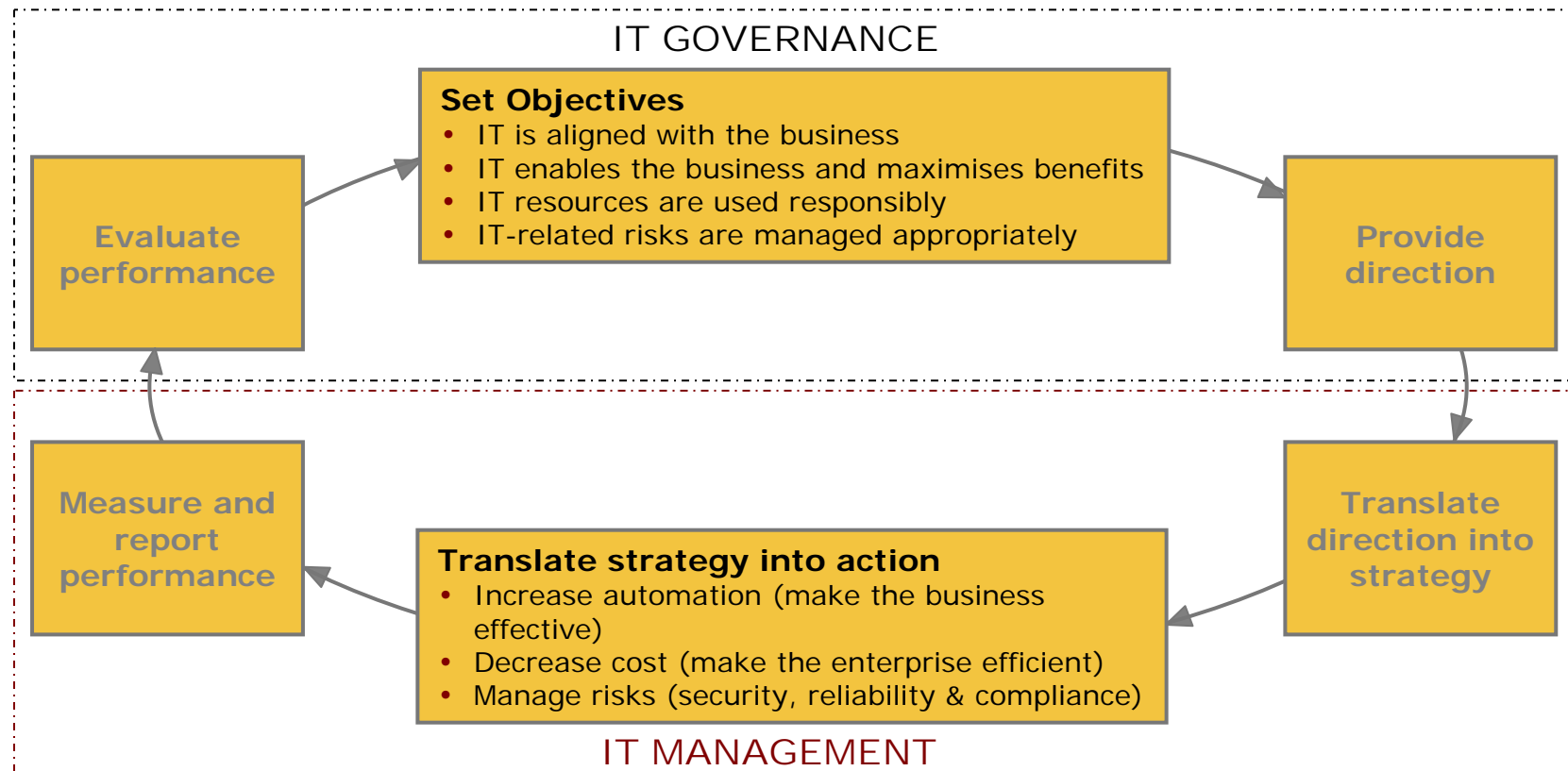
Robert.Stroud@ca.com



Kubernán (gr): to steer a ship – the process of continually orienting and adjusting

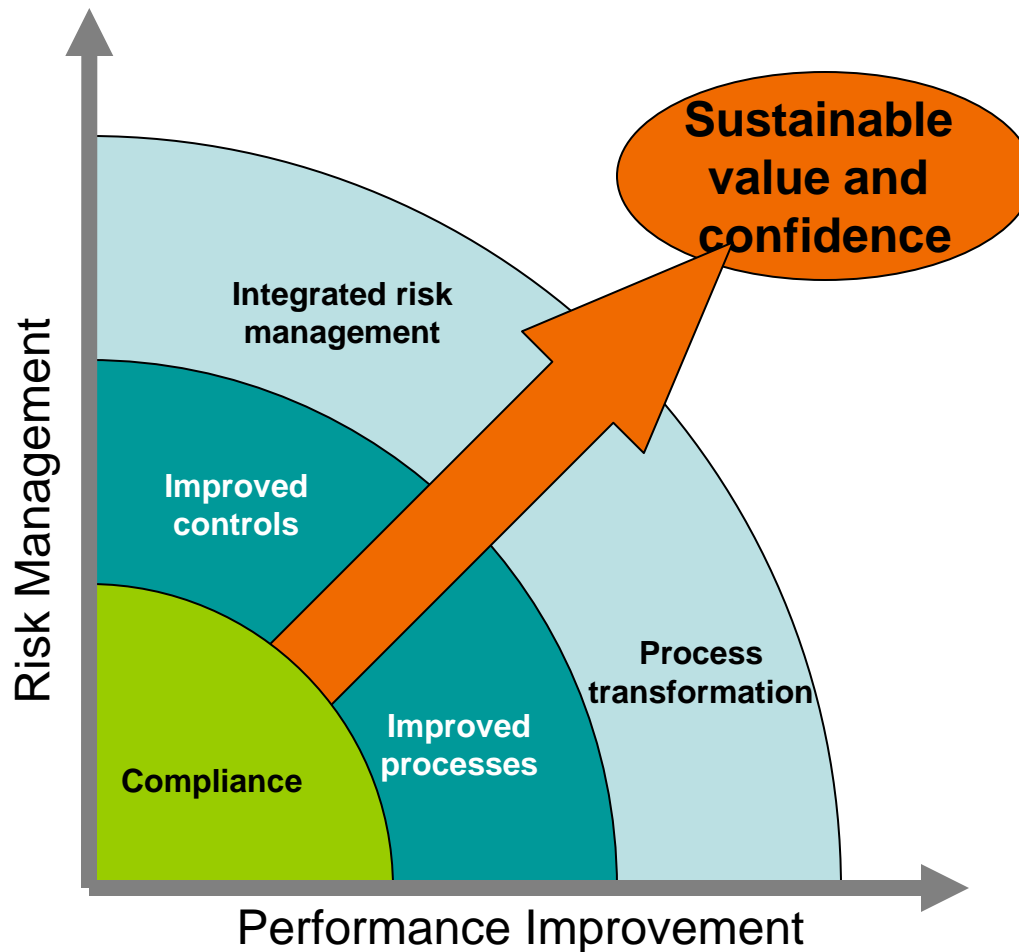


What is IT Governance?



- **Objective:** ensure that IT enables, sustains and extends the organisation's strategies and objectives
- **Method:** providing direction and exercising control
- **Content:** Leadership, organisational structures and processes
- **Responsibility:** board of directors and executive management

Performance vs. Control



Legislation is forcing the pendulum toward the Risk Management axis

Competition and market pressures are forcing the pendulum toward the Performance Improvement axis

Good IT Governance can help an organization balance risk management and performance improvement forces.

Robert.Stroud@ca.com



COBIT



Robert.Stroud@ca.com



COBIT



- COBIT® = **C**ontrol **OB**jectives for **I**nformation and **R**elated **T**echnology
- Process-oriented framework for IT Governance
- Focused on business goals and how IT supports their achievement
- A tool for
 - Business management
 - IT management
 - IT process managers
- First developed in 1992
- Issued by IT Governance Institute
- Content is managed by the COBIT Steering Committee
- Accepted globally as the de facto control framework for IT Governance
- Documents can be downloaded from www.isaca.org

Robert.Stroud@ca.com



How is COBIT Developed and Maintained?



- ITGI's independent status and desire to promote openly available guidance is a key influencing factor
- COBIT Steering Committee of volunteers and a management team drive the COBIT strategy and developments
- Over 100 experts from around the world (members, industry players) and eight volunteer teams form a unique support team (BE, UK, DK, AU, ZA plus 3 groups in the US)
- Development workshops create new content with no commercial pressures
- ISACA/ITGI International HQ provide support services to produce and distribute the finished products
- COBIT 4.0 has been a two-year effort with many interconnected projects
- COBIT 4.1 took an additional year

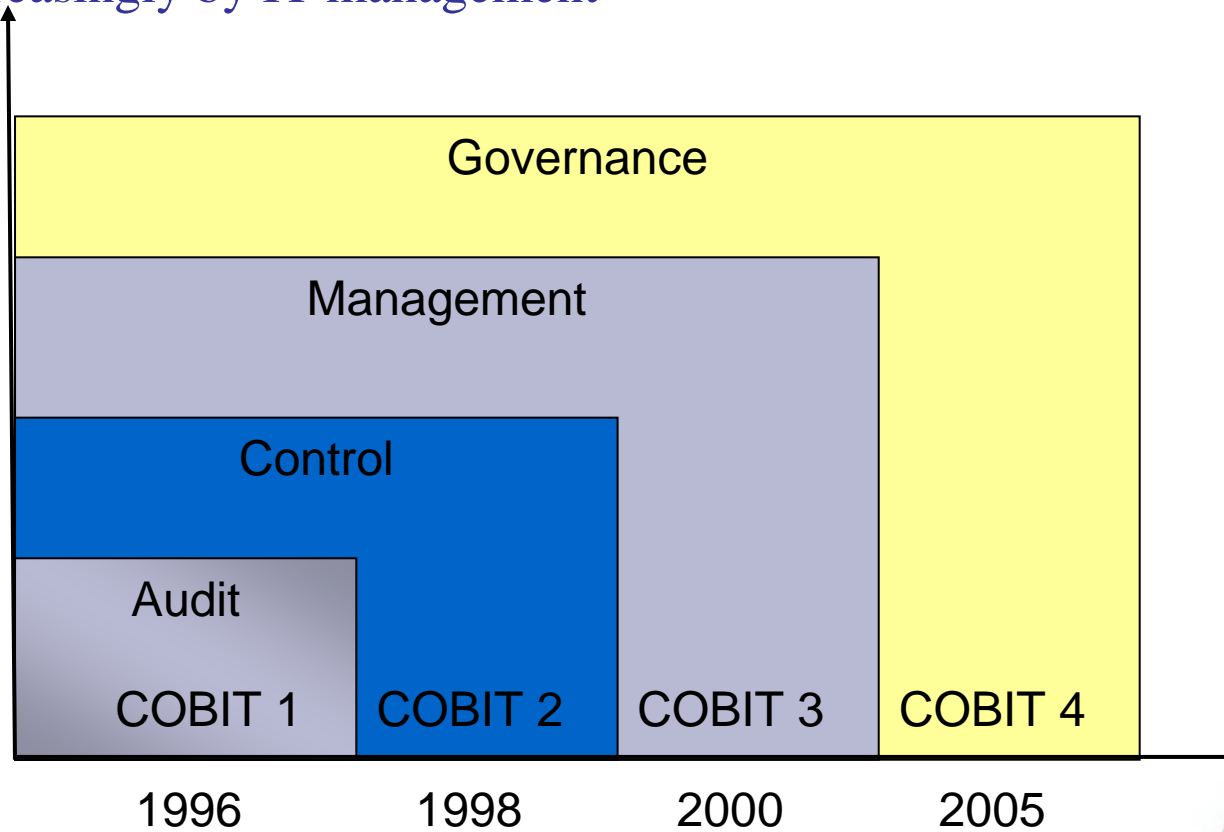
Robert.Stroud@ca.com



COBIT History



- COBIT has evolved from an auditor's tool to an IT governance framework, used increasingly by IT management



