The Impact and Opportunity of Compliance and IT Governance

Robert E Stroud CGEIT

VP Service Management & Governance

Service Management & Governance Evangelist

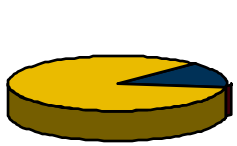
robert e stroud (CGEIT)

- Vice President, Service Management
  Service Management and Governance Evangelist
- 27 years Industry Experience
- 15+ years Banking Industry
- ITSM
  - Treasurer, itSMF International Executive Board
    Director Audit, Standards and Compliance
  - Former Director, itSMF USA
  - Member ITIL V3 Advisory Group (IAG)
  - Mentor ITIL V3 Service Transition
  - Contributor ITIL Business Perspectives Volume II
  - Author ITIL\COBIT\ISO17799 Management Overview
- IT Governance
  - International Vice President ISACA\ITGI
  - Chair COBIT Steering Committee
  - IT Governance Committee
  - Contributor to COBIT and VAL IT
  - Contributor to Basel II Guidance
- BLOG: www.ca.com/blogs/stroud

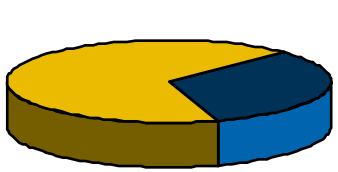

EG
POLICE

It’s no longer enough to align with the business

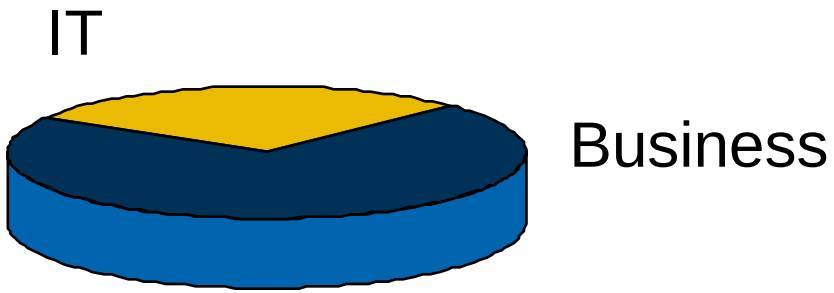
Automation of Work



Management of Information



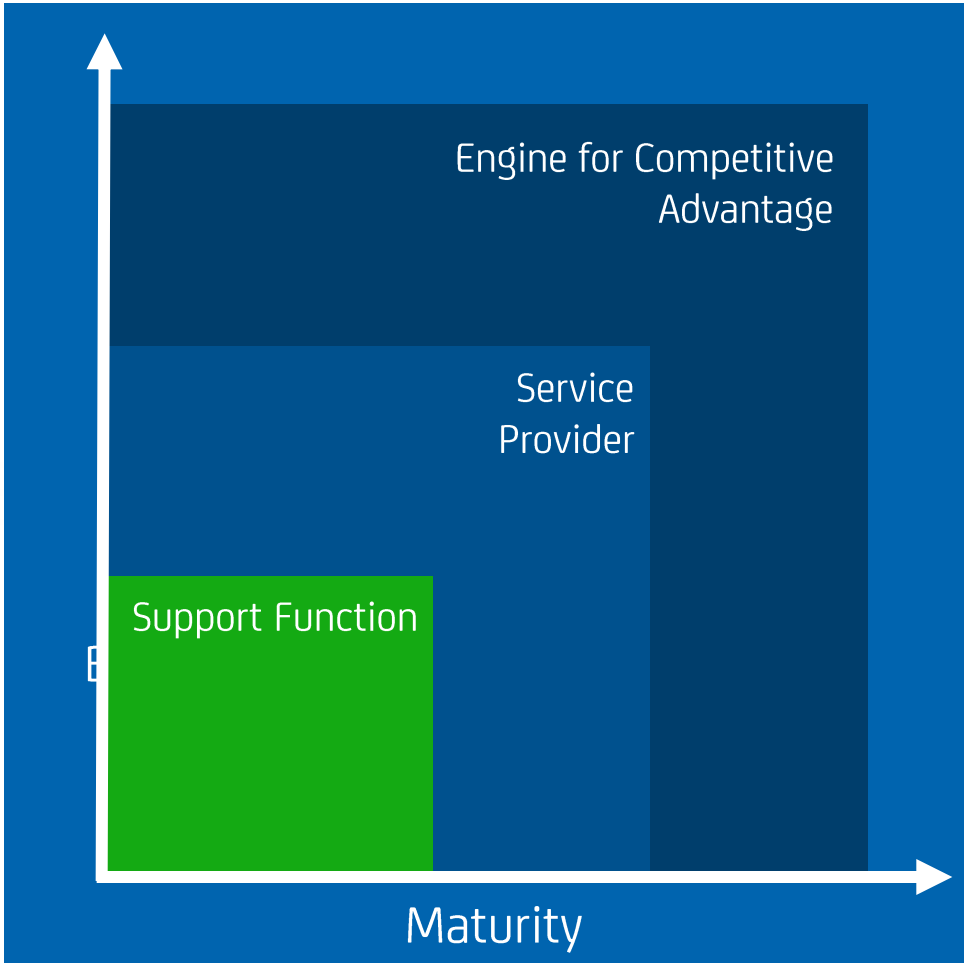
Transformation of Business



Imperative – business and IT integration

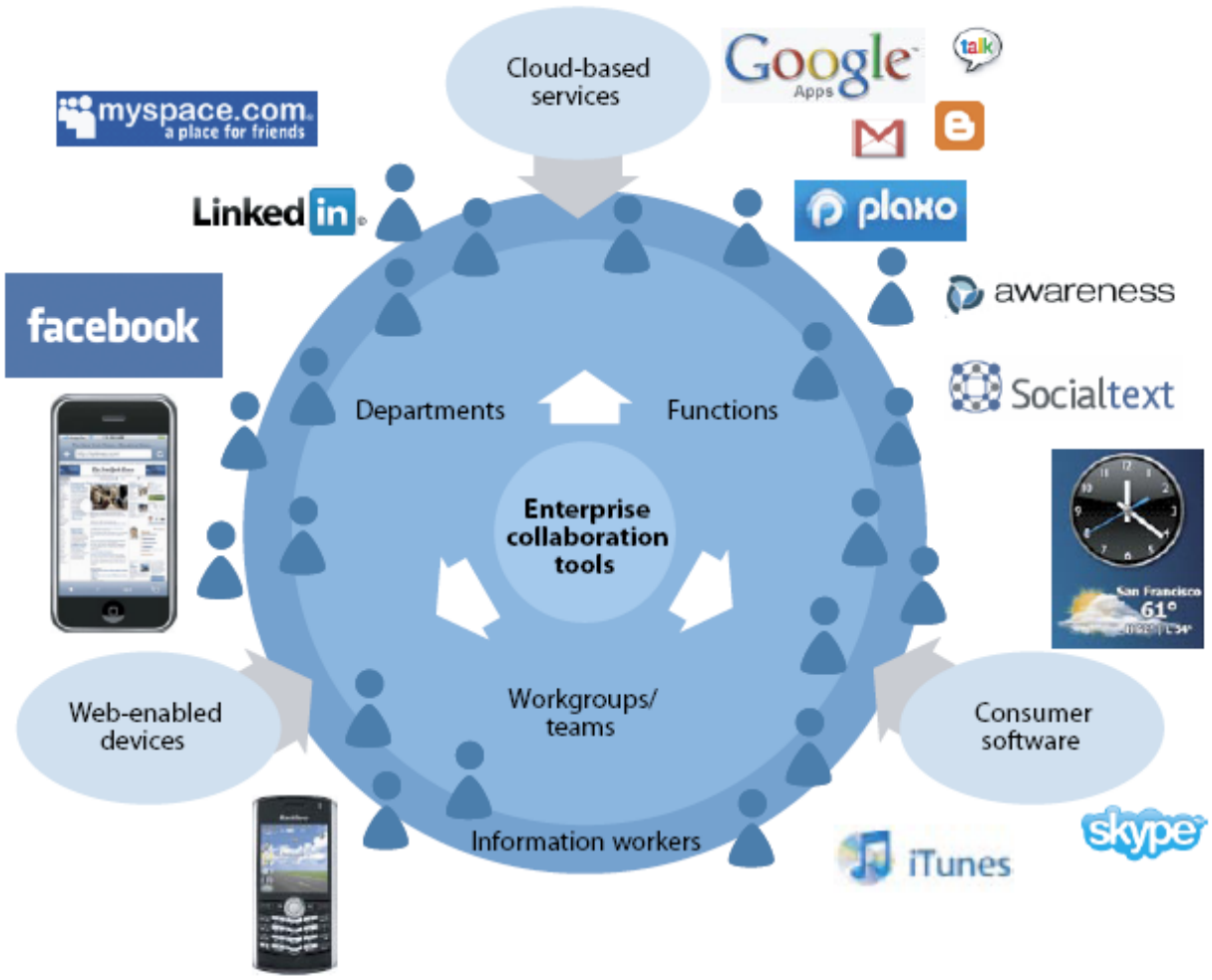
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Business Depends on IT for Competitive Advantage



