"The Total Control Package"

COBIT, ITIL V3 and ISO Certification

About McKesson…

McKesson is uniquely positioned to help shape healthcare's future

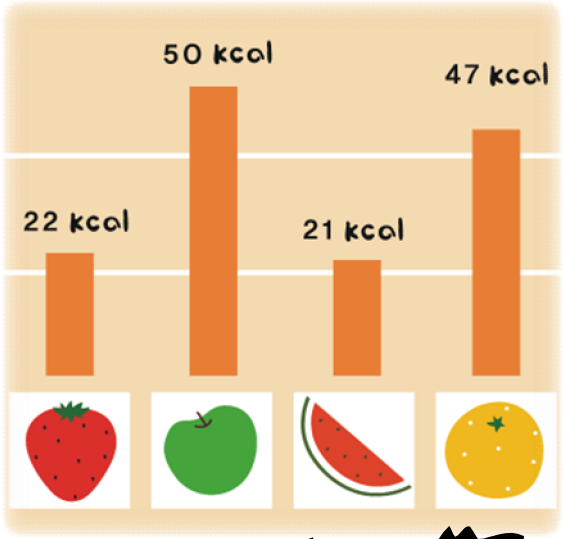
- Largest healthcare services company in the world
  - Fortune 15 – $112 billion in revenues (FY11)
  - More than 32,000 employees dedicated to healthcare
- Oldest U.S. healthcare company
  - Established 1833 – Over 175 years driving innovation in healthcare
- Deep clinical, IT and process expertise
- Only company offering solutions at every point of care

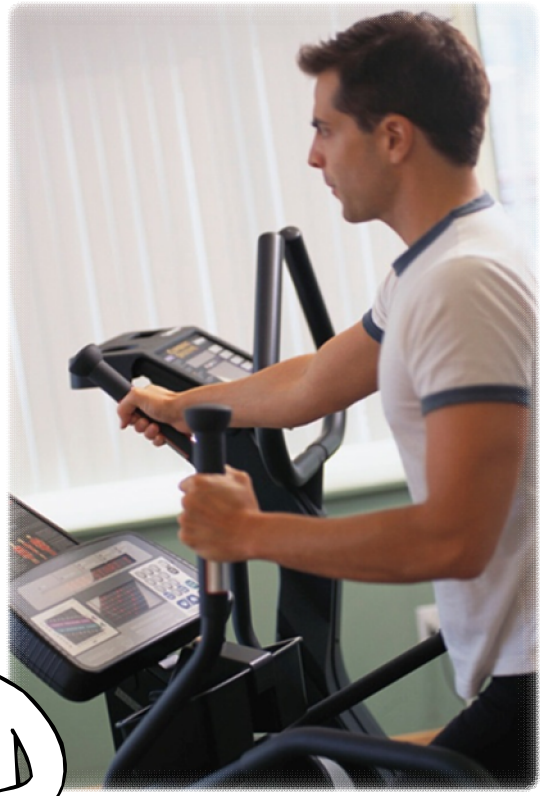
McKESSON
Empowering Healthcare

How can I ….

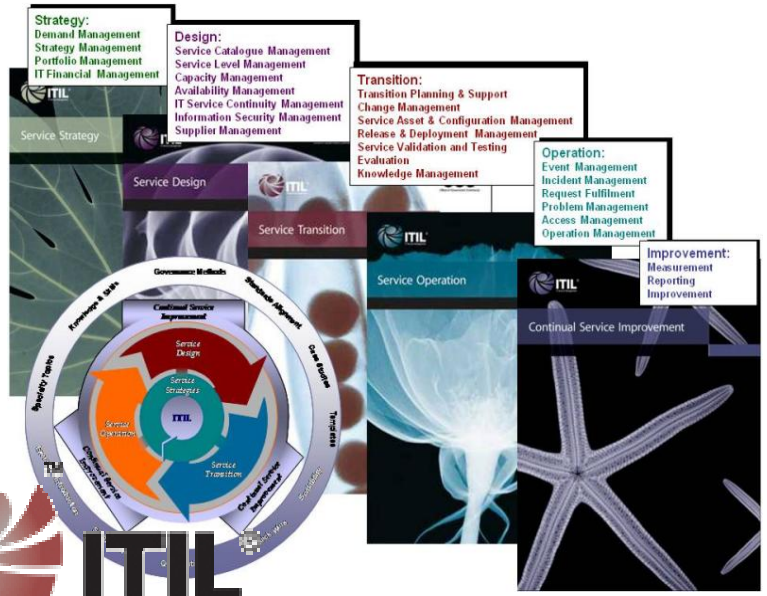
- Align IT objectives with business vision and strategy
- Gain/maintain the competitive advantage
- Comply with regulatory requirements
- Support information security
- Align risk management with business risk tolerance
- Reduce costs of IT services

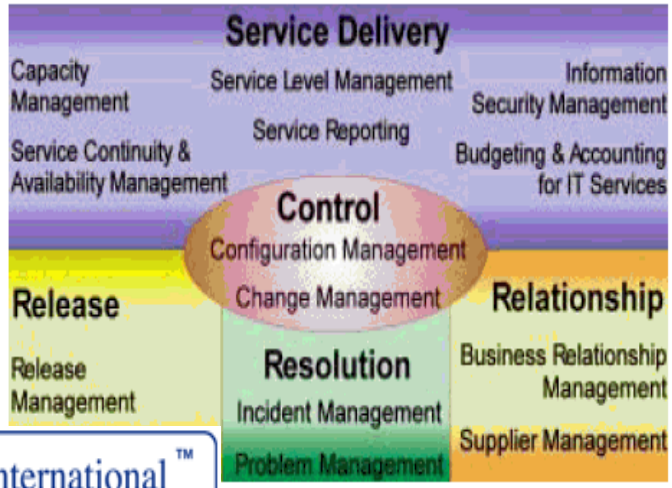
A Total Fitness Package





The Total CONTROL Package





What Will We Cover Today?

- How the *Total Control Package* elements work together
- The business value of The Total Control Package
- A model for customizing the *Total Control Package* to your organization
- A recognized model for cultural change
- Impact of recent ITIL V3, COBIT and ISO 20000 revisions
- Business case for certification
- Experience/expertise from the audience
- References to take a “deeper dive”