Robert.Stroud@ca.com



COBIT

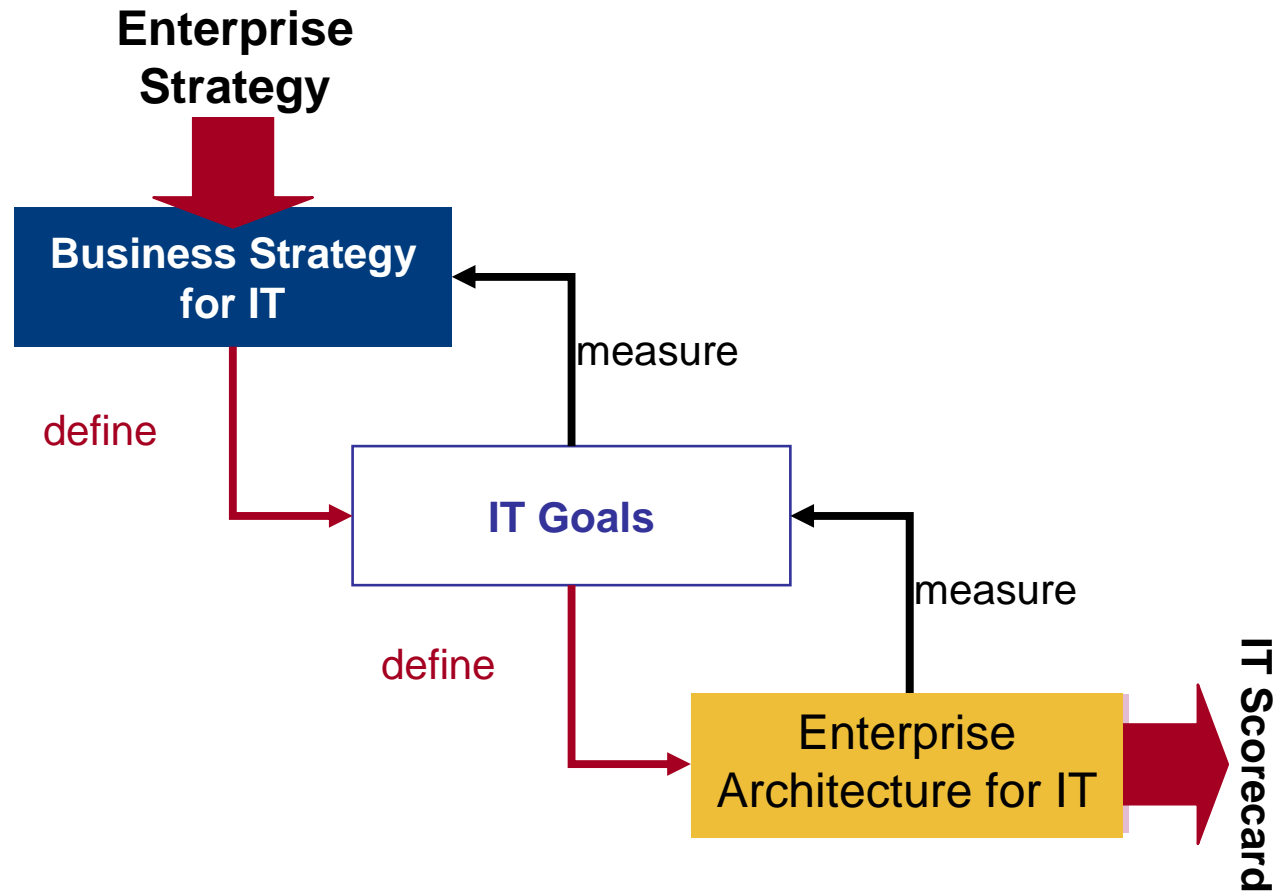


- *IT Governance* – Better coverage with governance practices in key processes to enable executives and the business to take their responsibility
- *Business Requirements* – Better business to IT linkages with cascading goals and supporting metrics
- *Harmonisation* – Improved integration with other key practices
- *Value Creation* – Extended focus on risk-adjusted IT investments
- *Enterprise Architecture* – Process structure and resources
- *Process Definitions and Process Flows* – Improved process descriptions, activities, inputs and outputs
- *Language and Presentation* – More concise, action-oriented and consolidate into one book
- *Feedback* – Responded to user comments

Robert.Stroud@ca.com



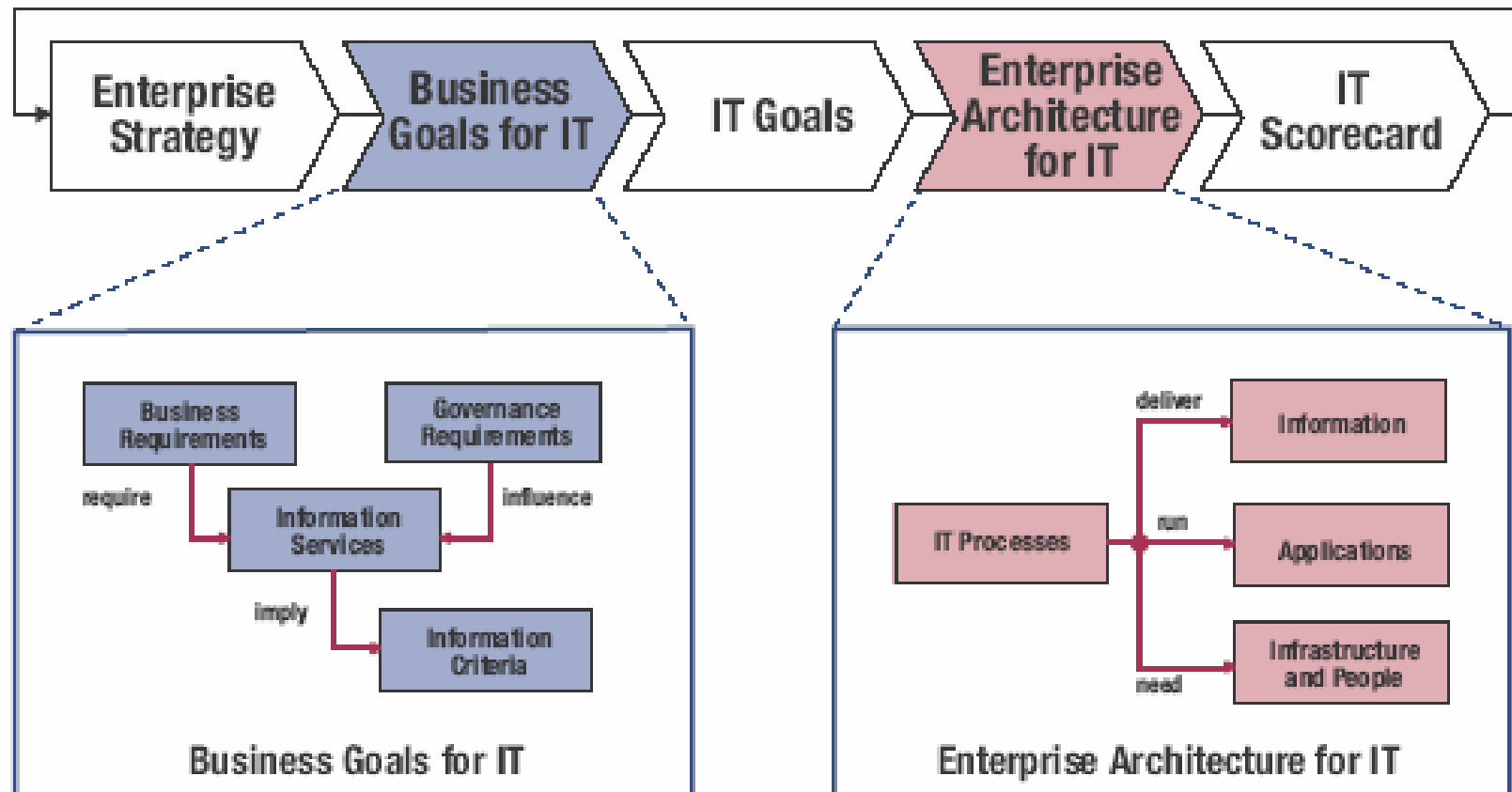
Top-down approach



Robert.Stroud@ca.com



COBIT 4.1 Business Focus



Robert.Stroud@ca.com



Linking Business Goals to IT Goals



	Business Goals		IT Goals							
<i>Financial Perspective</i>	1	Provide a good return on investment of IT-enabled business investments,	24							
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22
	3	Improve corporate governance and transparency.	2	18						
<i>Customer Perspective</i>	4	Improve customer orientation and service.	3	23						
	5	Offer competitive products and services.	5	24						
	6	Establish service continuity and availability.	10	16	22	23				
	7	Create agility in responding to changing business requirements.	1	5	25					
	8	Achieve cost optimisation of service delivery.	7	8	10	24				
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26			
<i>Internal Perspective</i>	10	Improve and maintain business process functionality.	6	7	11					
	11	Lower process costs.	7	8	13	15	24			
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27	
	13	Provide compliance with internal policies.	2	13						
	14	Manage business change.	1	5	6	11	28			
	15	Improve and maintain operational and staff productivity.	7	8	11	13				
<i>Learning and Growth Perspective</i>	16	Manage product and business innovation.	5	25	28					
	17	Acquire and maintain skilled and motivated people.	9							