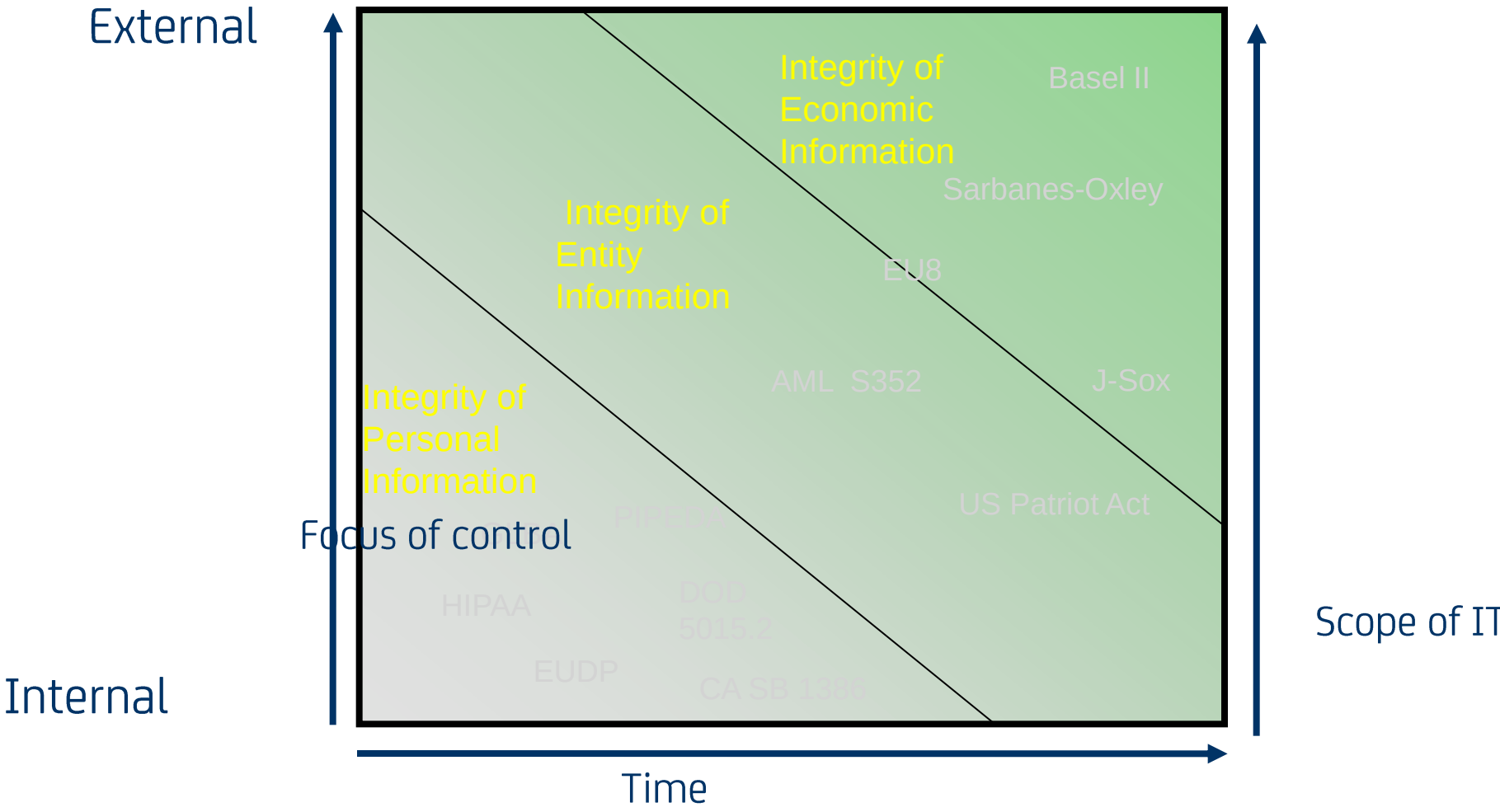
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Collaboration



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Compliance growing every day



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Compliance must be part of your DNA!

- Not a one-time event
- An increasingly urgent topic of discussion
- Penalties and fines for noncompliance are significant – both civil and criminal penalties
- Multiple pieces of legislation

Compliance with government regulations is no longer just a legal matter but,

rather a critical business function

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud


Hercu
U.P. CY

Business and IT integration

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Risk and Compliance
Big Challenge — Big Opportunity

Things We Know About Risk and Compliance

> It's not going away

> More regs are coming

> Failure is not an option

Turning Risk & Compliance to Advantage

> Reduce the cost

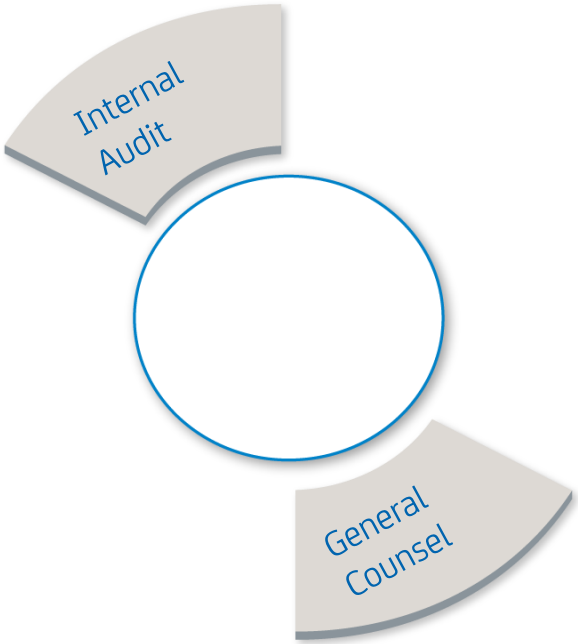
> Reduce the disruption

> Use it to drive operational improvement

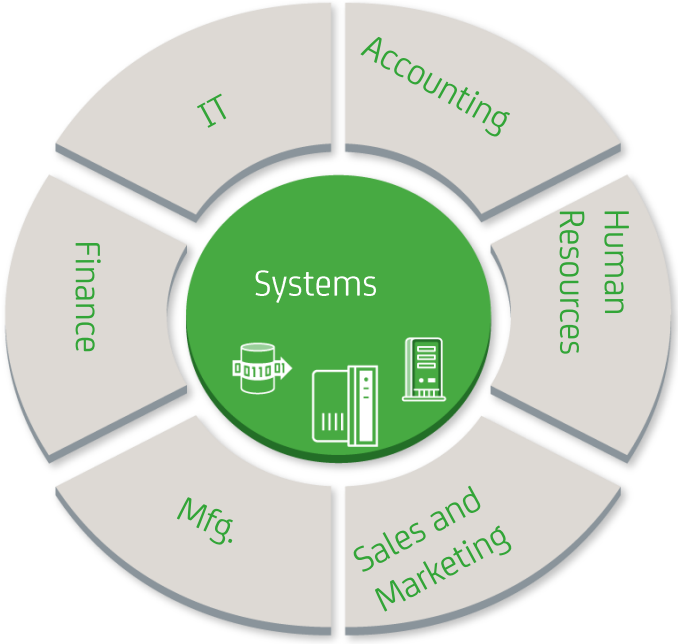
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Compliance: The Early Days