Working Together To Achieve Control

COBIT drives *"what to do"*

- *Supported by ITIL V3 Service Strategy*

ITIL V3 guides *"how to achieve improvement"*

- *Supported by COBIT's control objectives and practice*

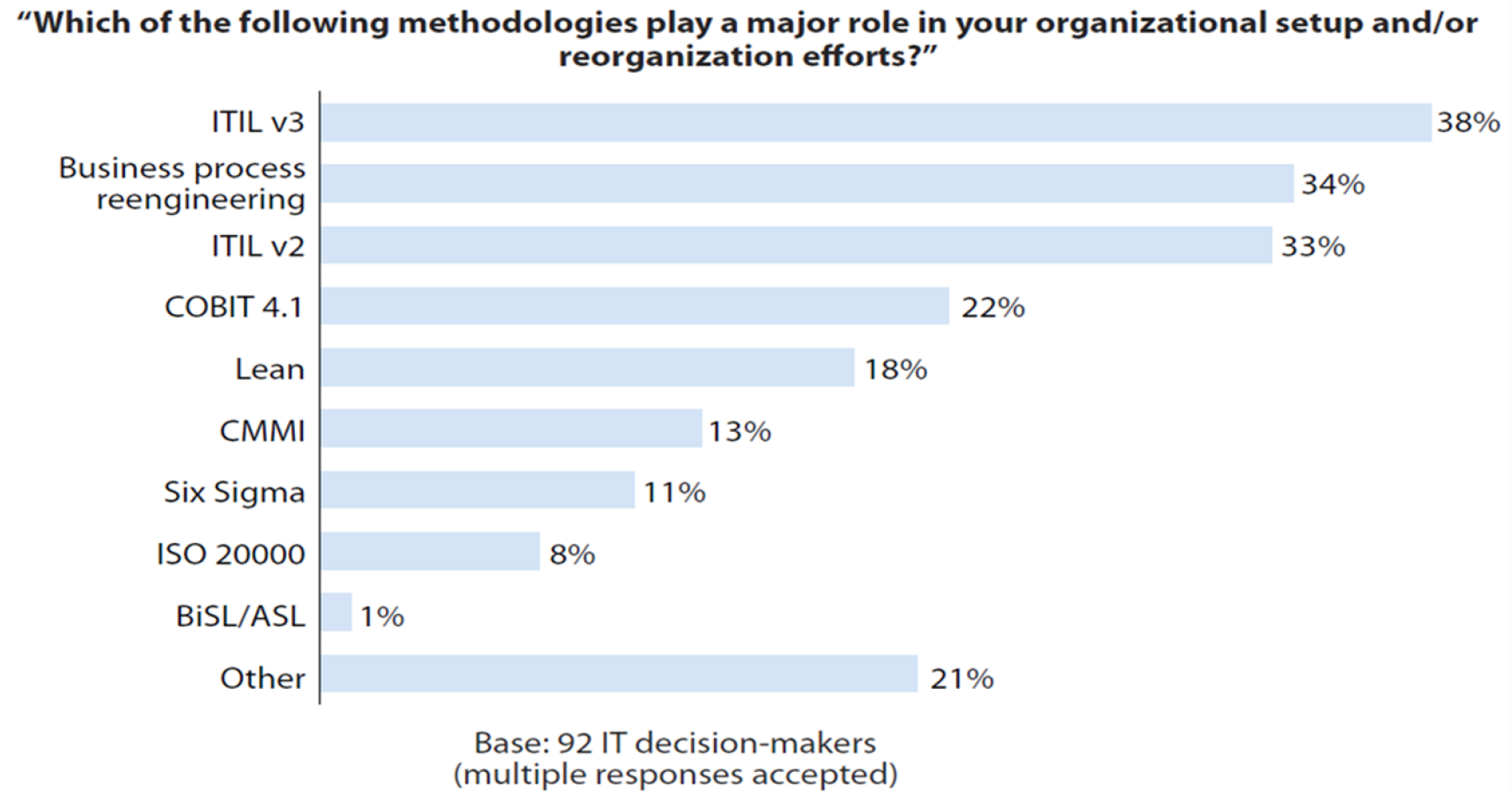
ISO certifies *"organizations against international standards*

- *ISO 20000 provides specific requirements for ITIL*
- *ISO 270001 provides specific requirements for information security*
- *Other ISO certifications as applicable to the organization*

ISO Certifies Organizations

ITIL V3 Guides Organizational Structure

Figure 1 The Service-Oriented ITIL v3 Is The Most Applied Methodology For Organizational Setup

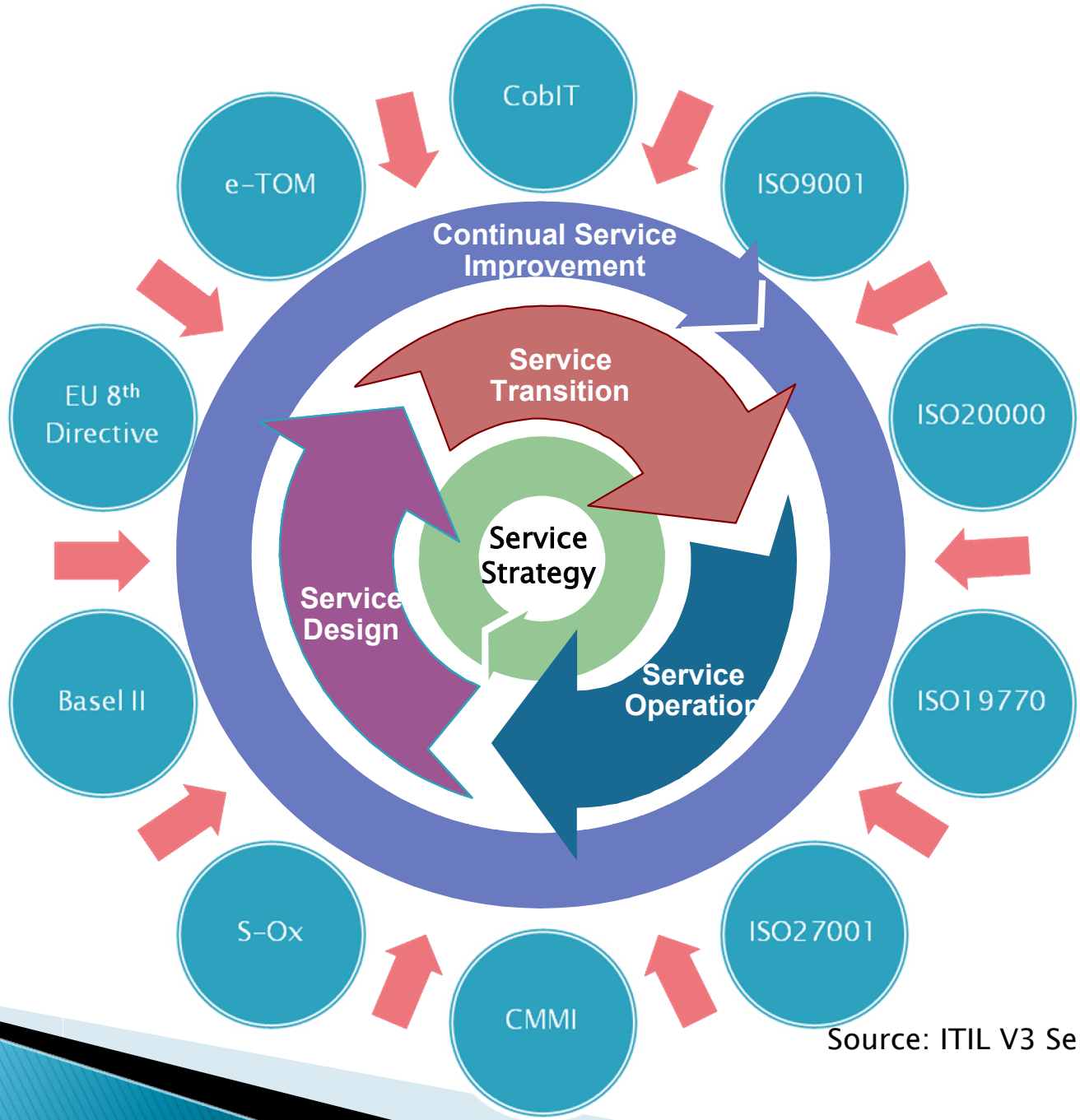


Source: Q3 2009 Global IT Service Orientation Online Survey

56627

Source: Forrester Research, In

Support for The Total Control Package



Source: ITIL V3 Service Design Volume

2011 AICPA Top Technology Initiatives

How the Total Control Package Measures Up?