Robert.Stroud@ca.com

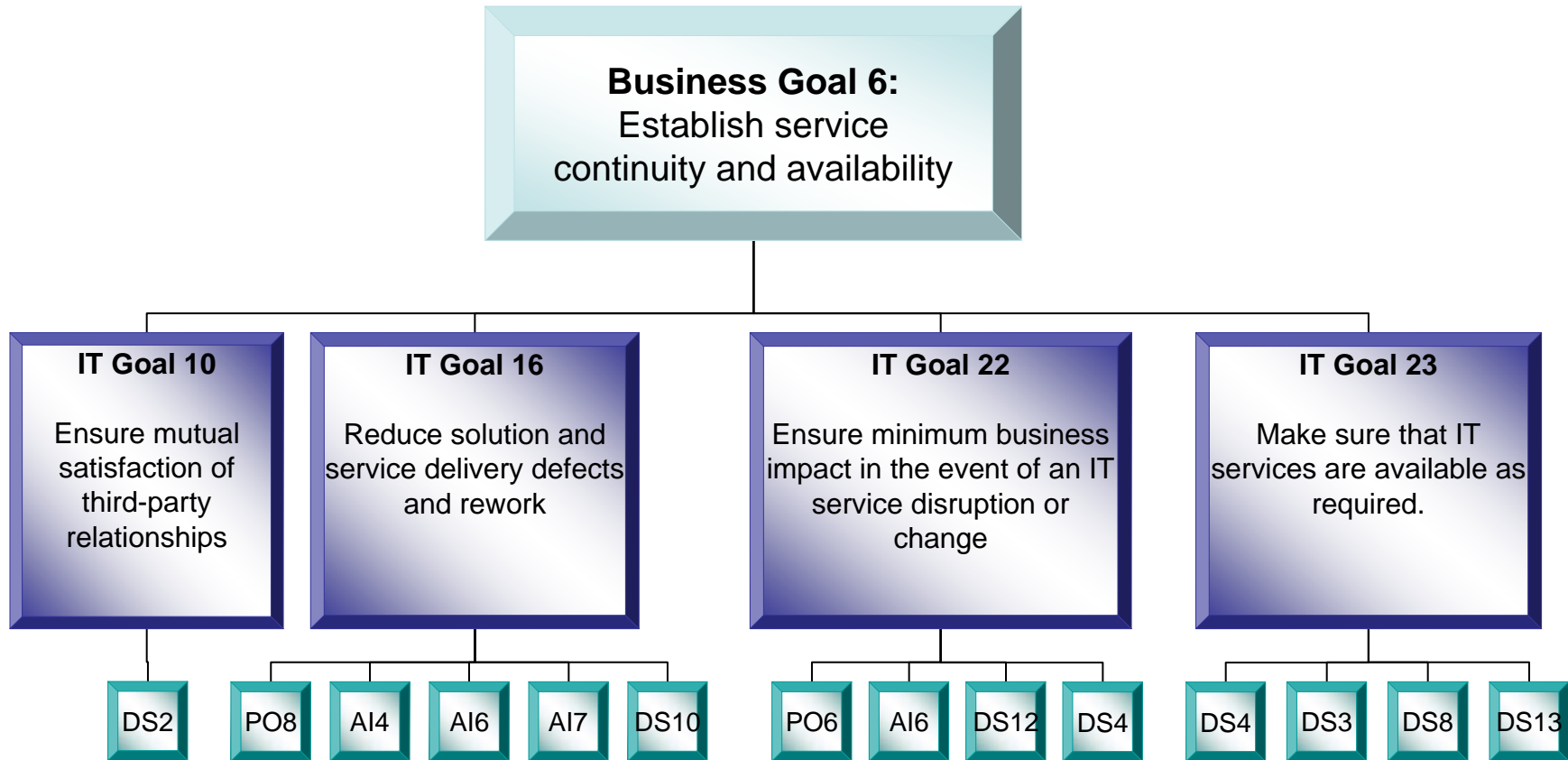


Linking IT Goals to IT Processes



1	Respond to business requirements in alignment with the business strategy.	P01	P02	P04	PO10	AI1	AI6	AI7	DS1	DS3	ME1
2	Respond to governance requirements in line with board direction.	P01	P04	PO10	ME1	ME4					
3	Ensure satisfaction of end users with service offerings and service levels.	P08	AI4	DS1	DS2	DS7	DS8	DS10	DS13		
4	Optimise the use of information.	P02	DS11								
5	Create IT agility.	P02	P04	P07	AI3						
6	Define how business functional and control requirements are translated into effective and efficient automated solutions.	AI1	AI2	AI6							
7	Acquire and maintain integrated and standardised application systems.	P03	AI2	AI5							
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5								
9	Acquire and maintain IT skills that respond to the IT strategy.	P07	AI5								
10	Ensure mutual satisfaction of third-party relationships.	DS2									
11	Ensure seamless integration of applications into business processes.	P02	AI4	AI7							
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	P05	P06	DS1	DS2	DS6	ME1	ME4			
13	Ensure proper use and performance of the applications and technology solutions.	P06	AI4	AI7	DS7	DS8					
14	Account for and protect all IT assets.	P09	DS5	DS9	DS12	ME2					
15	Optimise the IT infrastructure, resources and capabilities.	P03	AI3	DS3	DS7	DS9					
16	Reduce solution and service delivery defects and rework.	P08	AI4	AI6	AI7	DS10					
17	Protect the achievement of IT objectives.	P09	DS10	ME2							
18	Establish clarity on the business impact of risks to IT objectives and resources.	P09									
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	P06	DS5	DS11	DS12						
20	Ensure that automated business transactions and information exchanges can be trusted.	P06	AI7	DS5							
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	P06	AI7	DS4	DS5	DS12	DS13	ME2			
22	Ensure minimum business impact in the event of an IT service disruption or change.	P06	AI6	DS4	DS12						
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13						
24	Improve IT's cost-efficiency and its contribution to business profitability.	P05	DS6								
25	Deliver projects on time and on budget, meeting quality standards.	P08	PO10								
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5								
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4						
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	P05	DS6	ME1	ME4						

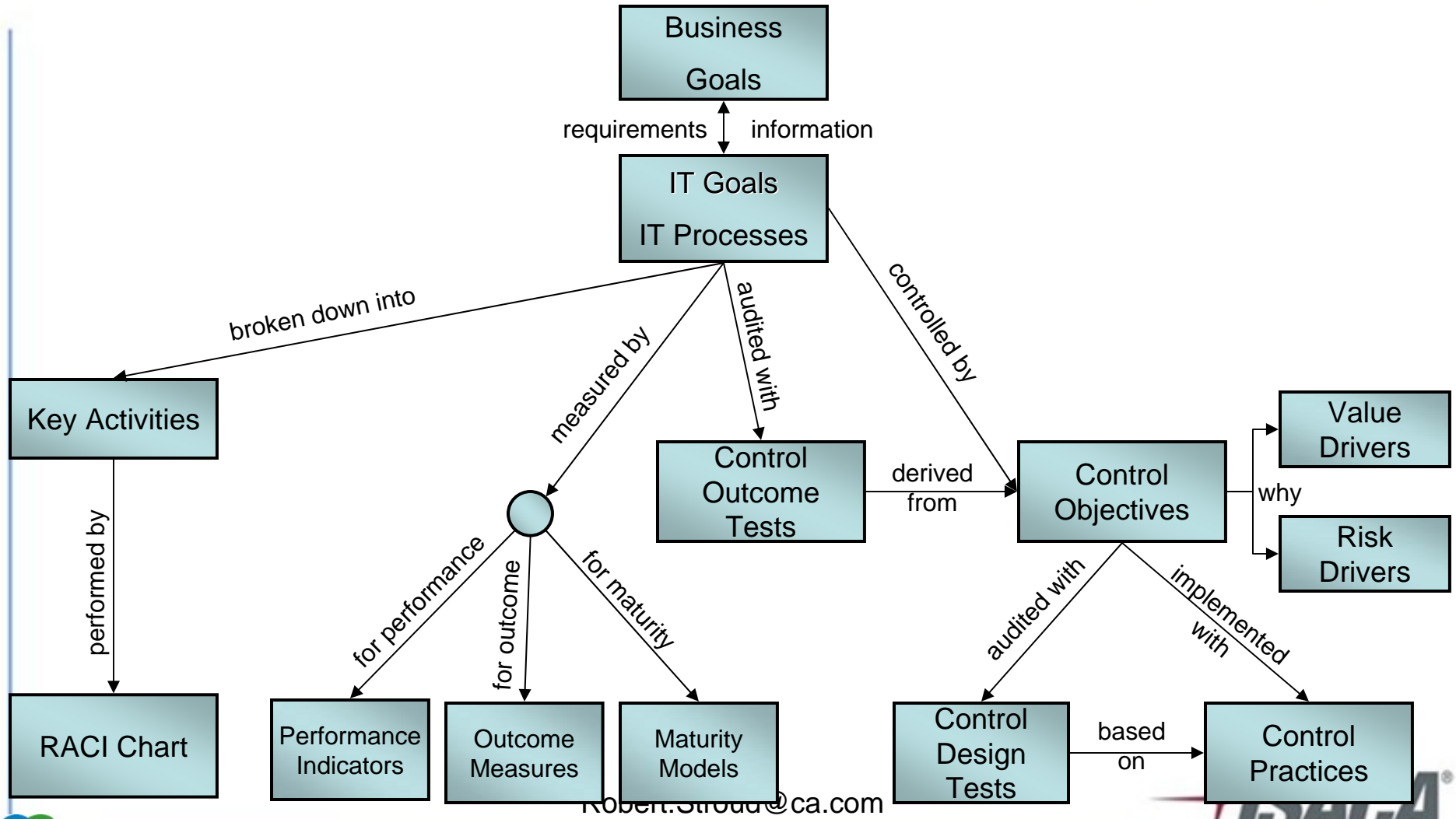
The links



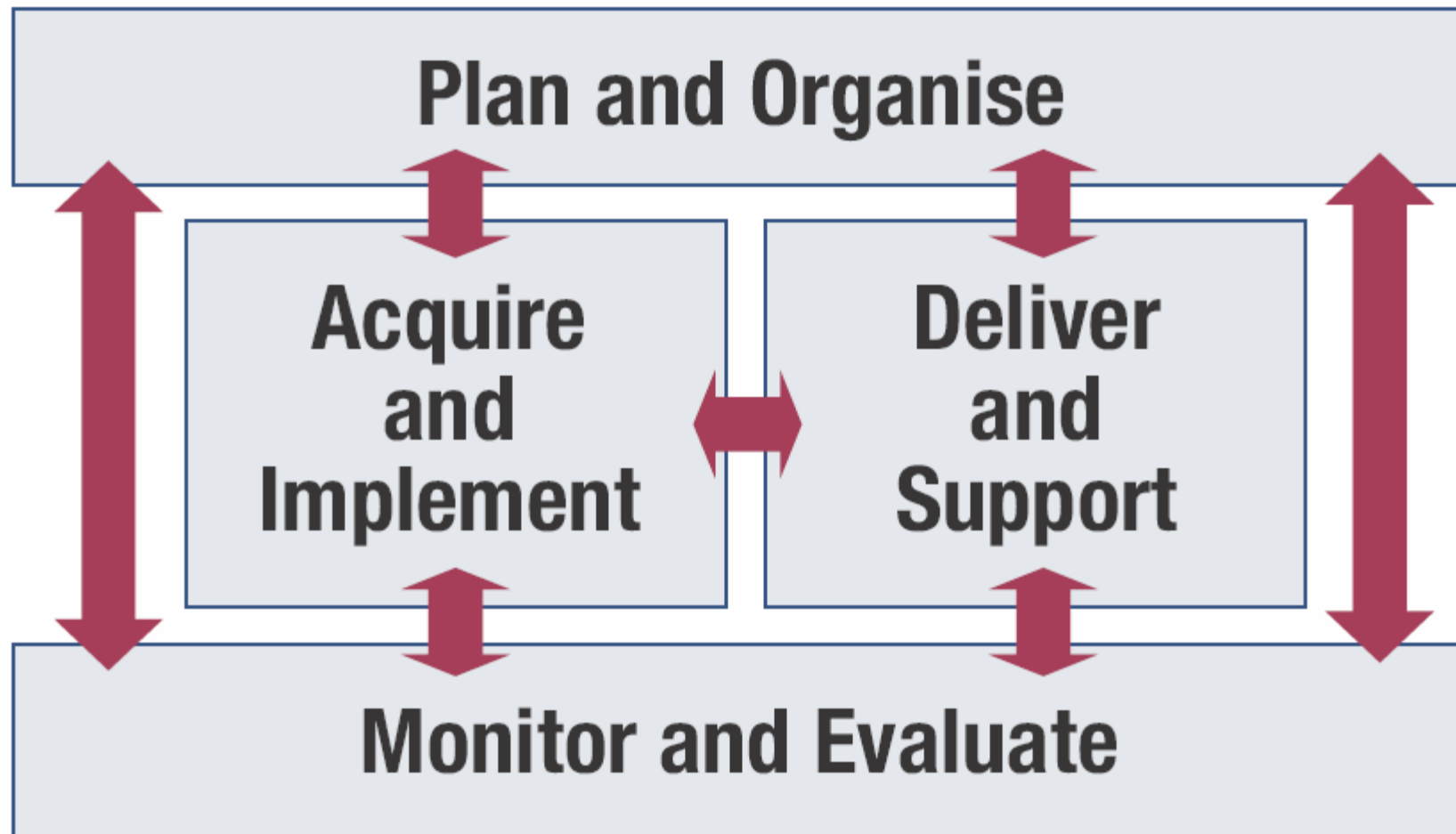
Robert.Stroud@ca.com



COBIT Components and interrelationships



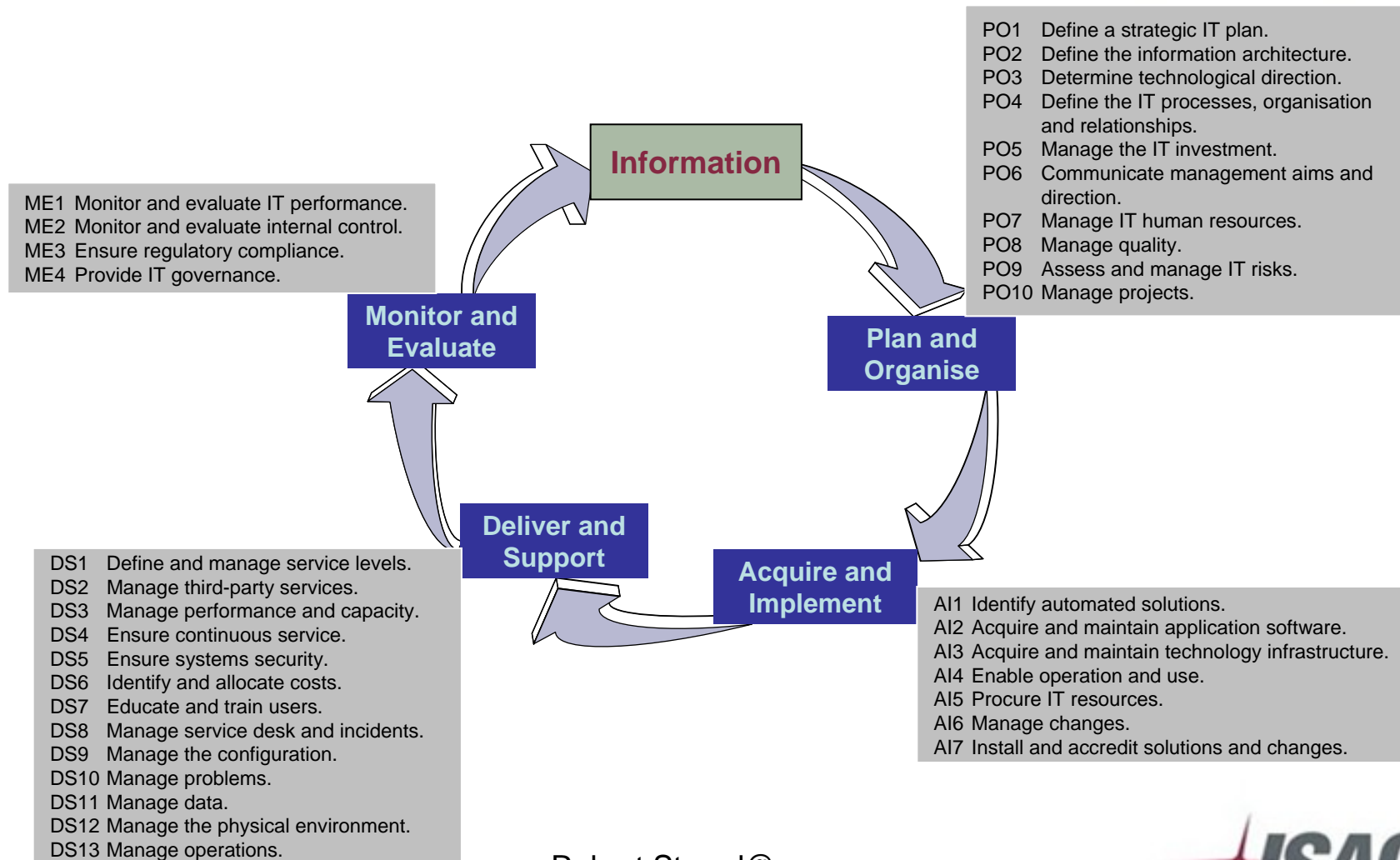
COBIT Domains



Robert.Stroud@ca.com



COBIT IT Processes



Robert.Stroud@ca.com



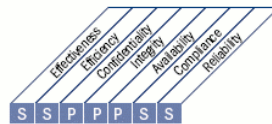
For 34 IT processes you have ...