Risk and Compliance

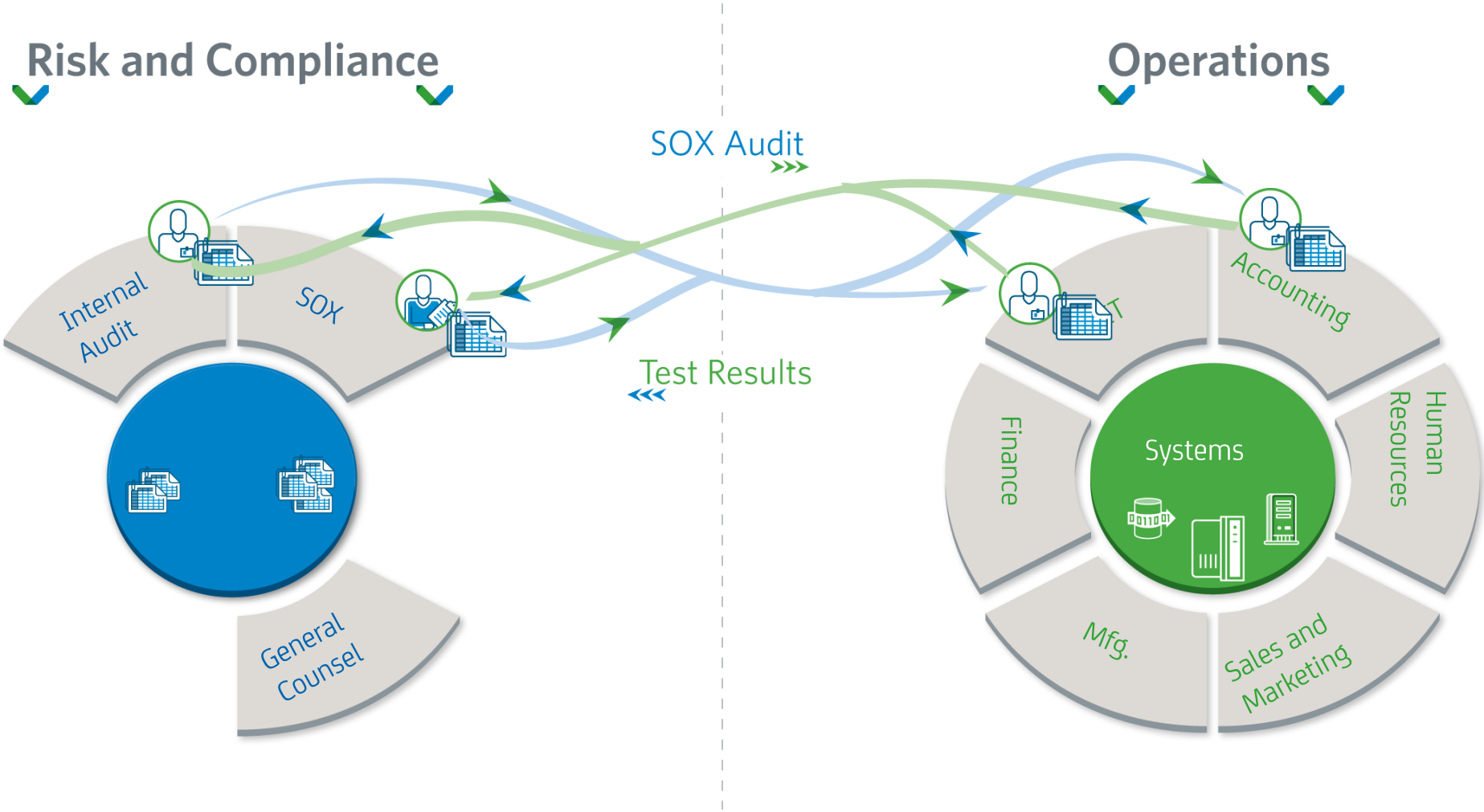


Operations



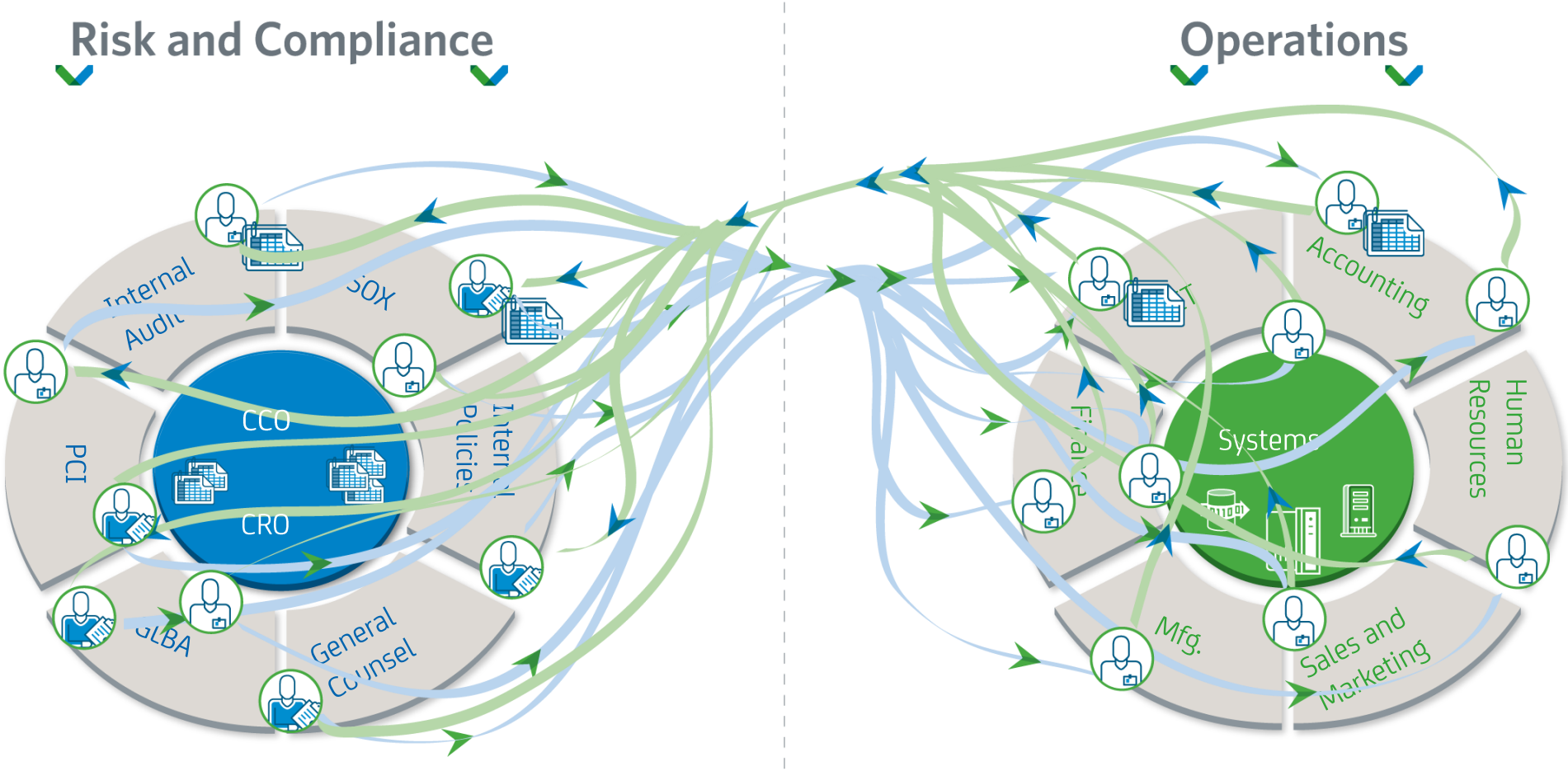
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Enter SOX