How important are each of the following questions that you, your senior management team, or your client may be encountering during the next 12 to 18 months? (example: the audit committee, CEOs, CFOs, CIOs, etc.)	COBIT	ITIL V3	ISO 27001
Is our information security policy adequate?	X	X	X
Are we ensuring that our data and technology resources are protected against hacking, viruses, or other compromises?	X	X	X
Are our current internal controls and IT governance policies and procedures effective?	X	X	
How can we best implement document retention and e-discovery policies?	X	X	
Can our data remain safe if we utilize cloud computing/Software as a Service (SaaS) services?	X	X	X
Are we receiving the most relevant and current information from our reporting functions (business intelligence, dashboards, etc.) or are there areas for improvement?	X	X	
Should we refresh our core and financial accounting software to leverage technology efficiencies every few years?	X	X	
Have we implemented a sound/appropriate privacy policies and procedures within the organization and for our customers?	X		
How can we best align IT investment to our three and five year business plan?	X	X	X
What is the biggest/most important technology investment that has not been made?	X	X	

Source: AICPA Website

The Total CONTROL Package

COBIT 5 Supports the *Total Control Package*

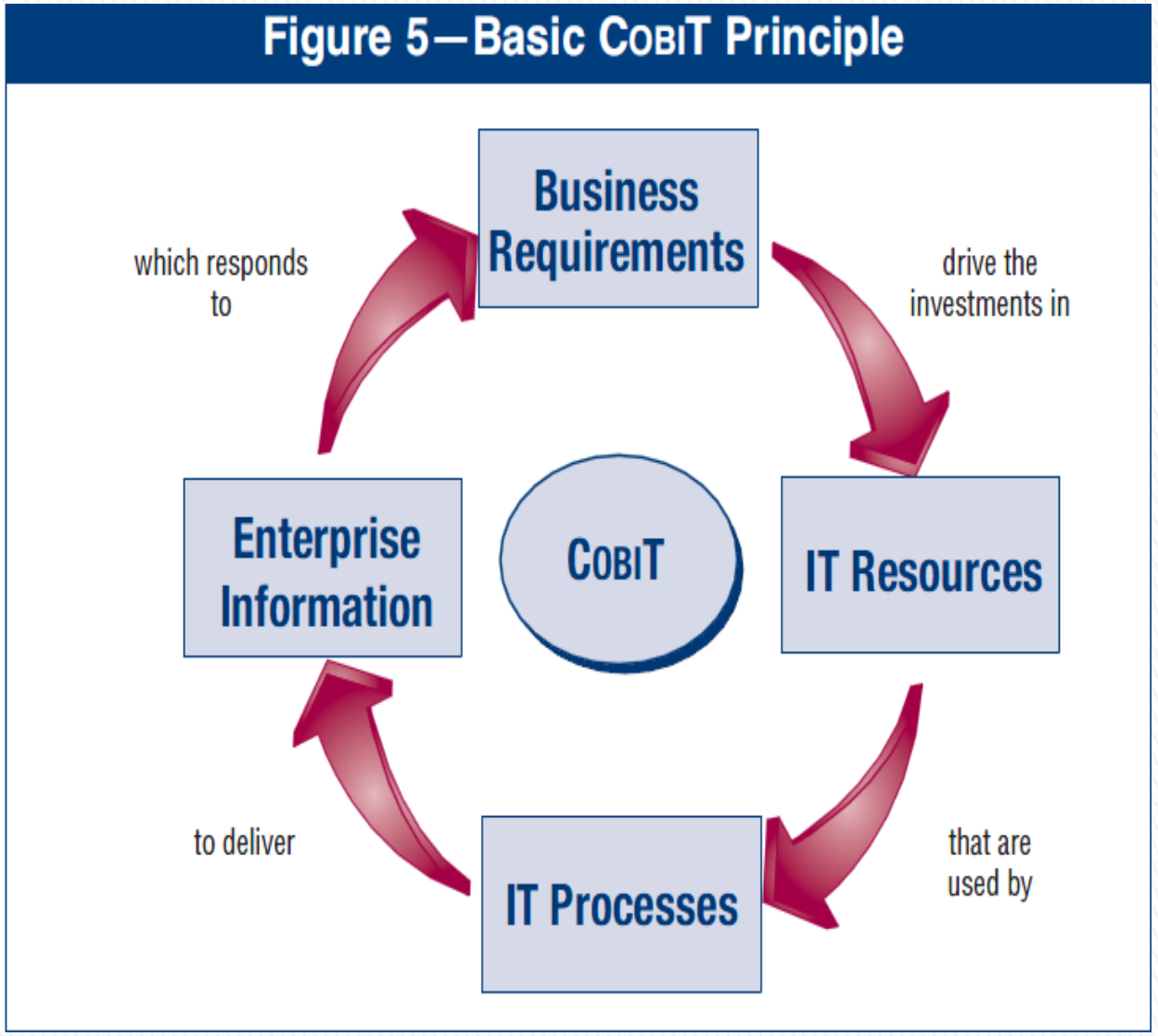
- Connect with other major frameworks and standards
  - ITIL, ISO, ISF, OECD, AICPA and NIST
- Increased value creation from use of IT
- User satisfaction with IT engagement and services
- Compliance with laws, regulations and policies
- The development of a more business-focused IT function
- Increased user contribution to the enterprise
- Integrate other ISACA guidance
  - Val IT, Risk IT, the IT Assurance Framework & Bus. Model for Info. Security (BMIS)

Source: ISACA Website

COBIT is Business Oriented

COBIT:

- Business-focused
- Process-oriented
- Controls-based
- Measurement-driven



Source: COBIT 4.1

Risks of Not Including COBIT

- Misaligned IT services
- Excessive IT cost & overhead
- Unsuccessful IT system implementation
- Dissatisfied IT customers
- Regulatory breaches (SOX, HIPAA, PCI)
- Liability on directors and officers
- Fraud
- Weak enterprise architecture for IT
- Changes in business or IT processes may impact controls