➤ Process Overview

P09 Assess and Manage IT Risks

Create and maintain a risk management framework. The framework documents a common and agreed level of IT risks, mitigation strategies and agreed-upon residual risks. Any potential impact on the goals of the organisation caused by an unplanned event should be identified, analysed and assessed. Risk mitigation strategies should be adopted to minimise residual risk to an accepted level. The result of the assessment should be understandable to the stakeholders and expressed in financial terms, to enable stakeholders the alignment of risk to an acceptable level of tolerance.



- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business process and goals

is achieved by

development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

is managed by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remedial action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plan developed
- Percent of risk management action plans approved for implementation



■ Primary ■ Secondary



- ➔ Process description
- ➔ IT domain & Information indicators
- ➔ IT goals
- ➔ Process goals
- ➔ Key practices
- ➔ Key metrics
- ➔ IT Governance & IT Resource



For 34 IT processes you have ...



➤ Inputs

From	Inputs
P01	Strategic and tactical IT plans, IT service portfolio
P010	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

➤ Outputs

Outputs	To						
Risk assessment	P01	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	P06						
IT-related risk remedial action plans	P04	AI6					

Robert.Stroud@ca.com



For 34 IT processes you have ...



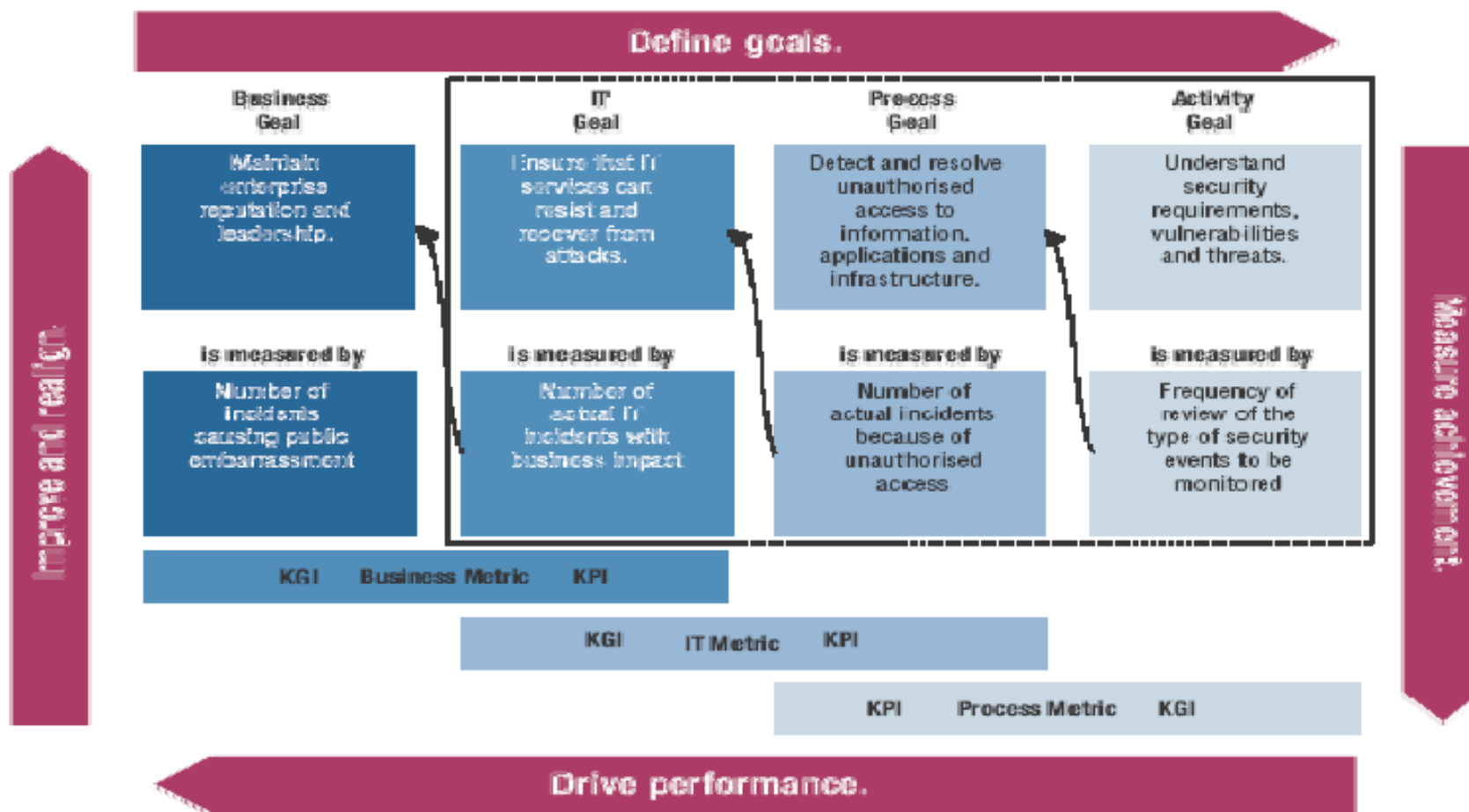
➤ RACI chart

	CEO	CFD	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit Risk and Security
Create and maintain corporate/enterprise information model.		C	I	A	C		R	C	C		C
Create and maintain corporate data dictionary(ies).				I	C		A/R	R			C
Establish and maintain data classification scheme.	I	C	A	C	C	I	C	C			R
Provide data owners with procedures and tools for classifying information systems.	I	C	A	C	C	I	C	C			R
Utilise the information model, data dictionary and classification scheme to plan optimised business systems.	C	C	I	A	C		R	C			I

Robert.Stroud@ca.com



Measurement System



Robert.Stroud@ca.com



Assurance Steps (1/2)



Control Objective	Value	Risk
<p>AC.6 Transaction Authentication and Integrity Before passing transaction data between internal applications and business or operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.</p>	<ul style="list-style-type: none"> • Complete and error free processing • Improved security over sensitive data output • Errors are detected in a timely manner 	<ul style="list-style-type: none"> • Compromised data integrity • Access control violations to data transactions • Transaction errors remain undetected
<p>Testing the Control Design</p>		
<p>Enquire and confirm a process has been designed to ensure that, for critical transactions, appropriate agreements have been made with counterparties that include communication and transaction presentation standards, responsibilities, authentication and security requirements.</p> <p>Enquire and confirm that systems are designed to incorporate appropriate mechanisms for integrity, authenticity and non-repudiation, such as adoption of a secure standard or one that is independently verified.</p> <p>Enquire and confirm that systems are designed to incorporate industry standard output tagging to identify authenticated information.</p> <p>Inspect manuals and documentation for critical applications to confirm that design specifications require that input is appropriately verified for authenticity.</p> <p>Enquire and confirm that systems are designed to identify transactions received from other processing applications and analyze that information to determine authenticity of origin of the information and</p>		

ROBERT.STROUD@CA.COM



Assurance Steps (2/2)



Testing the Outcome of the Control Objective

Obtain and inspect agreements made with counter parties for critical transactions and ensure that the agreements specify requirements for: communication and transaction presentation standards, responsibilities, authentication and security requirements.

Select a sample of counterparty agreements for critical transactions and verify that they are complete. Select a sample of authentication failures to verify that the counterparty agreements operate effectively. Review documentation and perform a “walk-through” to identify applications are critical for transaction authenticity, integrity and non-repudiation. For these applications enquire and confirm that an appropriate mechanism for integrity, authenticity and non-repudiation is adopted, i.e., a secure standard or one that is independently verified.

Inspect application manuals and documentation for critical applications to confirm that specifications and design state that output is appropriately tagged with authentication information.

Perform a walk-through of the code of a sample of applications to confirm that this specification and design is applied. Verify that these specifications have been tested with good result.

Select a representative sample of transactions and verify that authenticity and integrity information is correctly carried forward throughout the processing cycle.

Review error logs for transactions that failed authentication and verify the cause.

Documenting the Impact of Control Weaknesses

Perform a walk-through of the code of a sample of applications to confirm that specifications for authenticity have been applied. Verify that these specifications have been tested with good result.

Review error logs for transactions that failed authentication and verify the cause.

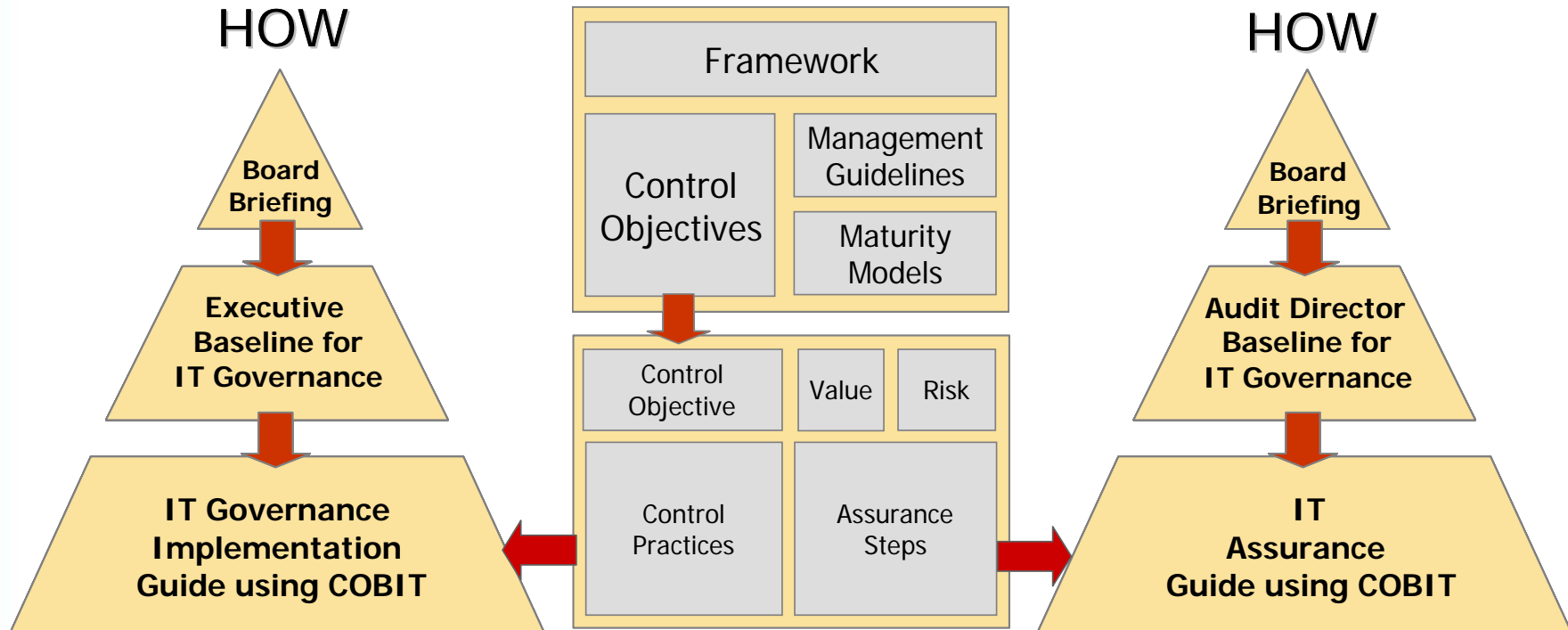
ROBERT.STROUD@CA.COM



Assurance



WHAT



Robert.Stroud@ca.com



COBIT Mapping Project



➤ Further mappings

- In progress
 - ✓ TOGAF (Architecture)
 - ✓ COSO ERM
 - ✓ GBPM
- On our radar
 - ✓ ITIL v3
 - ✓ FFEIC (US banking)
 - ✓ NIAC (Insurance)
 - ✓ NIST SP800-53
 - ✓ FISMA
 - ✓ IAIS Framework (Solvency II)
 - ✓ HIPAA (Health Insurance)
 - ✓ GLBA (Privacy)
 - ✓ ISO19770-1 (SW Asset Mgmt)
 - ✓ ISO 20000 (Service Mgmt)
 - ✓ ISO 27005 (Risk Mgmt)
 - ✓ ISO 27002 (ISO17799)