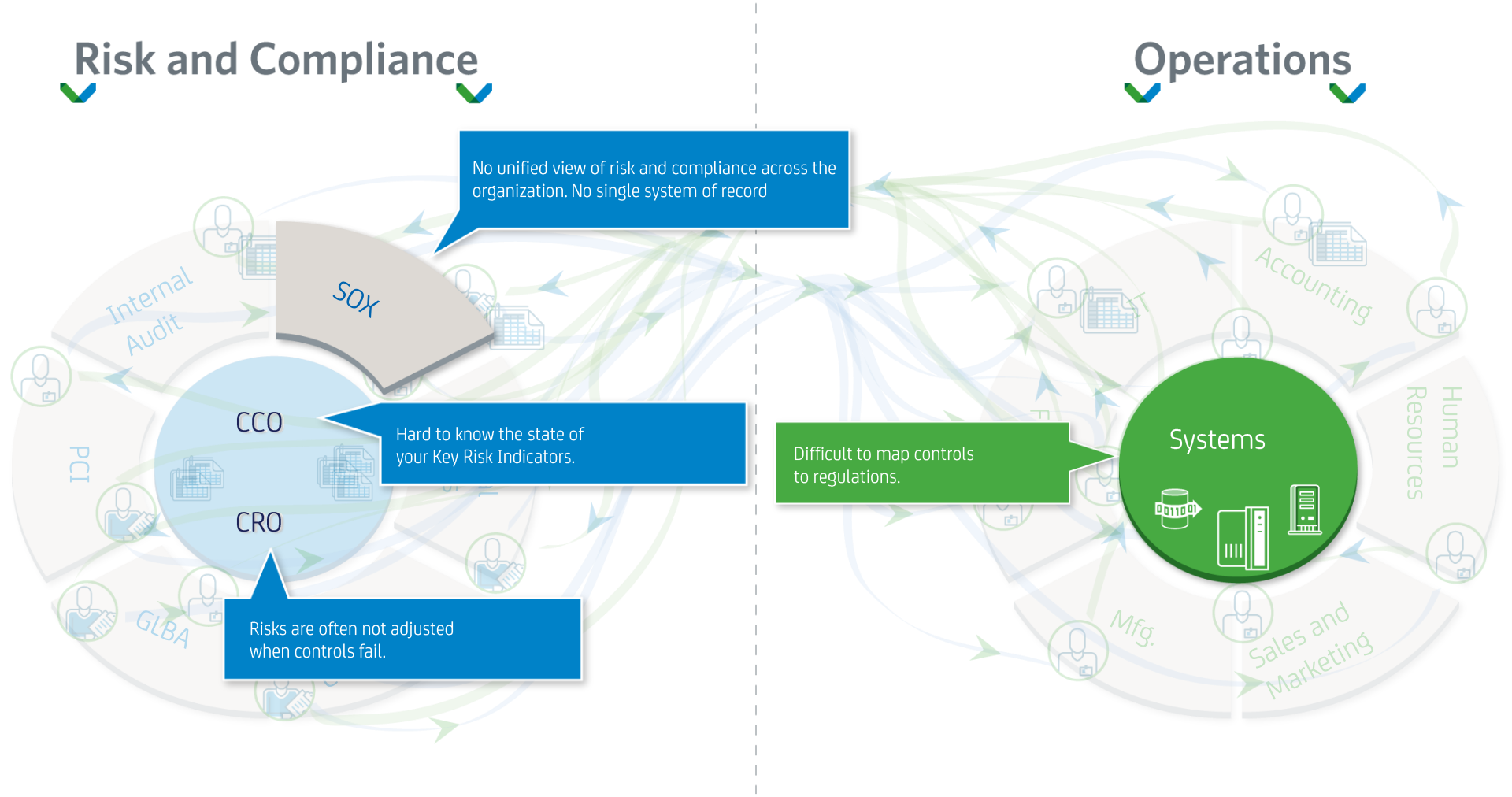
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Next Come PCI, GLBA, Internal Policies (as well as Compliance Management)



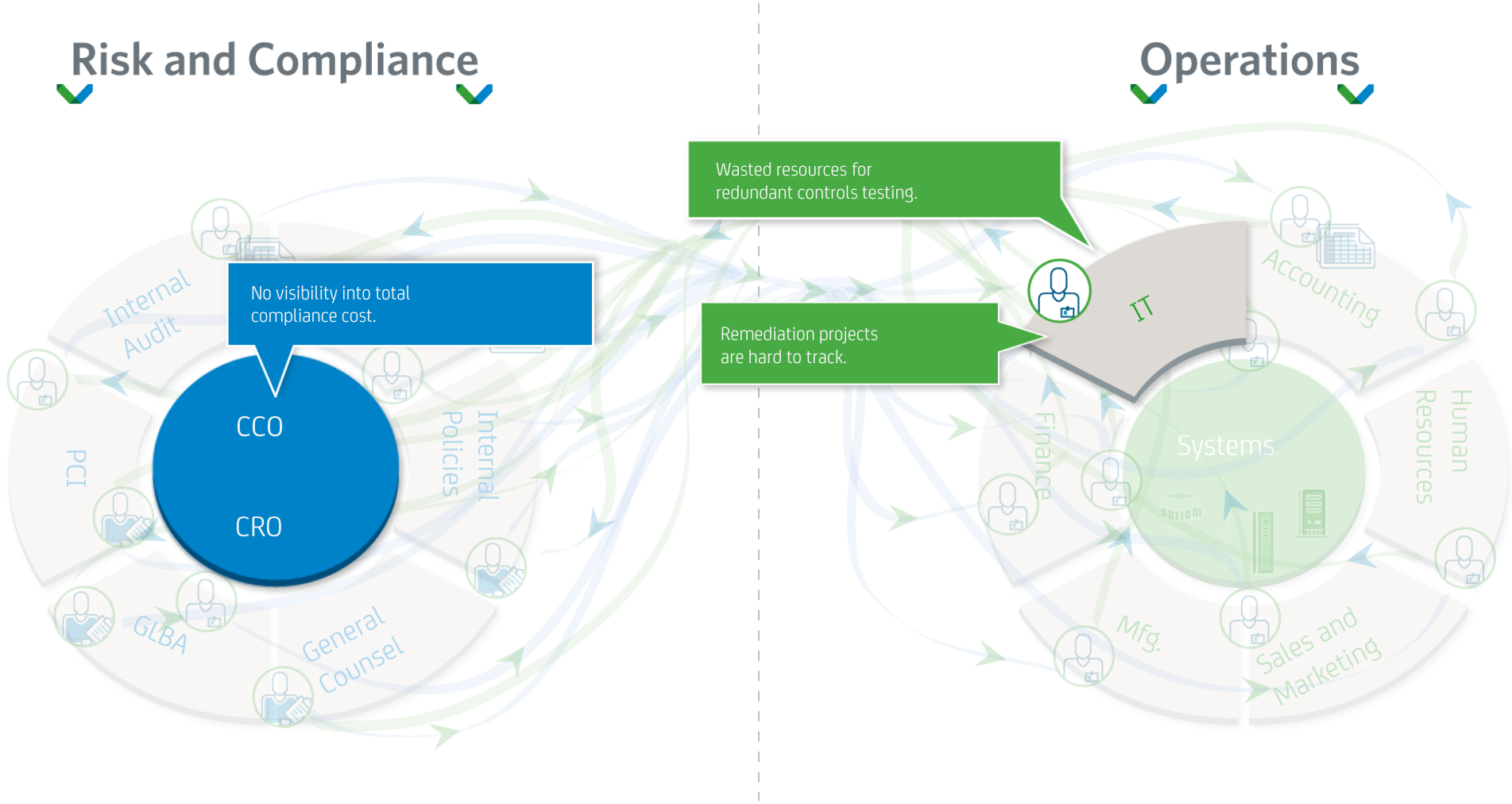
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Risk and Compliance Is Fragmented, Complex