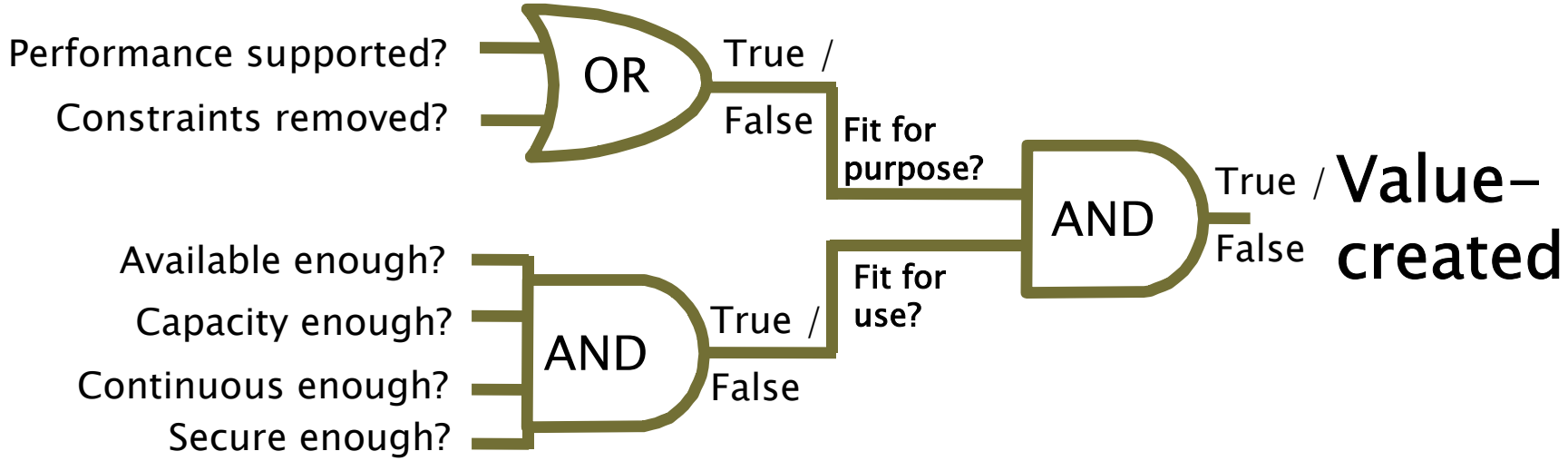
Reference: Mapping ITIL V3 and COBIT IT Governance Institute

The Total CONTROL Package

Core ITIL V3® Concepts:
Services and Value

SERVICE: *A means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs and risks.*

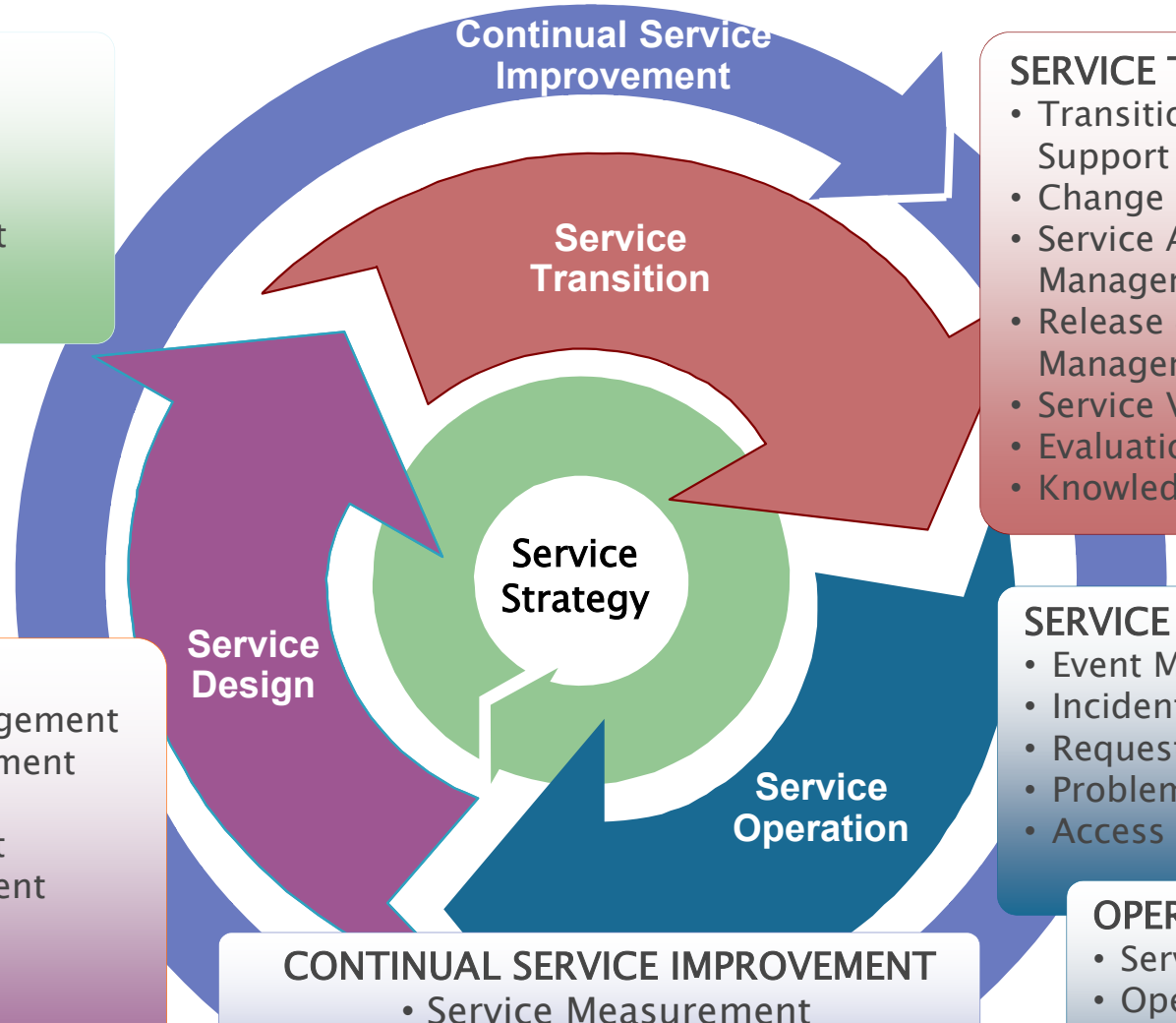
UTILITY – increases business performance



WARRANTY – reduces performance variation

Source: ITIL V3® Service Strategy

ITIL V3® Lifecycle Framework



SERVICE STRATEGY
- Service Strategy
- Service Portfolio Management
- Financial Management
- Demand Management

SERVICE TRANSITION
- Transition Planning and Support
- Change Management
- Service Asset & Configuration Management
- Release & Deployment Management
- Service Validation
- Evaluation
- Knowledge Management