Mapping of ITIL®
With COBIT® 4.0



LEADING THE IT GOVERNANCE COMMUNITY

com



Differences between COBIT 4.0 and 4.1



➤ Changes in the Core Content

- No fundamental update to the framework but fine-tuning
- Executive Overview enhanced
- Explanation of Performance Measurement
- Control Objectives
 - ✓ Definition updated
 - Moving towards management practice statement
 - ✓ Lessons learned
 - Control Practices
 - ValIT development
 - Input from users
 - ✓ Grouped / reworded Control Objectives
 - ✓ Update of Application Controls
- List of Business and IT Goals (Appendix I)

Robert.Stroud@ca.com



Future developments



- No radical changes of COBIT 4.x in the next years
- Ongoing update and improvement
- Alignment of COBIT-Products
 - COBIT Online
 - QuickStart
 - Mapping
 - Slicing & Dicing
 - ValIT & RiskIT
- COBIT has a *BIG* impact
 - Relationship Governance, Business and IT
 - Control **Objectives** for **Business** and **IT**

Robert.Stroud@ca.com



[E-mail this to a friend](#)

[Printable version](#)

Flights resuming after disruption

Flights are returning to normal after an air traffic control computer failure saw planes grounded across the UK.

The West Drayton control centre is now fully operational and National Air Traffic Services says it is investigating the cause of the problem.

Nats' Flight Data Processing System failed at around 0600BST for an hour, after overnight testing of an upgrade.



Air safety was said to be unaffected by the computer failure

Planes had to be grounded at airports including Gatwick, Heathrow, Manchester and Inverness.

Investigation

Nats Chief Executive Richard Everitt said flights were

SERVICES

[TELL A FRIEND ABOUT](#)

BBC NEWS

BREAKING NEWS

Civil cot death

Thousands of pa

News alerts

Get the latest breaking news delivered to your desktop with the new alert service

SEE ALSO:

- ▶ [UK airports facing flight backlog](#)
03 Jun 04 | UK
- ▶ [Air delays after computer failure](#)
03 Jun 04 | Northern Ireland
- ▶ [Scotland hit by flight delays](#)
03 Jun 04 | Scotland
- ▶ [Flights disrupted by computer failure](#)

▶ [BBC Travel News](#)

RELATED INTERNET LINKS:

▶ [BAA](#)

The BBC is not responsible for the content of external internet sites

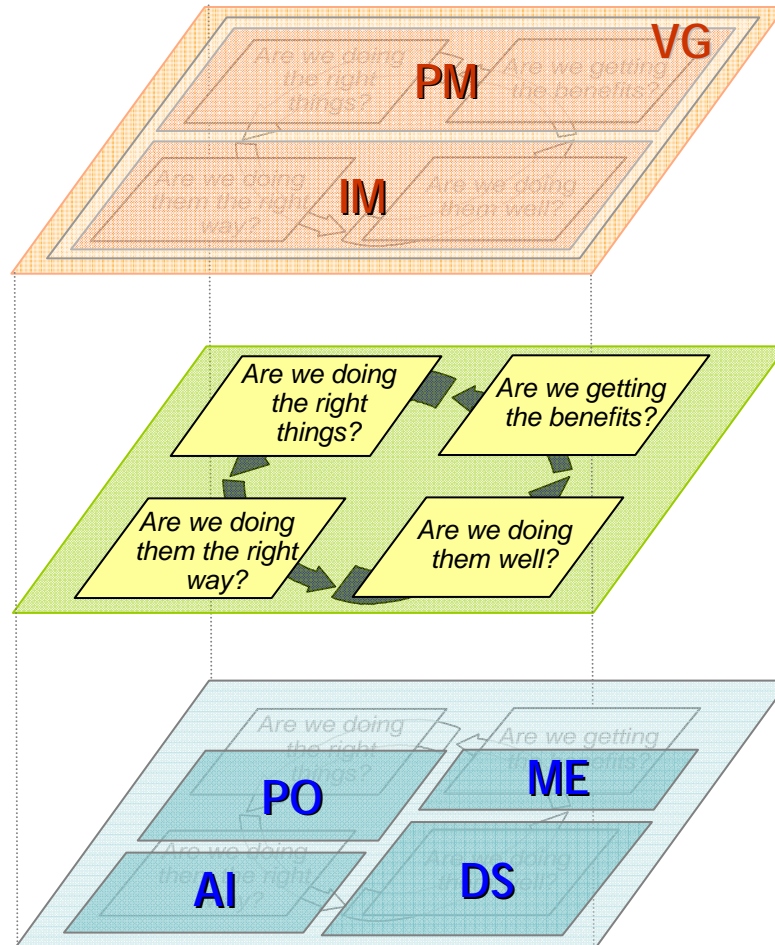
TOP UK STORIES NOW

▶ [Flights resuming after disruption](#)

Nats' Flight Data Processing System failed at around 0600BST for an hour, after overnight testing of an upgrade.



ValIT - “a value lens into COBIT”



Val IT

Governance & management of a portfolio of business change programmes

COBIT

Governance & management of a portfolio of technology projects, services, systems & supporting infrastructure

Robert.Stroud@ca.com



What fits where?



Val IT Initiative Status

DONE

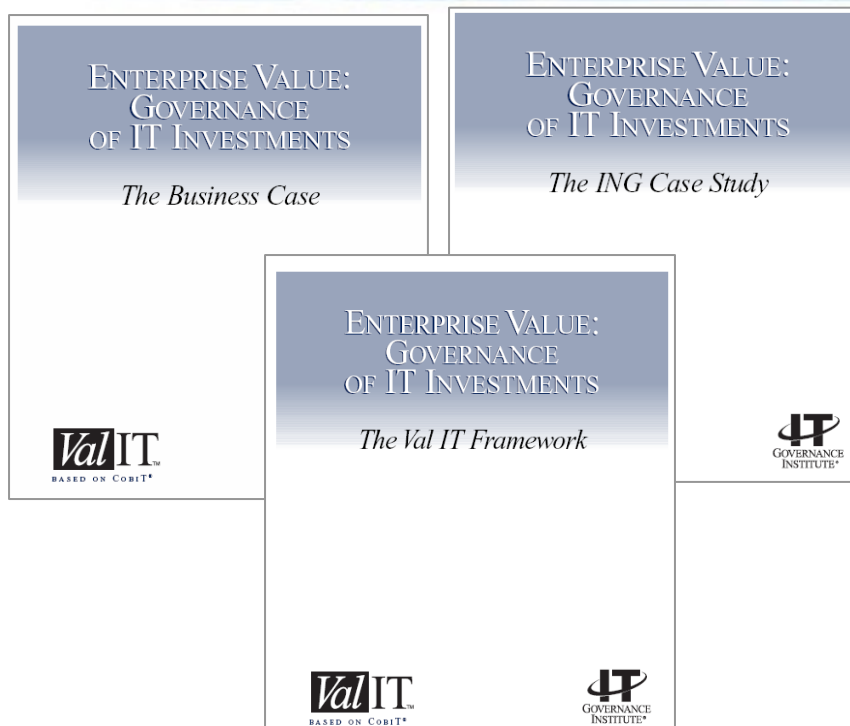
- Framework
- Business Case
- Case Study (initial)

IN PROCESS

- Empirical Analysis
- Maturity Models
- Management Guidelines
- Taxonomy

PLANNED

- Extend FW to services & other IT resources
- Business Case v2.0
- QuickStart Guide
- Forums
- Benchmarking



Available for free download from:

www.isaca.org or www.itgi.org

Robert.Stroud@ca.com



The Four “Ares”

- continually asking:

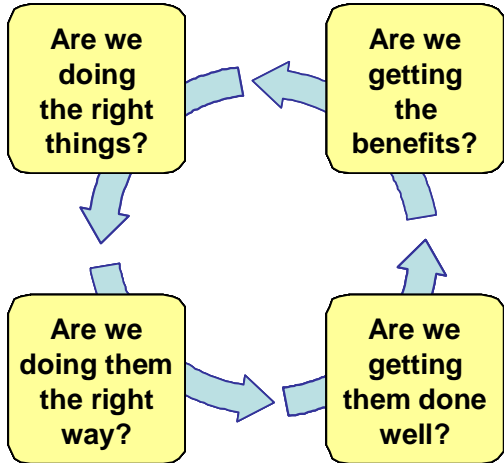


The *strategic* question. Is the investment:

- In line with our vision?
- Consistent with our business principles?
- Contributing to our strategic objectives?
- Providing optimal value, at affordable cost, at an acceptable level of risk?

- The the *value* question. Do we have:
 - A clear and shared understanding of the expected benefits?
 - Clear accountability for realising the benefits?
 - Relevant metrics?
 - An effective benefits realisation process?

Some fundamental questions



about the value delivered by IT

The *architecture* question. Is the investment:

- In line with our architecture?
- Consistent with our architectural principles?
- Contributing to the population of our architecture?
- In line with other initiatives?

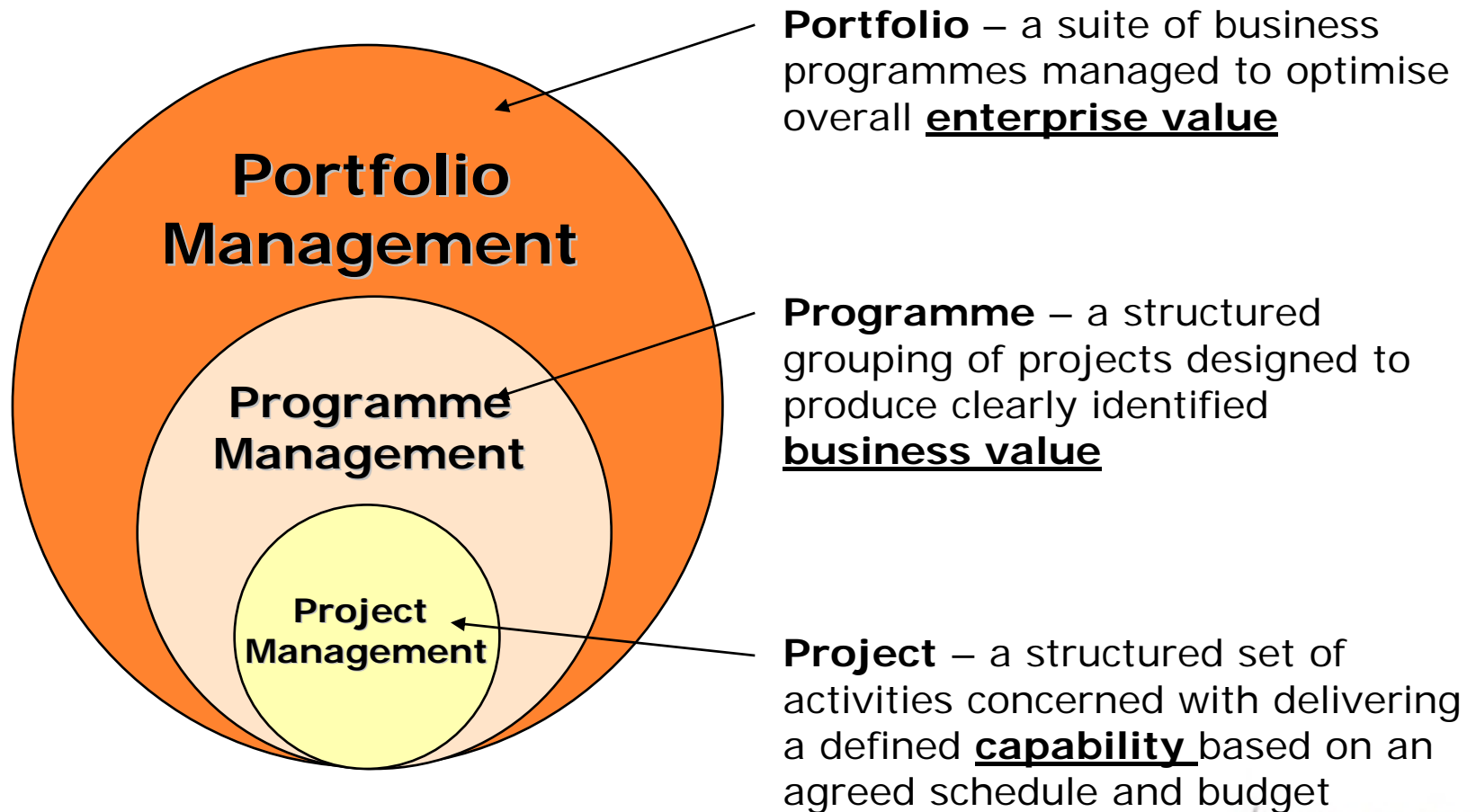
The *delivery* question. Do we have:

- Effective and disciplined delivery and change management processes?
- Competent and available technical and business resources to deliver:
 - the required capabilities; and
 - the organisational changes required to leverage the capabilities?