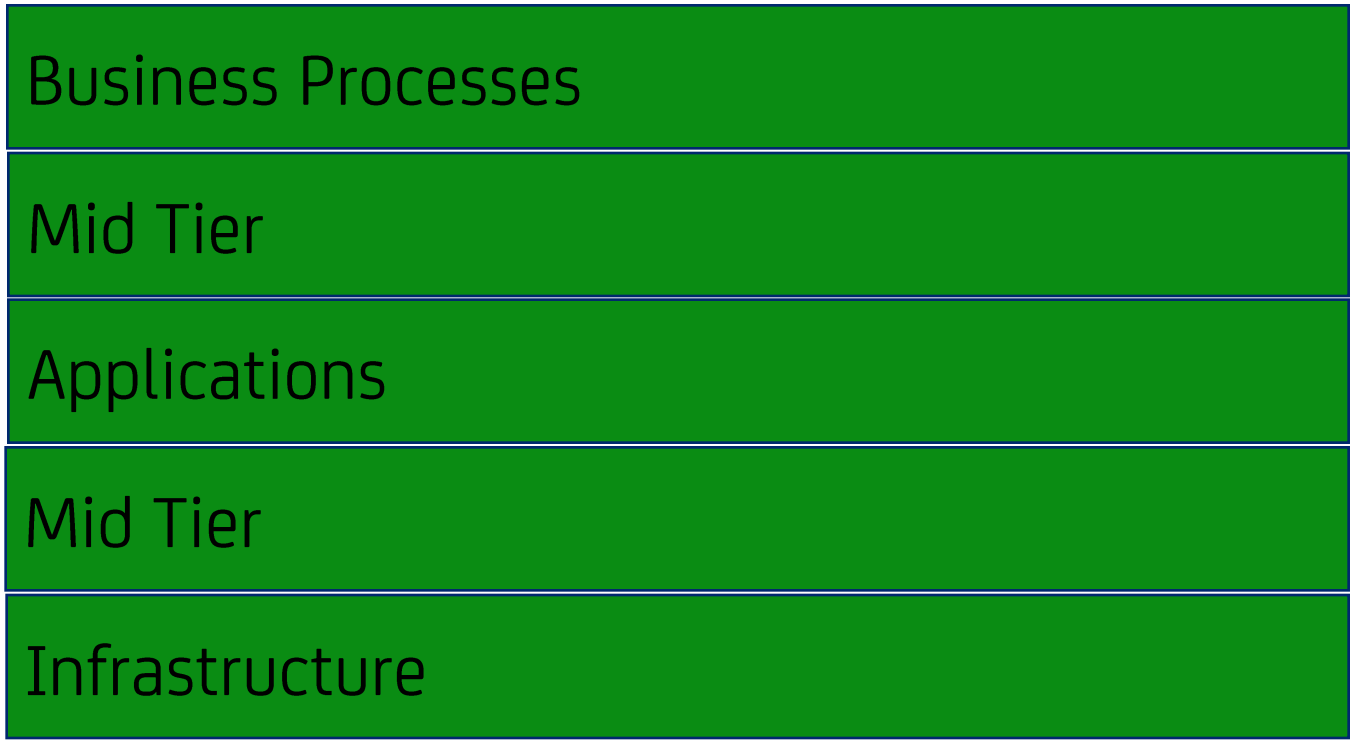
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Risk and Compliance Is Costly



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Changing World



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

GRC is key

- Organizations are sacrificing money, productivity and competitive advantage by not implementing effective GRC
- Executives need a method to:
  - Direct IT for optimal advantage
  - Manage IT-related risks
  - Measure the value provided by IT

Robert E Stroud (CGEIT) Robert.Stroud@ca.com

Definition

- Governance is more than compliance
  - Business strategy
  - Risk Appetite
  - Sound management
  - Business and IT alignment

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Definition of Governance

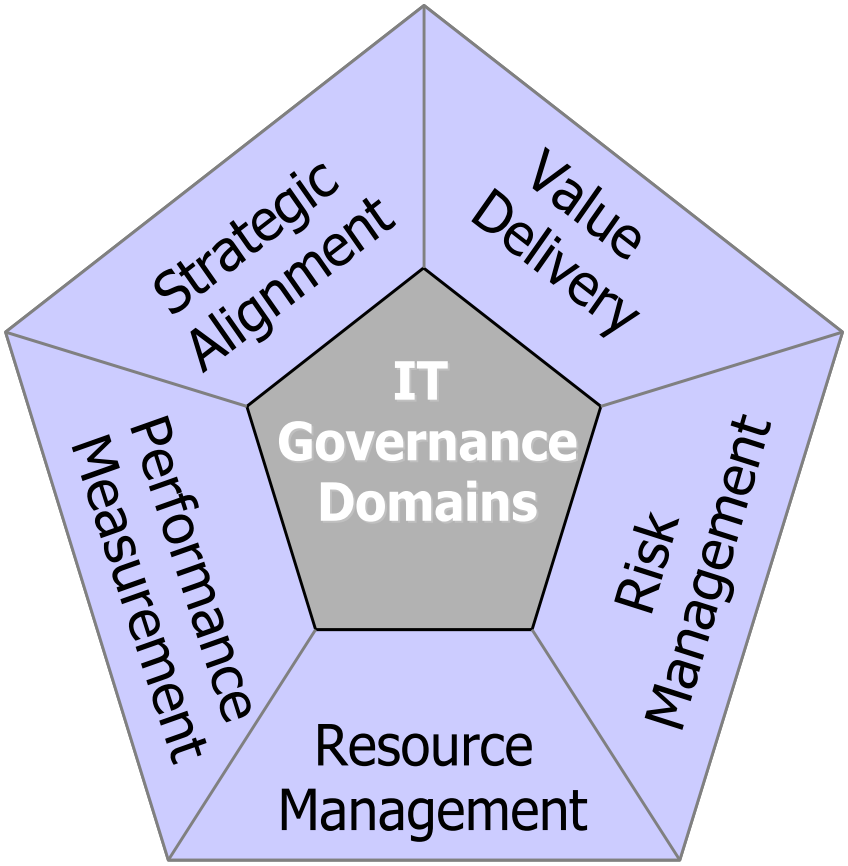
- Development of policies, procedures and rules within the domains must be developed
- Do not "make up" governance processes for each scenario
- Clear, consistent, definition of governance

Remember:
To much governance may kill innovation!

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Definition of Governance

—Definition of the domains that will be governed.