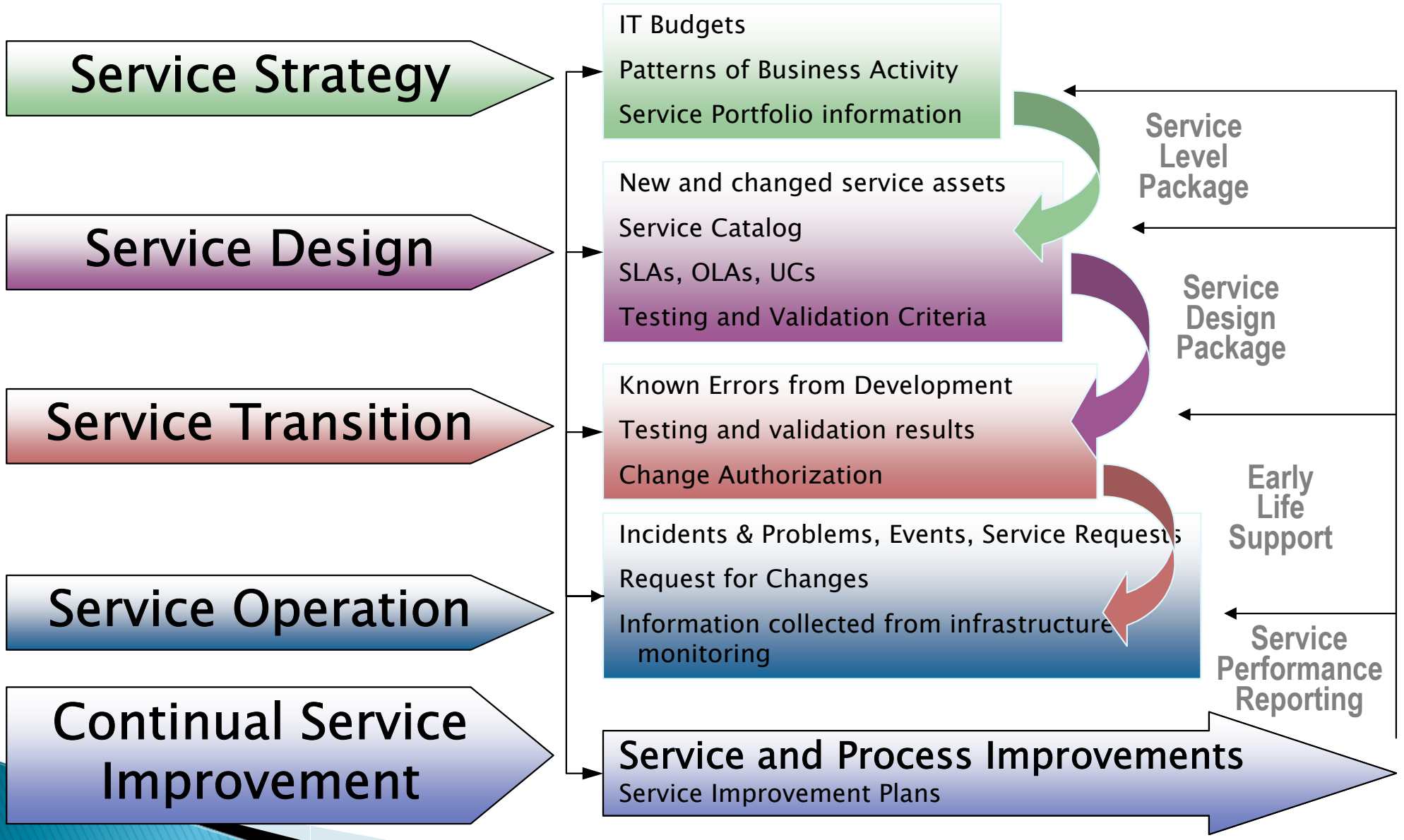
SERVICE DESIGN
- Service Catalog Management
- Service Level Management
- Supplier Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management

SERVICE OPERATION
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

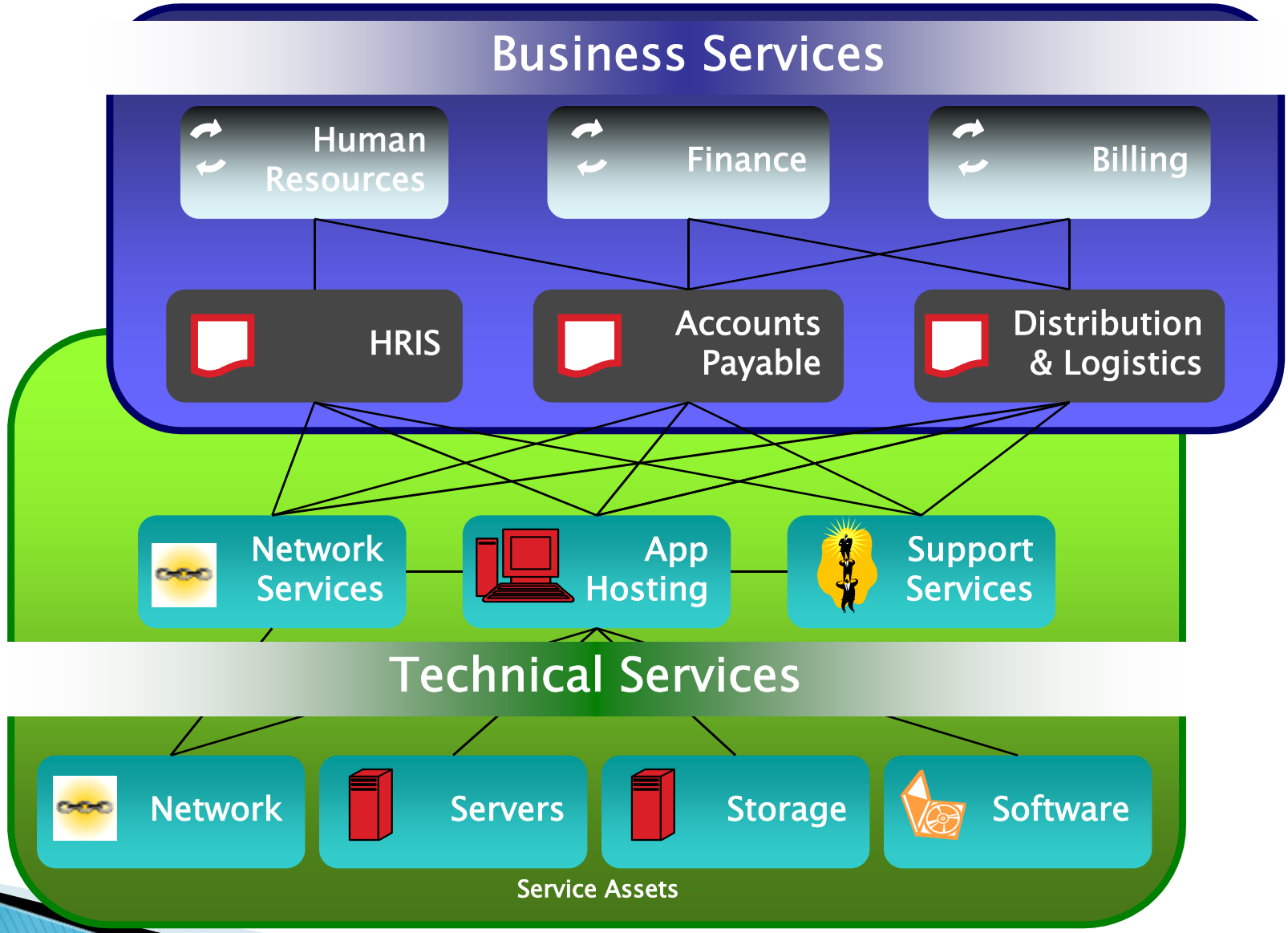
CONTINUAL SERVICE IMPROVEMENT
- Service Measurement
- Service Reporting
- Service Improvement

OPERATION FUNCTIONS
- Service Desk
- Operations Management
- Technical Management
- Applications Management