Robert.Stroud@ca.com



Projects, Programmes and Portfolios



Robert.Stroud@ca.com



Val IT Principles



- ❑ IT-enabled investments will be managed as a **portfolio of investments**.
- ❑ IT-enabled investments will include the **full scope of activities** that are required to achieve business value.
- ❑ IT-enabled investments will be managed through their **full economic life cycle**.
- ❑ Value delivery practices will recognise that there are **different categories of investments** that will be evaluated and managed differently.
- ❑ Value delivery practices will define and monitor **key metrics** and will respond quickly to any changes or deviations.
- ❑ Value delivery practices will engage all stakeholders and assign **appropriate accountability** for the delivery of capabilities and the realisation of business benefits.
- ❑ Value delivery practices will be **continually monitored, evaluated and improved**.

Robert.Stroud@ca.com



Val IT Processes



Value Governance (VG)

Portfolio Management (PM)

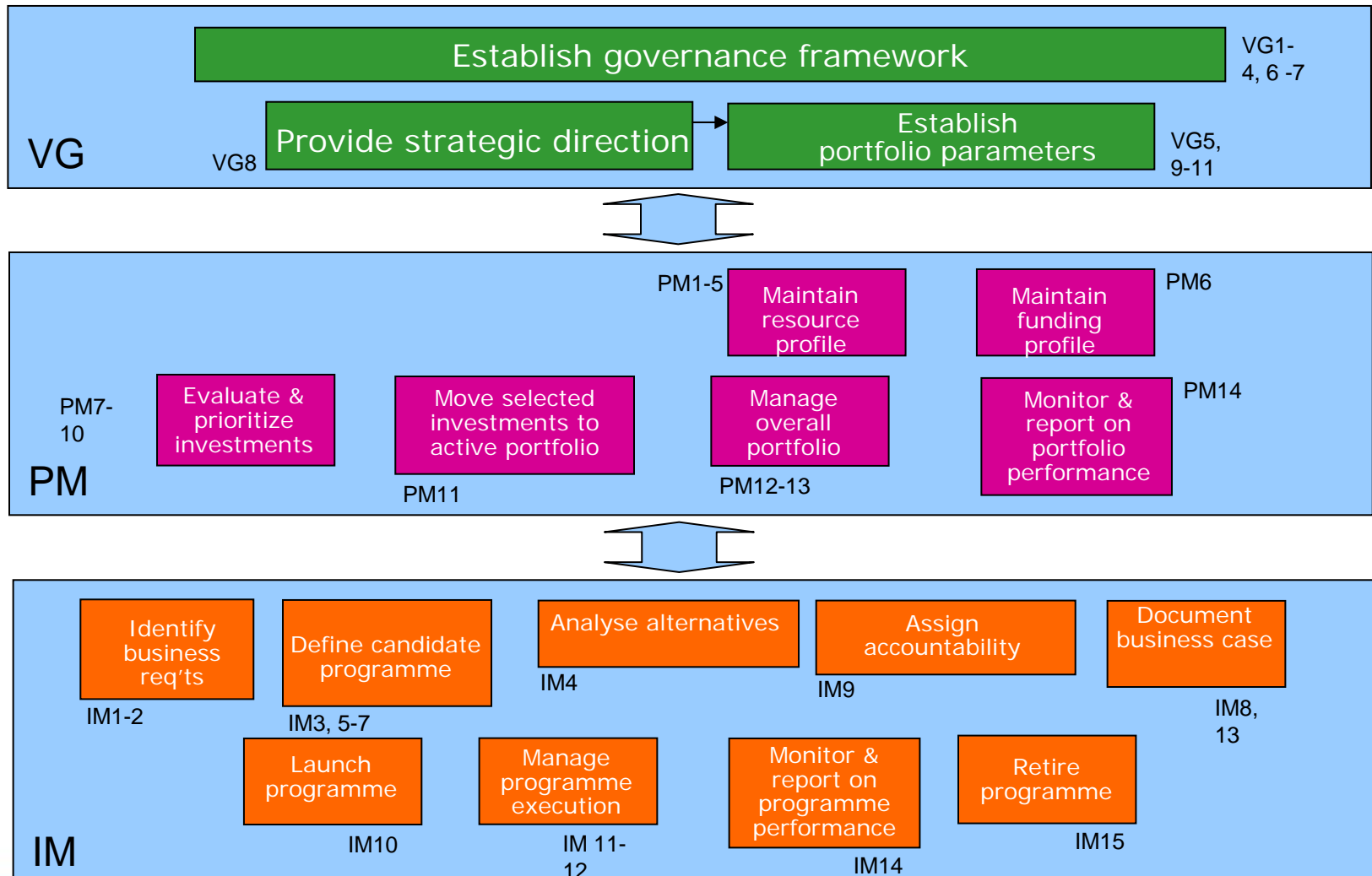
Investment Management (IM)

Robert.Stroud@ca.com



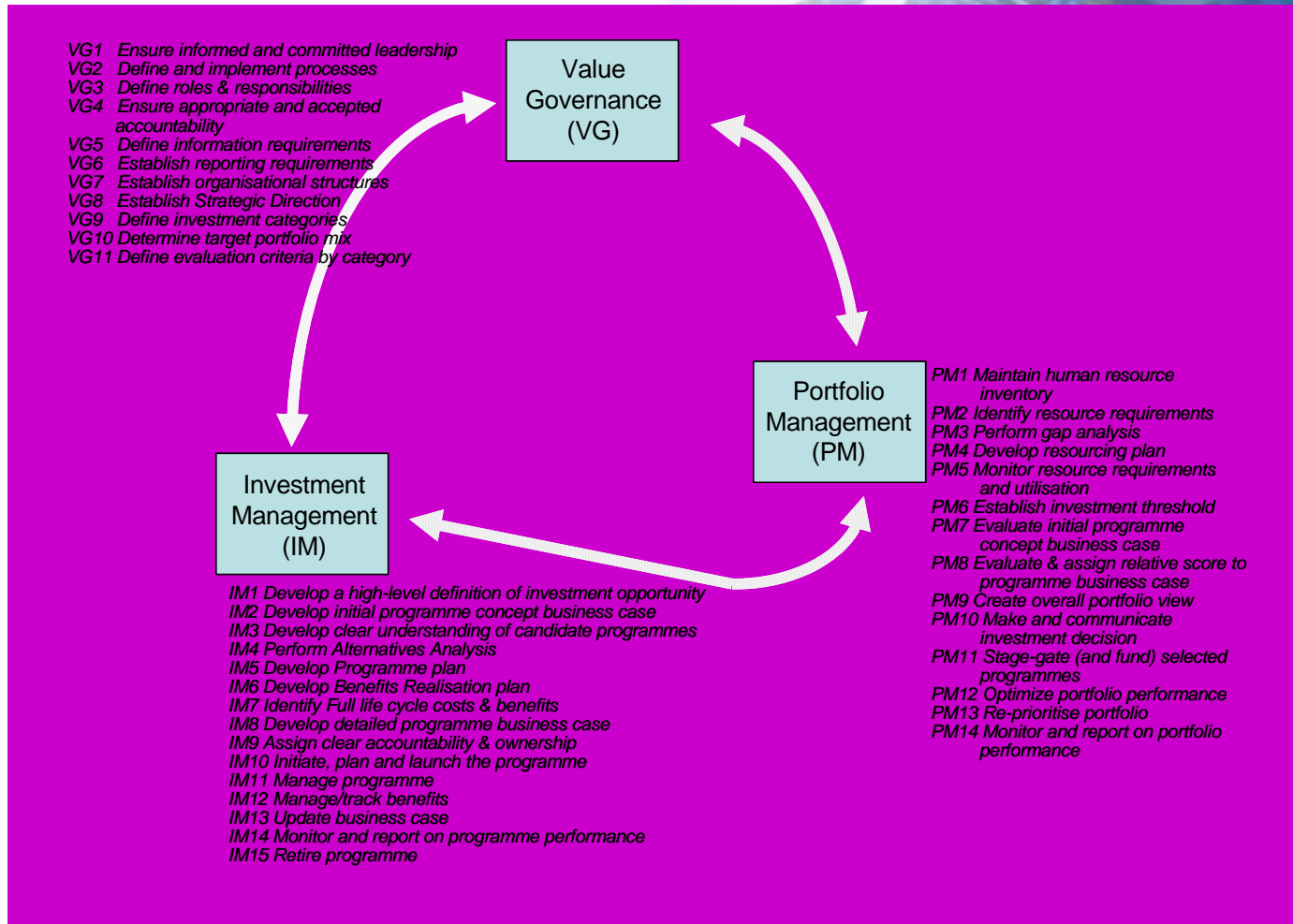
Val IT

Relationship between Processes & Practices



Val IT

Processes & Key Management Practices



Robert.Stroud@ca.com



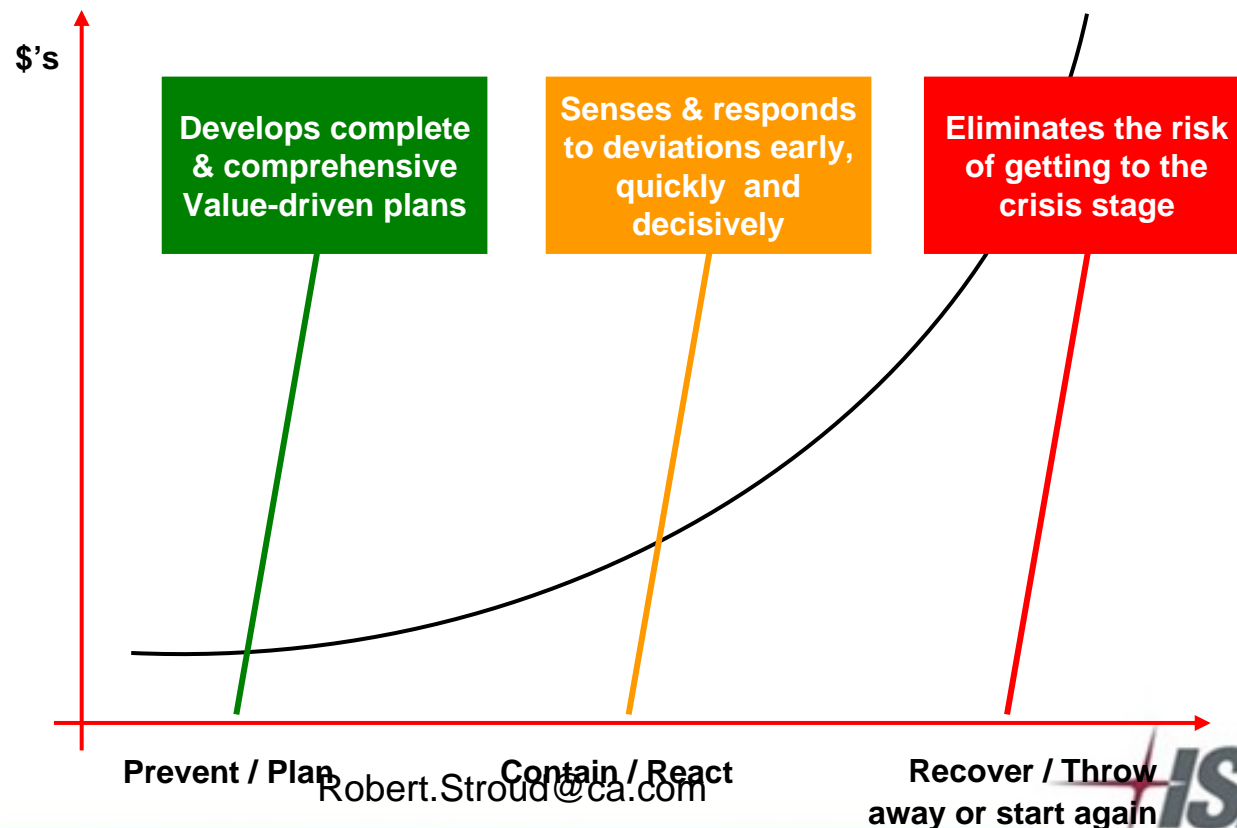
VG - Getting ahead of the Curve!