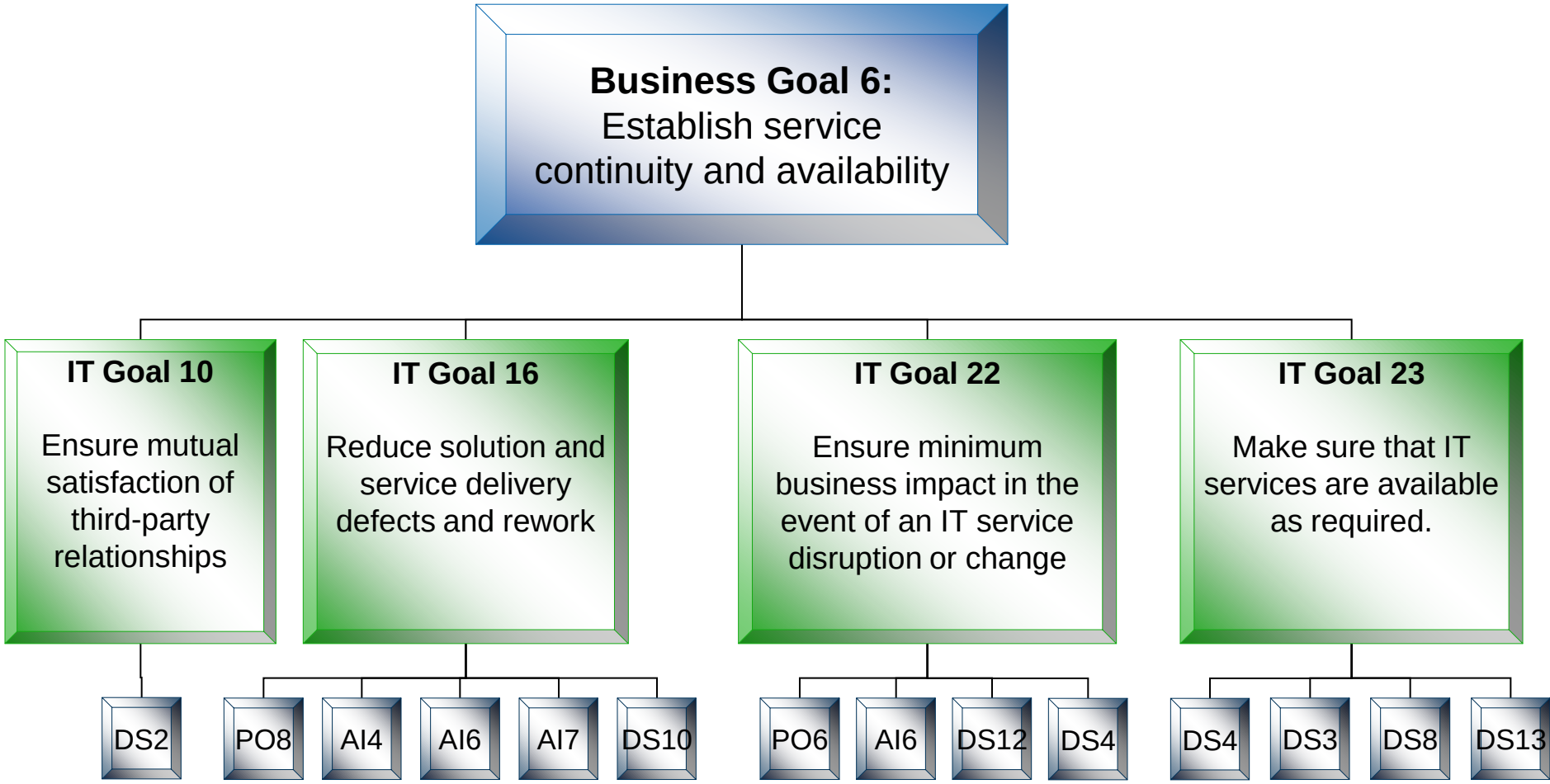


Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

		Business Goals	IT Goals					
Financial Perspective	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
	3	Improve corporate governance and transparency.	2	18				
Customer Perspective	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	
Internal Perspective	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
	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		
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28			
	17	Acquire and maintain skilled and motivated people.	9					

1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13		
4	Optimise the use of information.	PO2	DS11								
5	Create IT agility.	PO2	PO4	PO7	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.	PO3	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.	PO7	AI5								
10	Ensure mutual satisfaction of third-party relationships.	DS2									
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7							
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4			
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2					
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10					
17	Protect the achievement of IT objectives.	PO9	DS10	ME2							
18	Establish clarity on the business impact of risks to IT objectives and resources.	PO9									
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12						
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5							
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2			
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	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.	PO5	DS6								
25	Deliver projects on time and on budget, meeting quality standards.	PO8	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.	PO5	DS6	ME1	ME4						

Linking IT and Business



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Governance Ownership and Execution

- Governance is about policy, procedure and rule definition; that those policies, procedures and rules must be agreed on by senior leadership
- Management puts the governance processes in place and ensures that they're followed its individual groups.

Measurement

Governance without measurement is a waste of time!

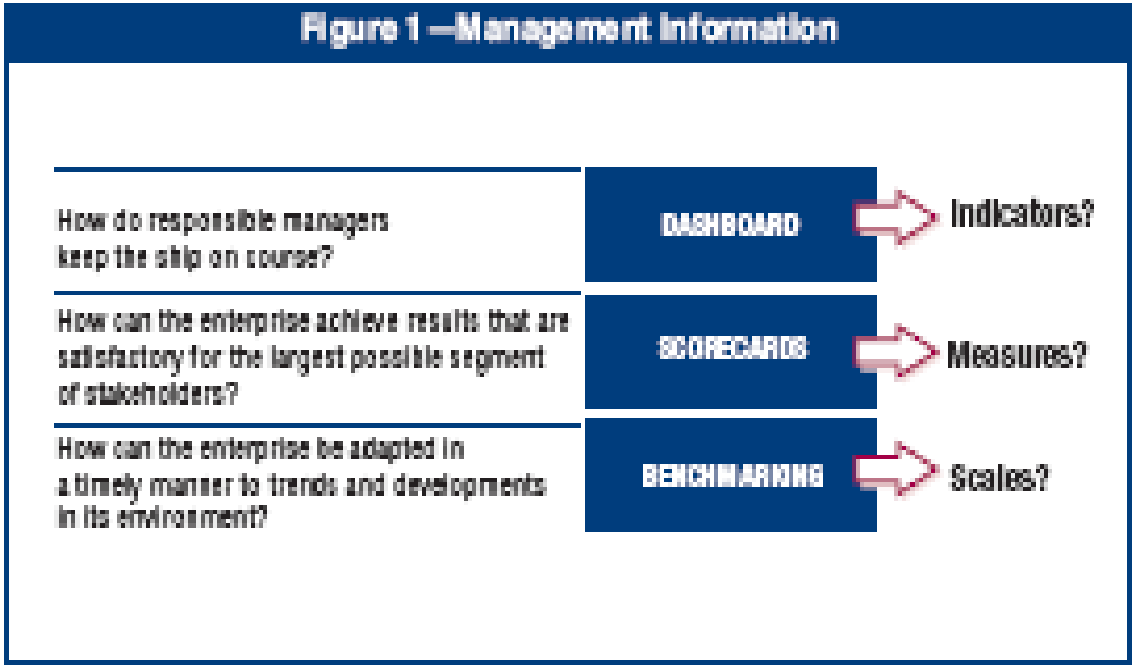
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Measurement

- Processes without measurement is not effective governance
- Governance must have a set of processes that provide feedback loops to understand whether the processes status
- Each of the major governance areas must have measures
- Balanced scorecard\dashboards to define your key process indicators.
- Responsibility for metrics must be allocated
- Every organization must have a set of key measures to use when charting status and progress

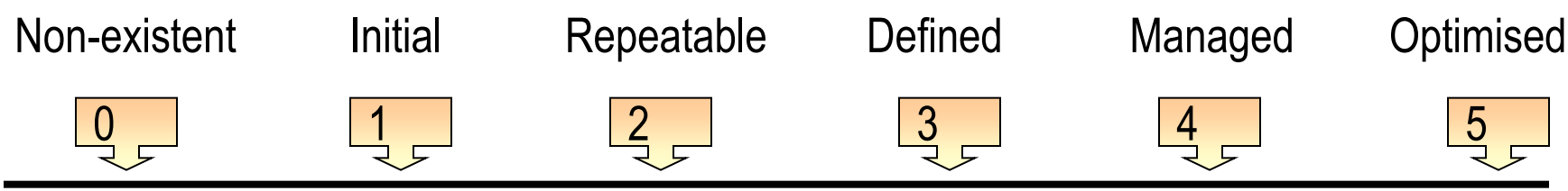
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Measurement



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Measurement



0 - Management processes are not applied at all.
1 - Processes are *ad hoc* and disorganised.
2 - Processes follow a regular pattern.
3 - Processes are documented and communicated.
4 - Processes are monitored and measured.
5 - Best practices are followed and automated.