Service Lifecycle in Action

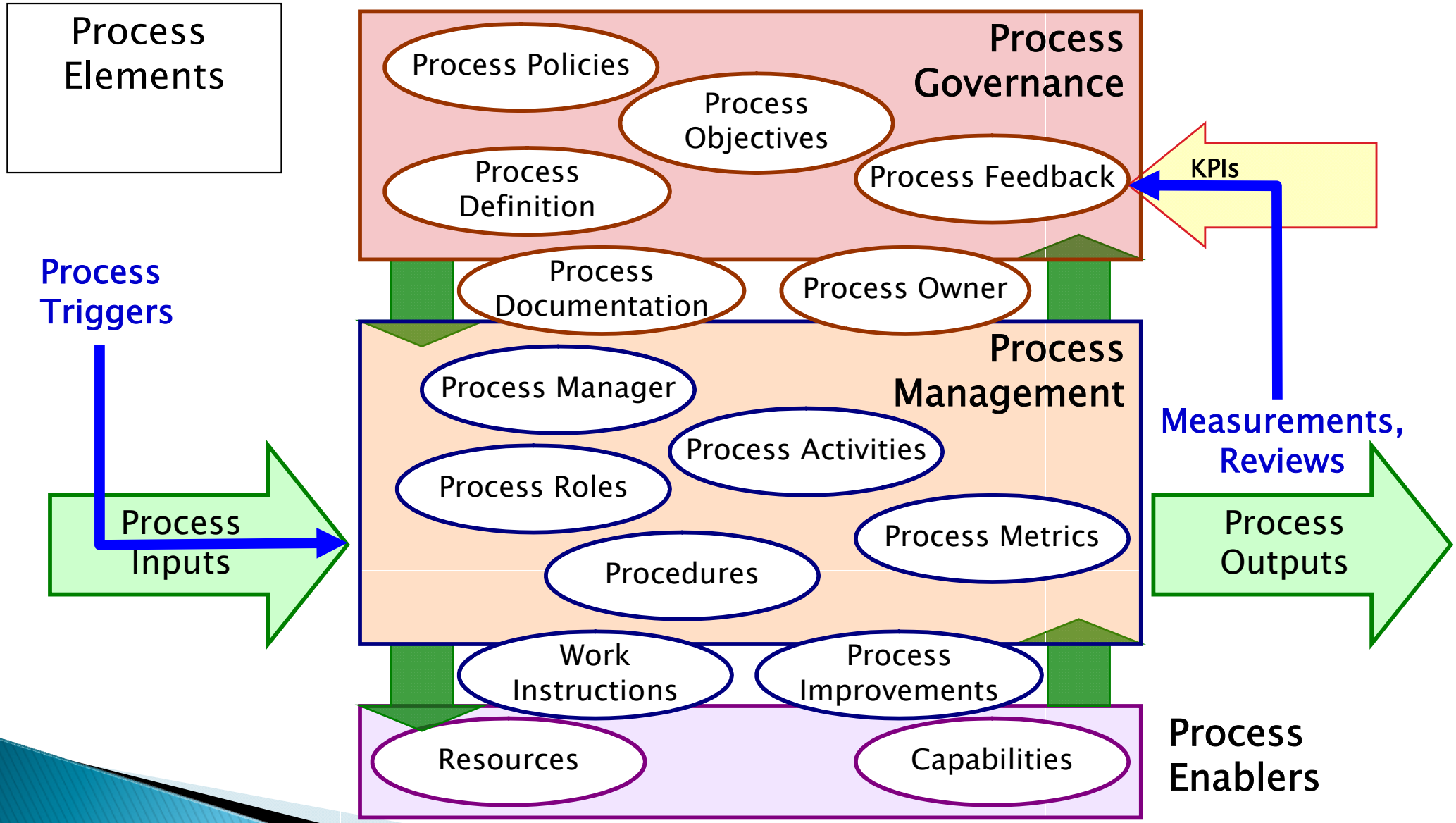


Business and Technical Services (example)