Requires an Effective Full Cycle Governance Process that...

“How does a project get to be a year behind schedule? One day at a time.”

Fred Brooks

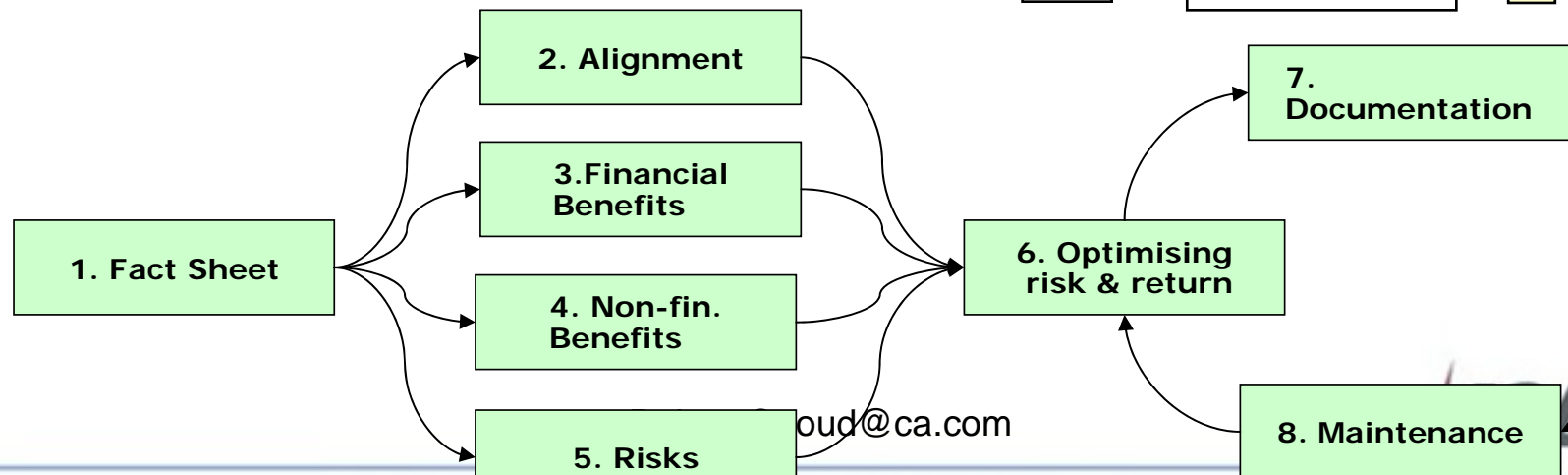
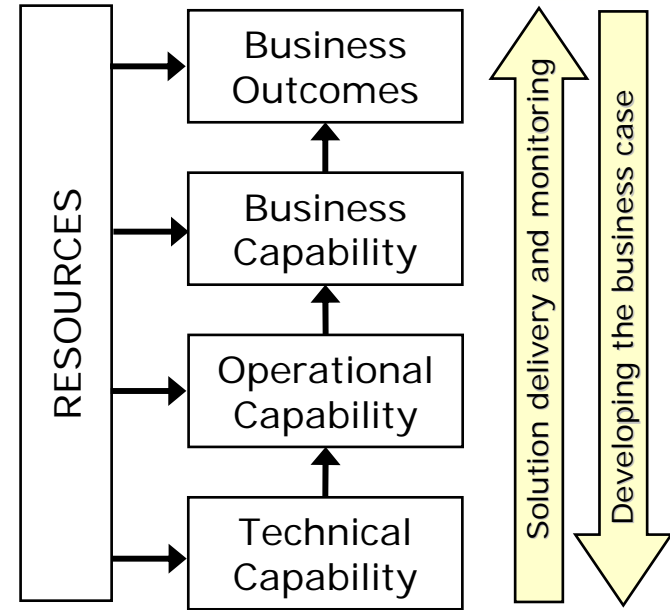


IM – The Business Case



Why the business case?

- Understanding of what you plan to achieve; how you are going to manage it and who is accountable
- Basis for comparison and choice
- Recording all that needs to be tracked (cost, risks, benefits, etc.)
- Maintain clarity on what you are doing



cloud@ca.com



7+1 Key Conditions for Activist Accountability



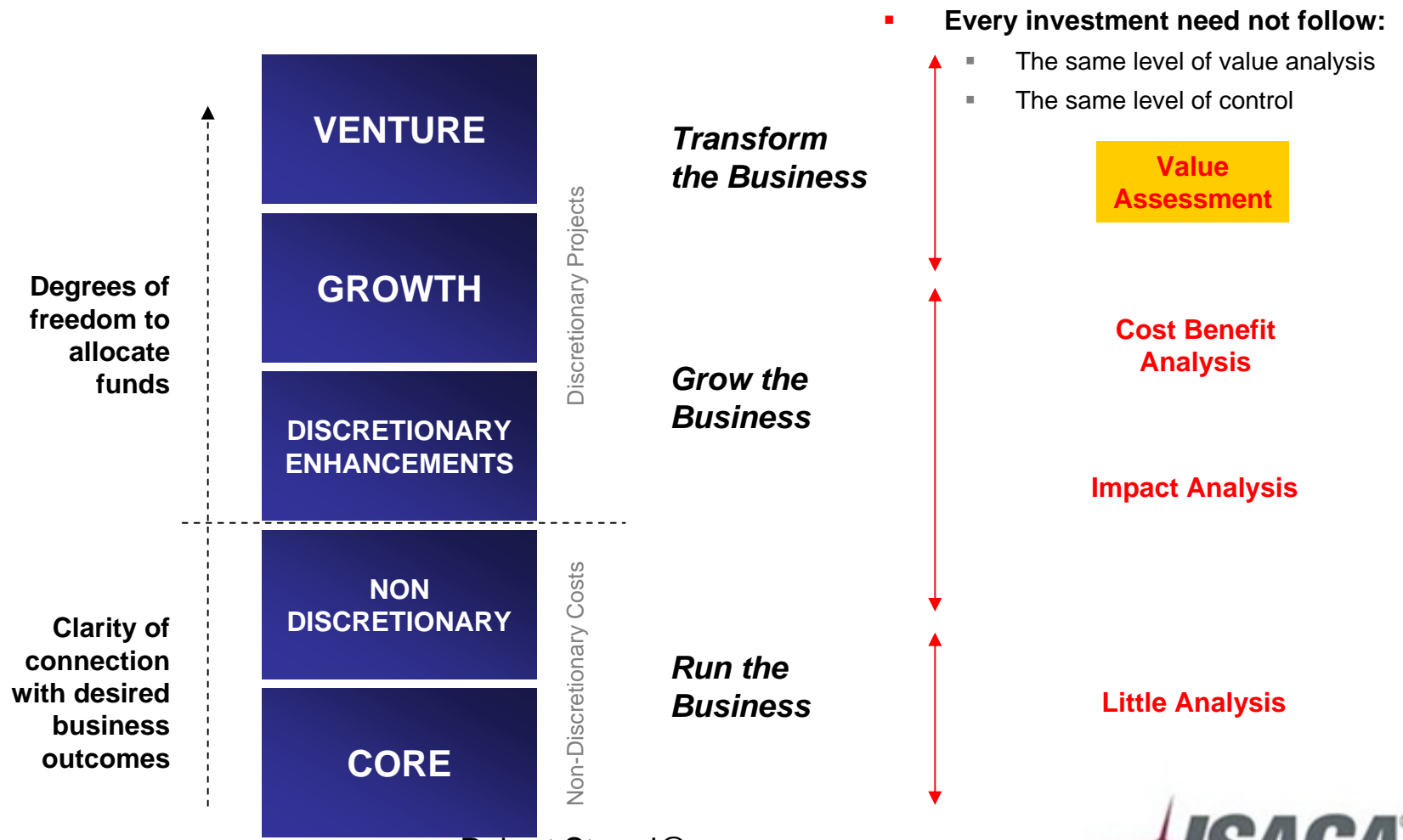
- Condition 1: Clear mandate and scope**
- Condition 2: Sufficient authority and latitude to act**
- Condition 3: Requisite competence**
- Condition 4: Commensurate resources**
- Condition 5: Clear lines of accountability**
- Condition 6: Understanding of rights and obligations**
- Condition 7: Relevant performance measures**

Plus... there must be acceptance of accountability

Robert.Stroud@ca.com



VG9 - Categorisation



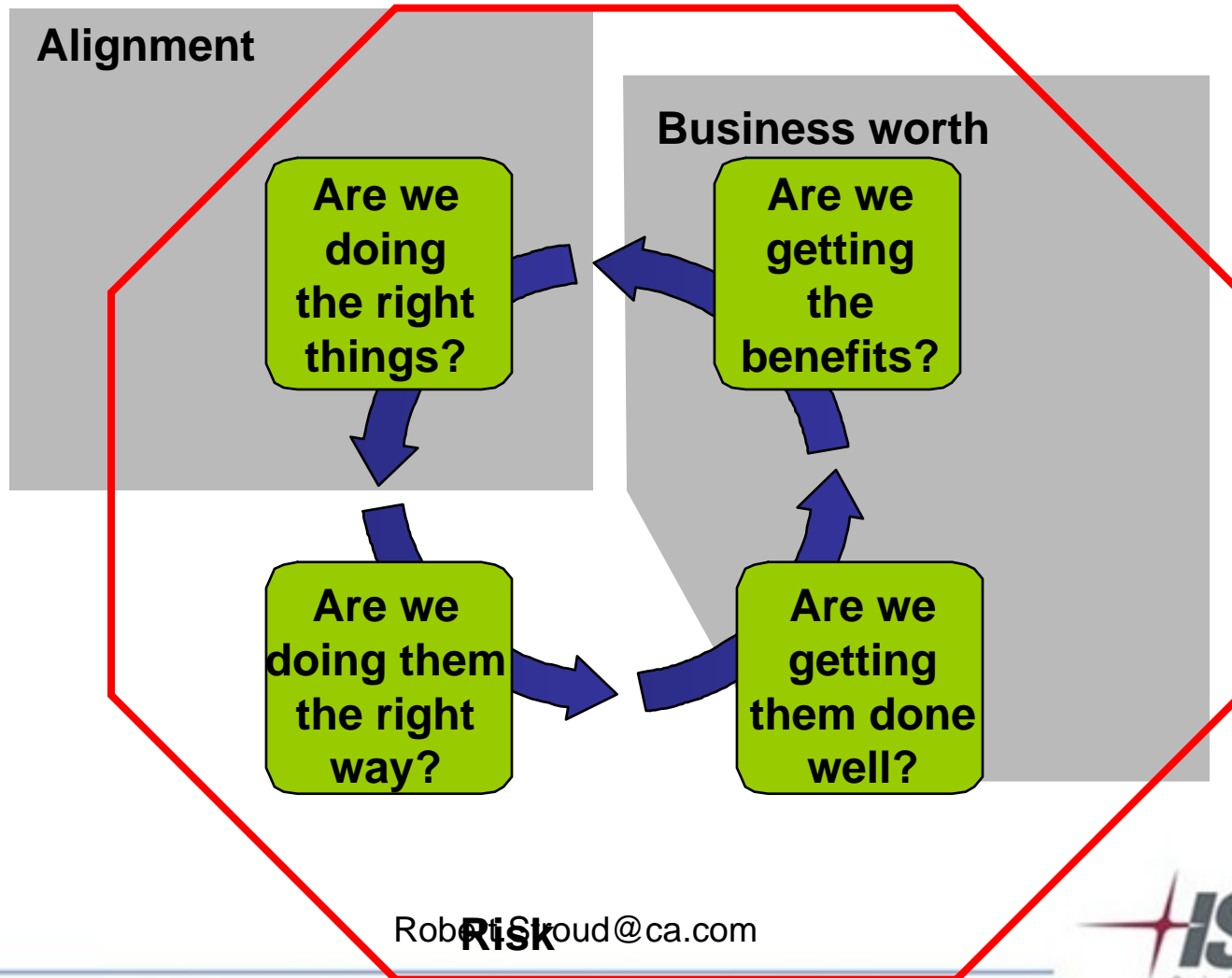
Robert.Stroud@ca.com



PM8 - Evaluation Criteria



Picking the Winners



Robert Cloud@ca.com

Risk



PM8 – Value Assessment -Alignment



Alignment element

Alignment with movement toward desired future state

Alignment with intent of business plan for information

Broad access to information services

To what extent does this initiative improve people's ability to access information services wherever they are working?