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

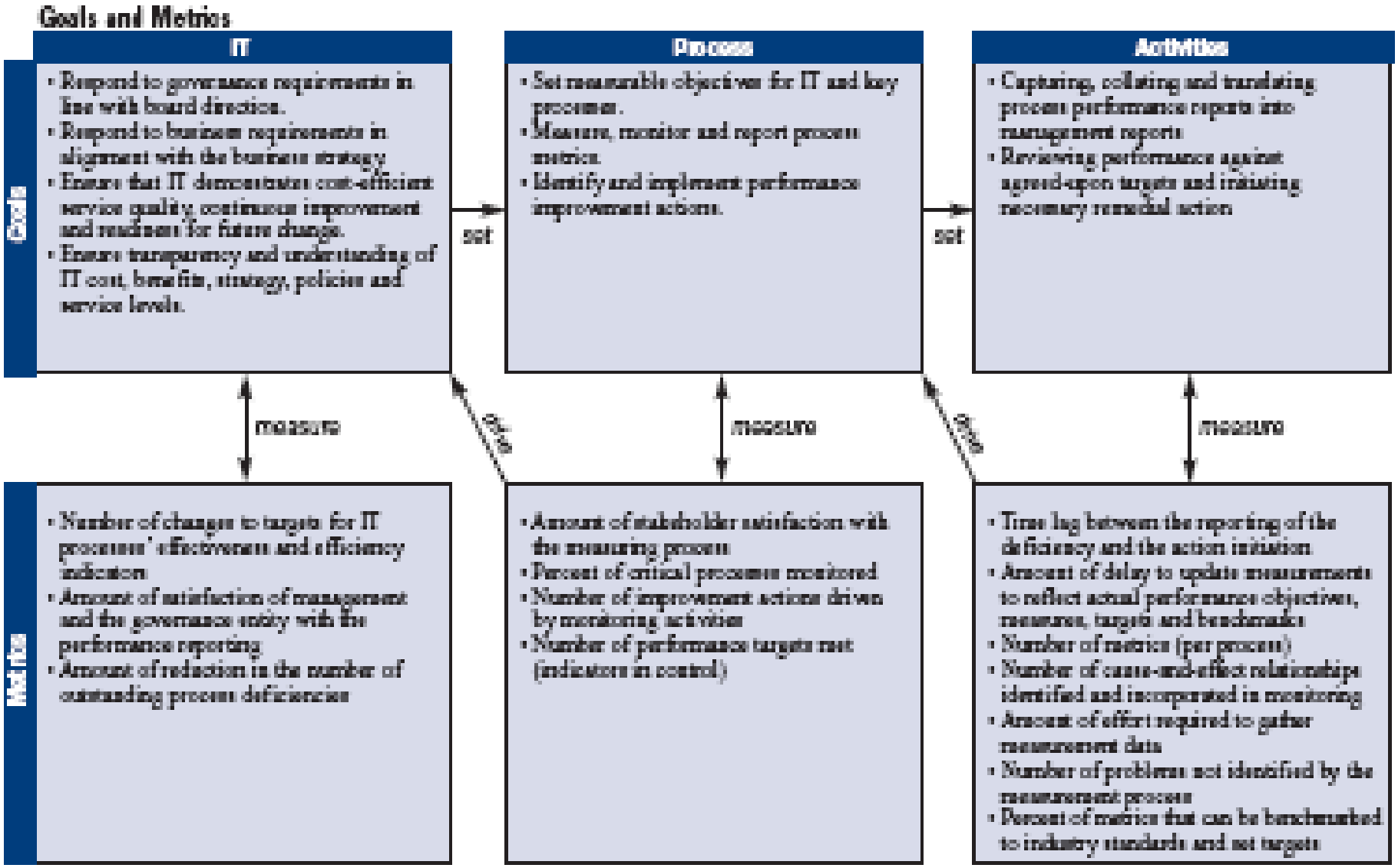
Management of the process of *Monitor and evaluate IT performance* that satisfies the business requirement for IT of *transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements* is:

0 Non-existent when
The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.

1 Initial/Ad Hoc when
Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. The accounting function monitors basic financial measures for IT.

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Measurement



Measurement

RACI Chart

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish the monitoring approach.		A	R	C	R	I	C	I	C	I		C
Identify and collect measureable objectives that support the business objectives.		C	C	C	A	R	R		R			
Create scorecards.					A		R	C	R	C		
Assess performance.			I	I	A	R	R	C	R	C		
Report performance.	I	I	I	R	A	R	R	C	R	C		I
Identify and monitor performance improvement actions.					A	R	R	C	R	C		C

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

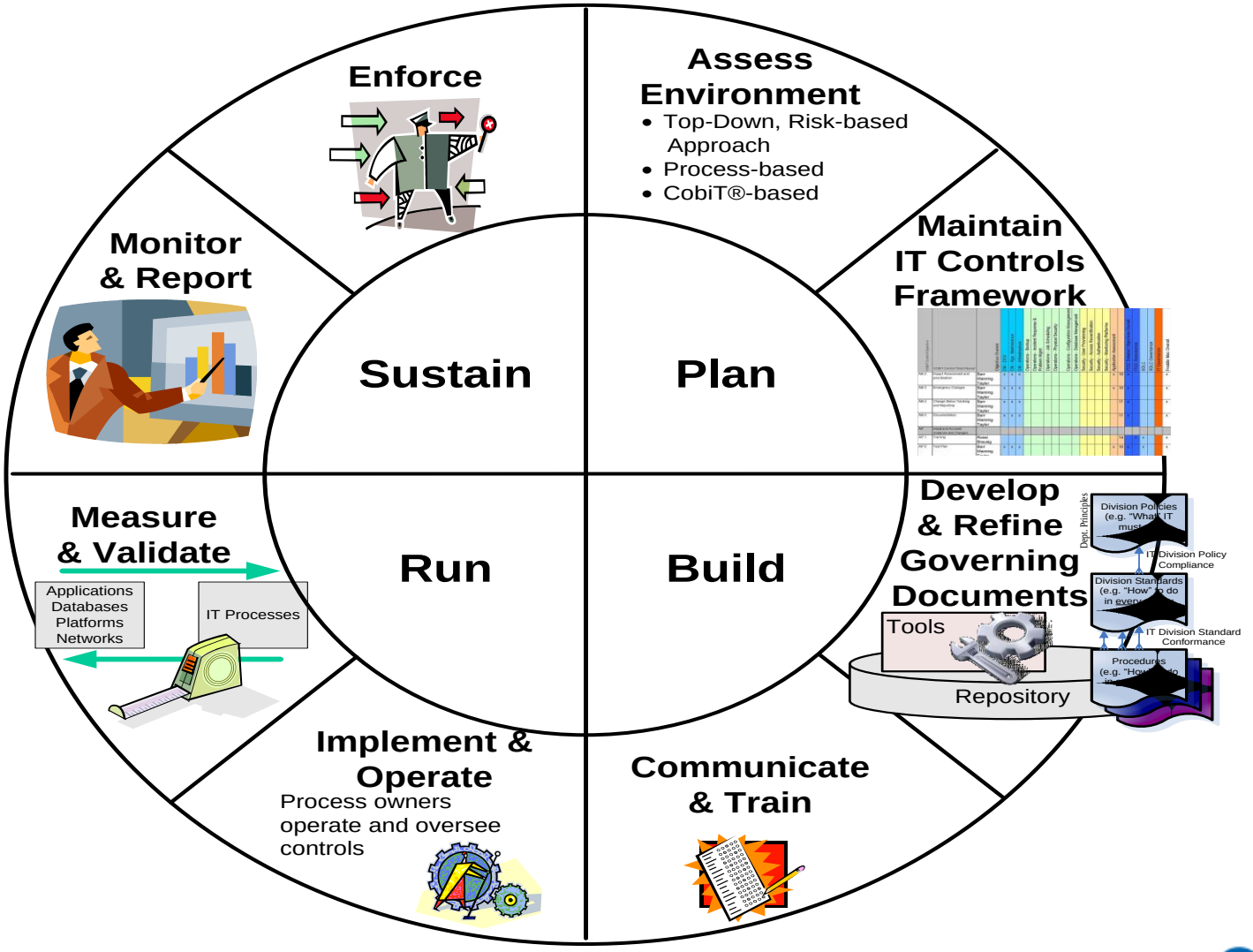
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

GRC Automation

- Governance processes require integration of information from multiple data sources
- Process collection manually is full of errors, develop the process and automate for consistent results
- IFRS must will mandate more controls around financial processes