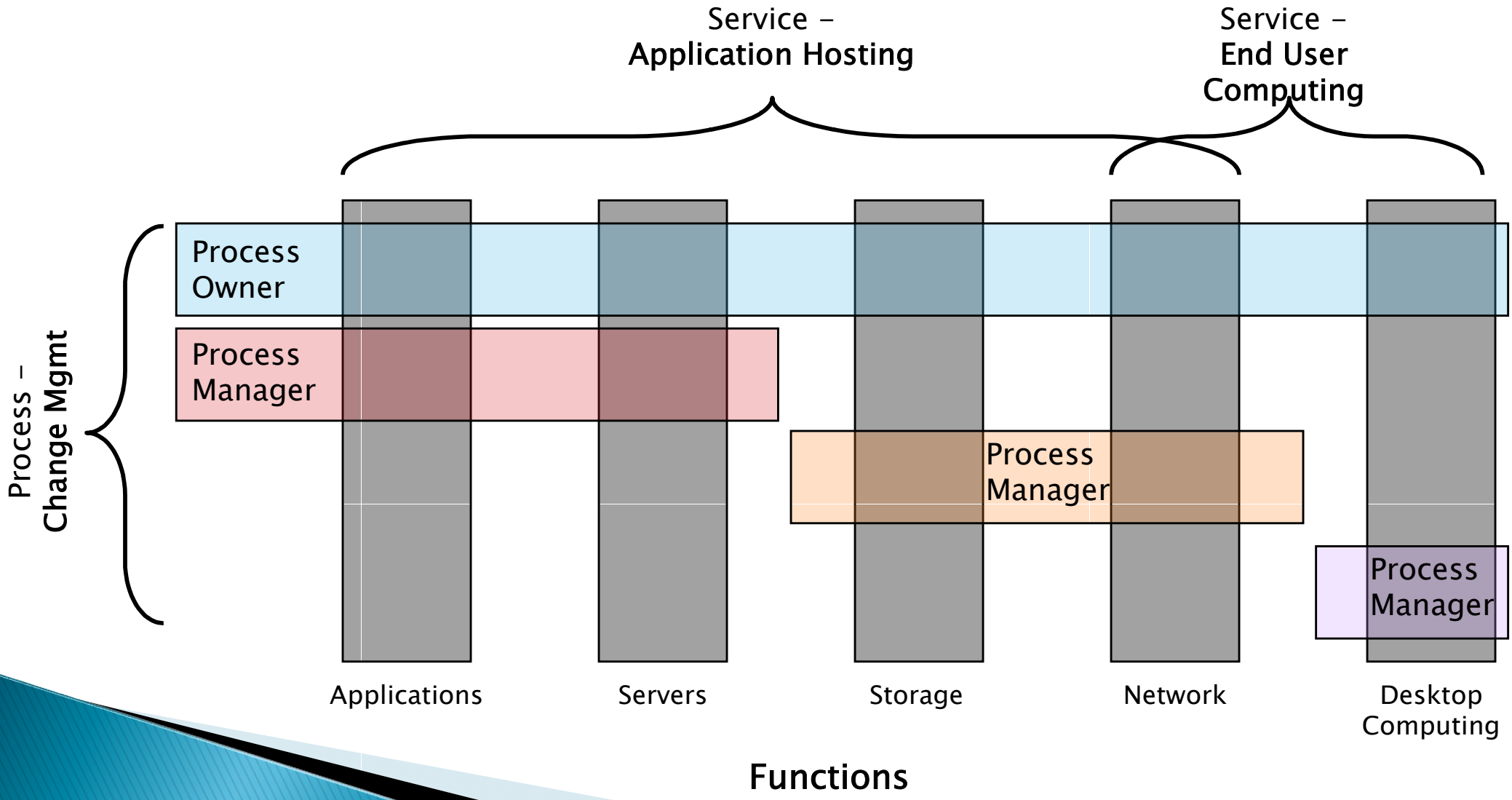


Reference: ITIL V3® Service Design

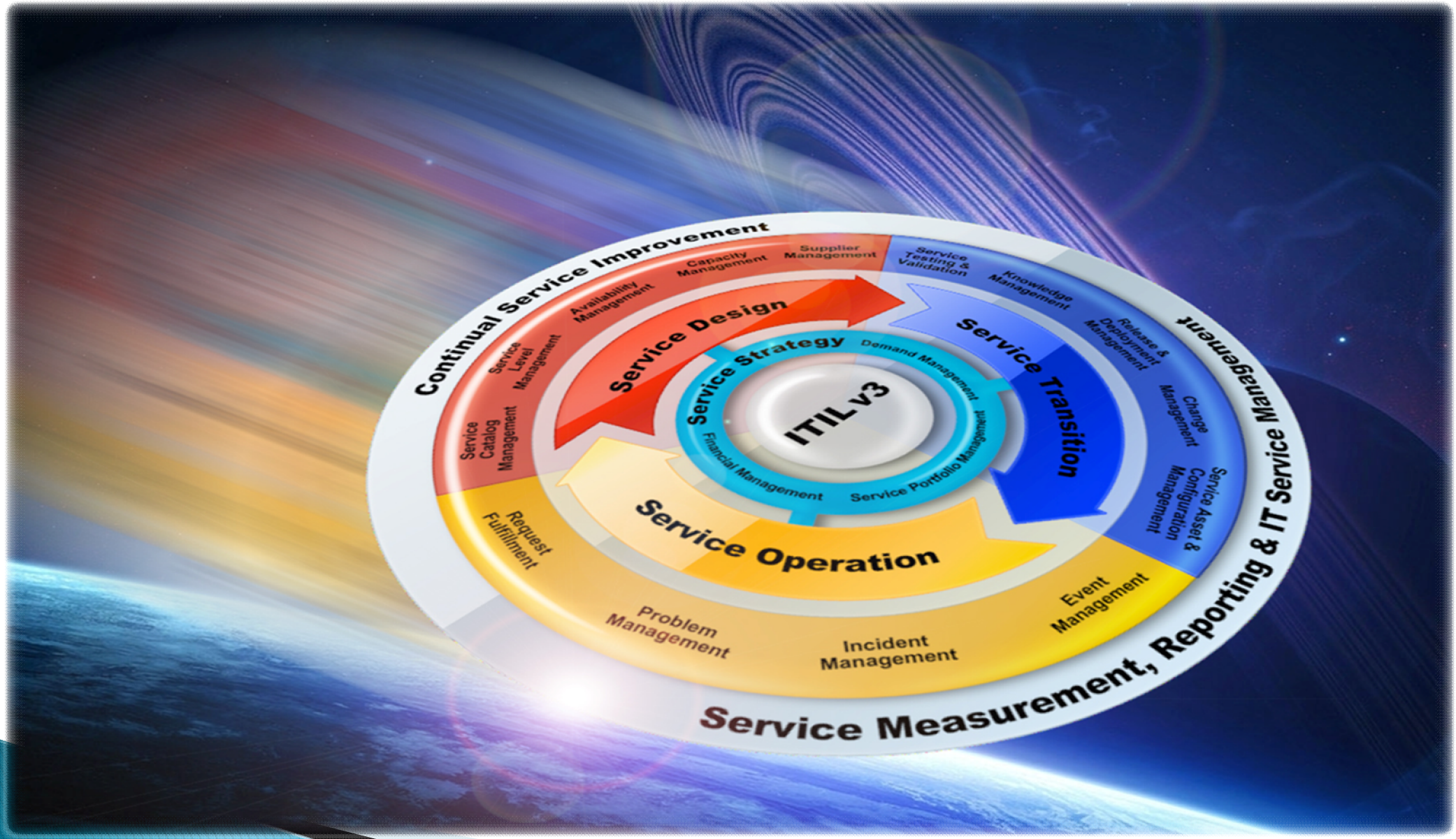
The Process Model – Governance



Services, Processes, Roles and Functions (EXAMPLE)



ITSM and Cloud Computing



The Total CONTROL Package

ISO/IEC 20000 Requirements

ISO 20000 Certification

"DO WE SAY WHAT WE DO?"

"DO WE DO WHAT WE SAY?"

"HAVE WE EFFECTIVELY IMPLEMENTED ITIL V3?"

There are two basic requirements for ISO 20000 Certification:

1. **Prove that your documented Service Management architecture complies with the ISO 20000 specifications - "Do you say what you do?"**
2. **Prove that your Behavior matches your Documentation – "Do you do what you say?"**

The most effective way of meeting Requirement 1 is an implementation of those portions of ITIL V3 that align with the ISO 20000 specifications.

Implementation of ITIL V3 as a Practice will also go a long way to ensuring that Requirement 2 will be met.

Source: Consulting Portal

ISO 20000 Demonstrates Value

- Rigor around process effectiveness/efficiency
- Enhances competitive edge
- Reduction time to market for new services
- Validates the foundation for internal controls
- A stable framework for ITSM automation
- Promotes commonality of ITSM language
- Leverages synergy with other ITSM activities
  - ISO 27001, ITIL V3, SAS 70 COBIT & Six Sigma

What's New with ISO 20000 in 2011?