Question to address specific indicator of alignment

No contribution to broad access	Provides some enhancement in information services provided: no systemic or extensible beneficial effect on information access across the organization	Capabilities will significantly extend the ability to access information either geographically, or in breadth of information available for one major process area	Capabilities will significantly extend the ability to access information either geographically, or in breadth of information available for more than one major process area	Provides key component needed to supply "universal" access to information services in the form needed
0	1	2	3	4

Anchored "typical" answers

Scoring grid

Robert.Stroud@ca.com



PM8 - Value Assessment – Business Worth



➤ Financial

- Value = (benefits-costs)*risk adjusted for time value of money, where
 - ✓ Benefits and costs are over the full economic life-cycle of the investment
- Many ways to calculate and many “religious arguments” over what is the best way...key is to ensure completeness and consistency...look for same level of rigour on benefits as costs

➤ Non-financial

Robert.Stroud@ca.com



PM8 - Types of Risk



➤ Delivery risk

- Risk of not being able to deliver the required capabilities (functionality) on time and on budget

➤ Benefits risk

- Risk of not being able to use the capabilities to realise and sustain the expected benefits

PM8 - Delivery Risk



- Quality of the programme and project plans (completeness and reasonability)
- Clarity of scope and deliverables
- Unproven technology
- Compliance with technology architecture and standards
- Project duration
- Size of the project in relation to earlier successful projects
- Level of interface required to existing systems and processes
- Senior business department staff involvement
- Key staff availability during project deployment
- Experience/quality of project managers
- Experience/quality of project teams
- Reliance on vendors
- Dependency on factors outside control of project teams
- Quality of risk control mechanisms
- Ability to provide ongoing operational support

Robert.Stroud@ca.com



PM8 - Benefits Risk

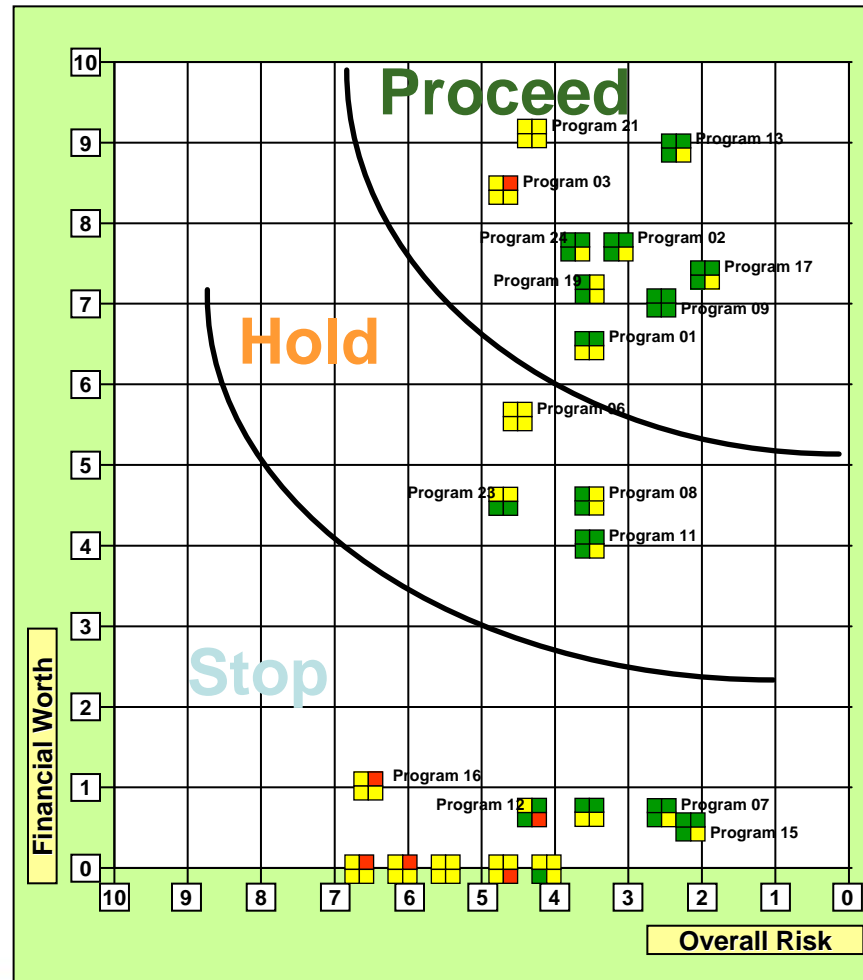


- Non-alignment with commercial policies or strategy
- Non-alignment with technical standards, architecture, etc.
- Compliance with security guidelines/policy
- Clarity and credibility of desired business outcomes
- Measurability of outcomes (lead and lag indicators)
- Benefits monitoring processes
- Sensitivity of outcomes to timing or external dependencies, including changes in the economy, market conditions or a specific industry sector.
- Extent of organisational change required (depth and breadth)
- Clarity of the scope of organisational change required
- Quality of the change management plan
- Preparedness and capability of business to handle the change
- Level of business organisational understanding of and commitment to the programme
- Quality and availability of business sponsorship
- Senior business department staff engagement
- 'Big bang' programme or 'do-able chunks'

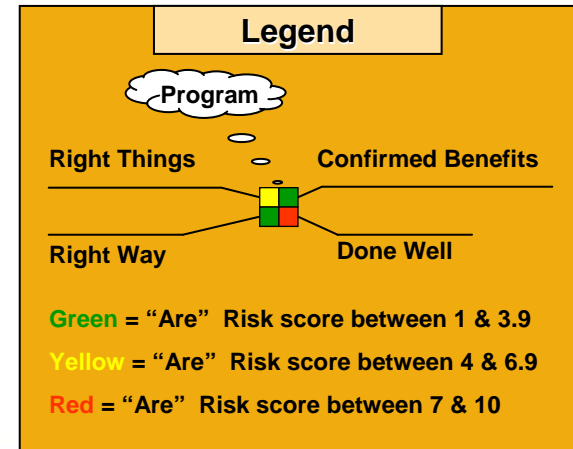
Robert.Stroud@ca.com



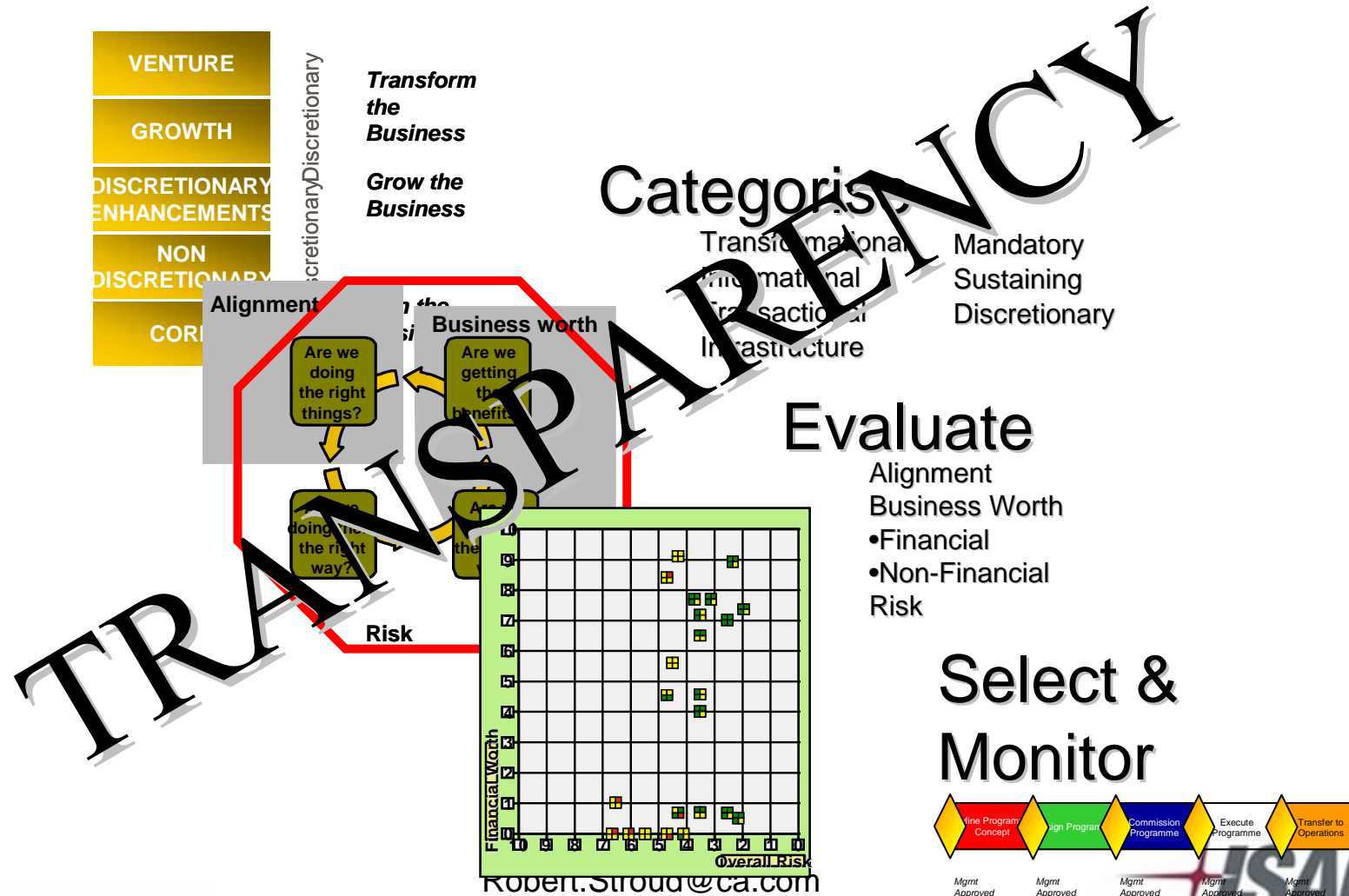
Evaluate & Select (PM9-10)



Financial Worth vs. Risk



Portfolio Management



IM12 - Benefits Register



Outcome	Metric / Frequency	Measurement Method	Baseline	Target Value	Profile	Tolerance Limit	Action if outside Tolerance	Accountability
Decreased Patient Transfers	No's of transfers/ 100 patients	Transfer Reports	5	40% reduction by 2005		+/- 10%	Examine Transfer reasons	
Increased Public Confidence in Health	Level of confidence / semi-annually	Public Opinion Survey	77%	90% by 2005		+/- 2%	Revisit communication plans	

Robert.Stroud@ca.com



Responsibilities of the CIO



- Deliver required technology services at an affordable cost with an acceptable level of risk
- Work in partnership with the (other parts of the) business to help them
 - optimize value from existing services
 - understand the opportunities for business change enabled by current, new or emerging technologies
 - understand the changes they will have to make (BPPTO) to realize value from these opportunities
 - select opportunities with highest potential value and execute such that value is maximized

Robert.Stroud@ca.com



What does this mean to you?



- Delivering the IT capability is not enough
 - Necessary but not sufficient
 - Value comes from how the business manages and uses IT
 - This increasingly requires significant organizational change
 - Business engagement and accountability are essential
- Look beyond IT practices/controls to business practices/controls
 - Business/IT partnership
- You can make a difference

Robert.Stroud@ca.com



Summary



Robert.Stroud@ca.com



Robert's advice



- Download the publications and the other good practices
 - Switch on your brain and read the guidance available
 - Stop any religious war
 - Get your stakeholders on board
 - Get a clear picture of where you are and where you want to be
 - Define the way and measurements
 - Do it!
 - Improve IT
 - Prove your improvement
-
- Remember read the materials and engage the brain!

Robert.Stroud@ca.com



Conclusion



- A wide range of good practices are available
- IT should not re-invent the wheel
- An overall control framework should be applied
- Good & best practices should be integrated
- It is possible & feasible
- External, independent support is beneficial
- If you still think, COBIT is for auditors only, go to www.isaca.org, download it and read it. You'll be surprised!



COBIT 4.1 and VALIT Updates!

Robert E Stroud
International Vice President ISACA
ITSM & IT Governance Evangelist
CA, Inc.

Robert.Stroud@ca.com