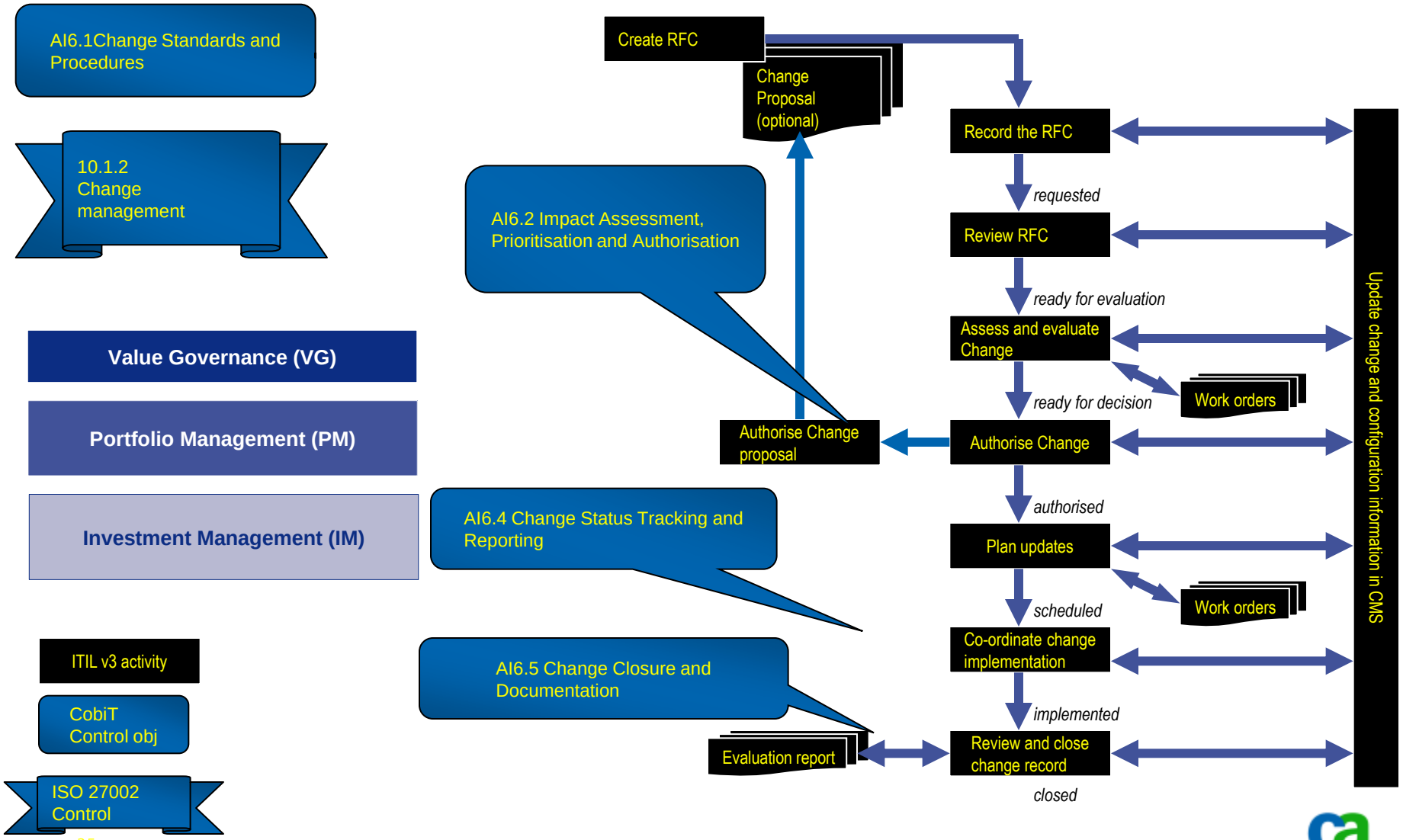
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Control Cycle



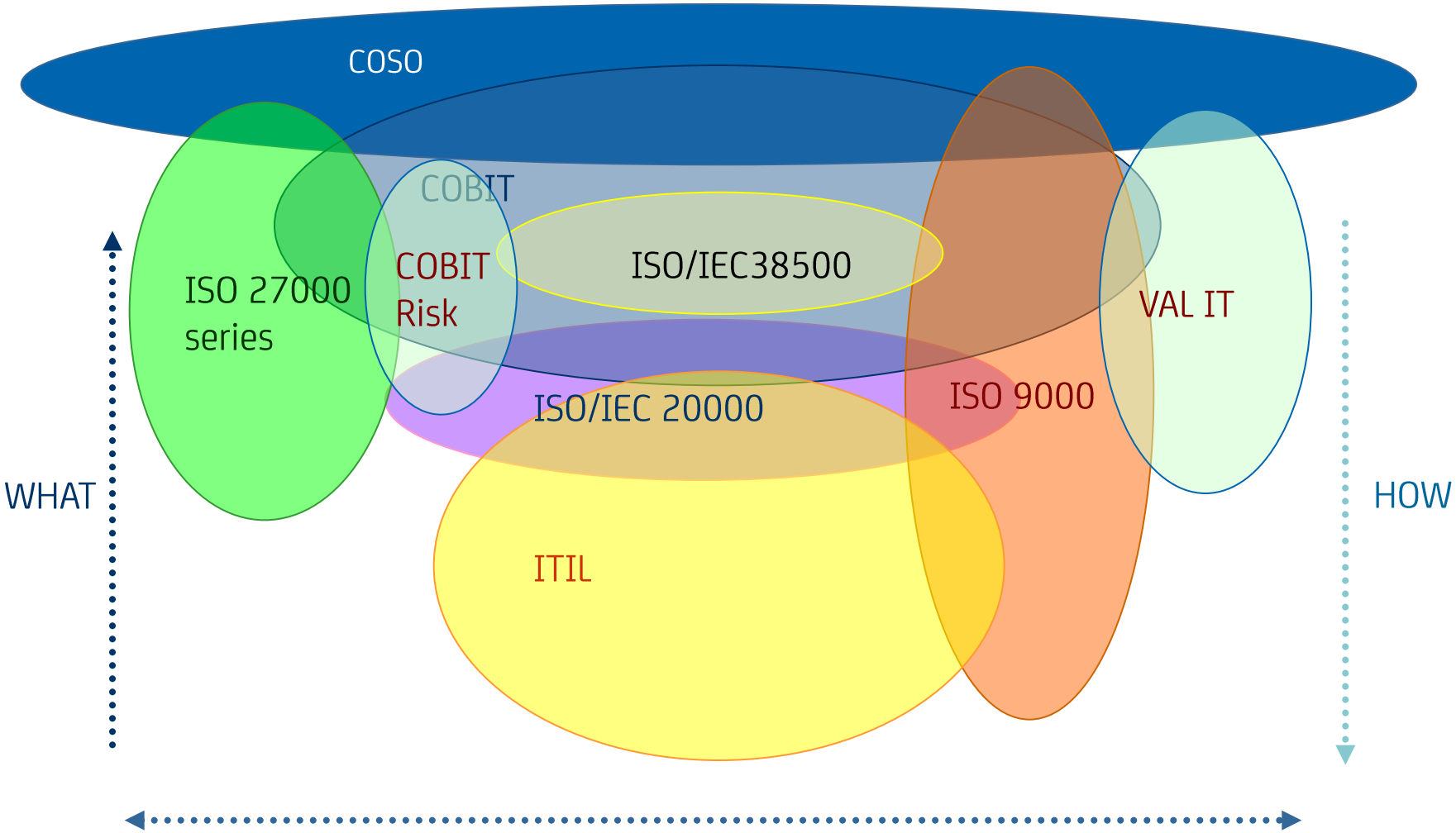
Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Example: Change Management



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Governance and Frameworks



Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Summary, Recommendations and Next Steps

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Summary

- Established Frameworks give you the descriptive guidance
- Use Standards to document, guide and measure the implementation
  - Maturity Models
  - Where do I need to be?
  - Industry Yardstick
- Quality
  - Reduce Errors
- Pick the components YOU require in YOUR Business.

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Summary

- "Just enough" should be the approach to governance in terms of "what" is governed and to what depth.
- Governance processes are the purview of senior management
- Your Management processes are how resources are used effectively every day

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Business Imperative Action Plan

- When you get back to the office
  - Visit www.isaca.org and download the guidance
  - Assess your current level of process maturity
  - Develop your metrics
  - Identify the gaps
  - Plan the implementation
  - Get moving!

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

GRC Ownership and Execution

- GRC must be the purview of the senior management team
- Accountability - senior management team
- Senior Management must ensure that the people working in their organization are doing the right things
- CIO is accountable execution
- Audit must be involved to ensure processes are followed
- Learn from others!

Robert E Stroud (CGEIT) Robert.Stroud@ca.com BLOG: www.ca.com/blogs/stroud

Thank you!

MORE INFORMATION

Email: Robert.Stroud@ca.com

Web: www.ca.com/itil

Twitter: www.twitter.com\RobertEStroud

BLOG: **www.ca.com/blogs/stroud**

The Impact and Opportunity of Compliance and IT Governance

Robert E Stroud CGEIT

VP Service Management & Governance

Service Management & Governance Evangelist