DRAFT

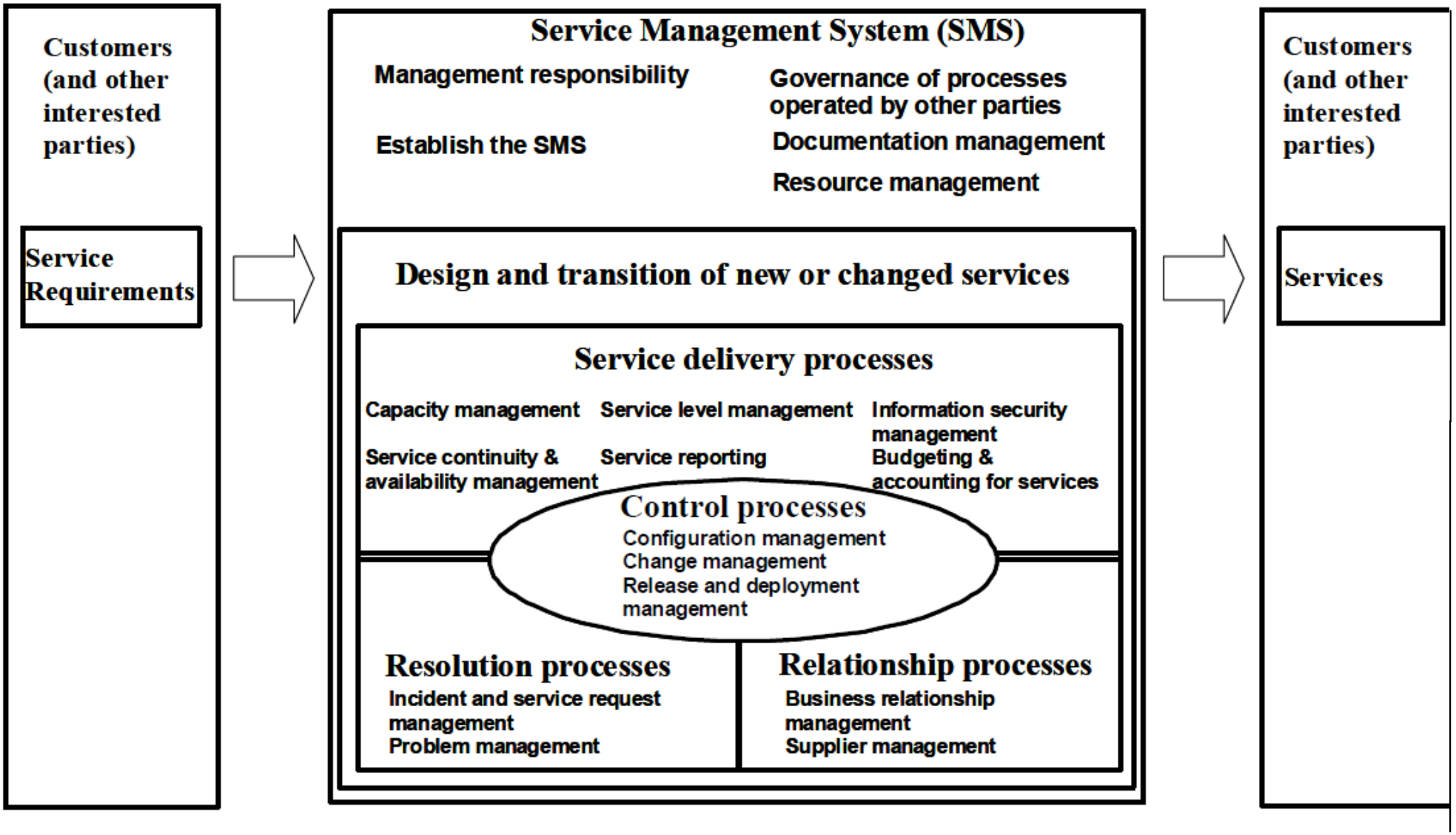


Figure 2 — Service management system

Source: Final Draft International Standard ISO/IEC FDIS 20000-1

ITIL V3 Maps to COBIT & ISO 20000
A Change Management Walkthrough

Service Manager Key Activities Based on ITIL V3	ITIL V3 Cross Reference	CobiT 4.1 Cross Reference	ISO/IEC 20000 Cross Reference	Example Deliverables
13. Change Management (*Service Transition* 4.2) (*cont.*)				
CM2. As a CAB or emergency CAB (eCAB) member, assist with impact, risk and financial assessment, prioritisation and approval of changes.	4.2.6.4 Assess and evaluate change requests	AI6.2 *Impact assessment, prioritisation and authorisation*	9.2 *	• Change schedule • Change windows • Resource plan
CM3. Participate as a CAB member in the appro[illegible] changes. Some changes, especially major or high[illegible]k changes, need final approval.	4.2.6.5 Authorise change	AI6.2 *Impact assessment, prioritisation and authorisation*	9.2	• Approved RFC
CM4. Verify the existence of change documentation and evaluate the effectiveness of the changes, to formally review the success of a change, the effect of the change and lessons learned. Participate in the review of changes prior to closure.	4.2.6.7 Review and close changes	AI6.5 *Change closure and documentation*	9.2	• Change review • Lessons learned • Known errors • Closed RFC
CM5. Participate as required and according to defined emergency change authorisation levels, approval of emergency change(s) and review of the change(s). Advise the service user of any associated risks and ensure that he/she accepts the change(s).	4.2.6.9 Emergency changes	AI6.3 *Emergency changes* AI6.4 *Change status tracking and reporting* AI6.5 *Change closure and documentation*	9.2	• Approved RFC • Change (build) plan, test plan, remediation plan with key milestones and corrective actions • Change reports

Source: IT Governance Institute, COBIT Users Guide for Service Managers

* Refers to Change Management Section [illegible]nced in the Final Draft of the International Standard ISO/IEC FDIS 20000-1

ISO 27001 Requirements for Management

- Systematically examine the organization's info. security risks, (i.e., threats, vulnerabilities and impacts)
- Design & implement a comprehensive info. security controls and/or risk avoidance/transfer to address unacceptable risks
- Adopt an overarching mgt. process to ensure that the info. security controls continue to meet the organization's needs

Source: Final Draft International Standard ISO/IEC FDIS 20000-1

IMPLEMENTING THE MODEL In your organization

Drivers for Customizing the Total Control Package in Your Organization

	COBIT	ITIL V3	ISO 20000	ISO 27001
Organization stock publicly traded (SOX)?	X	X		X
Does your organization host regulated or confidential data (HIPPA, PCI, etc)?	X	X		X
Internal or external service provider?			X	X
Are your competitors SSAE16, SAS70 or ISO certified?	X	X	X	X
Are IT services aligned with business needs?	X	X	X	
Is a significant % of revenue from the DOD or US Govt.?			X	X
Is your organization moving towards outsourcing some or all of your IT services?	X	X	X	X
Are critical service level targets being achieved?	X	X		
Is your organization moving towards mobile computing or cloud computing?	X	X	X	X
Are there cost reduction/avoidance initiatives planned or underway?	X	X		
Is IT continuity critical to the business?		X	X	X

IMPLEMENTING THE MODEL In your organization

Key Factors for Customizing the Total Control Package in Your Organization				
	COBIT	ITIL V3	ISO 20000	ISO 27001
Is there management alignment between business and IT?	X	X	X	X
Are there clear service and process ownership and responsibilities?	X	X		
Is there a common language and understanding among all stakeholders?	X	X		
Is there a proactive or reactive culture?		X		
Is there strong management support for IT Service Management as a practice?	X	X	X	
Do we manage our services and processes by measurement?	X	X	X	
Can we predictably and successfully implement new or changed services?		X	X	

Kotter Model– Implementing Change

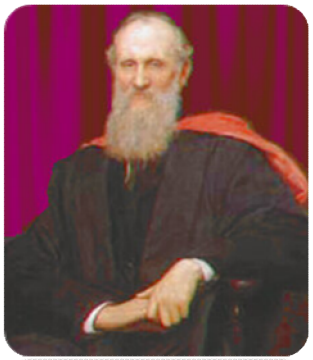
1	Creating a sense of urgency	'...50% of transformations fail in this phase.' '...without motivation, people won't help and the effort goes nowhere.' '...76% of a company's management should be convinced of the need...'
2	Forming a guiding coalition	'...underestimating the difficulties in producing Change...' '...lack of effective, strong leadership.' '...not a powerful enough guiding coalition ... opposition eventually stops the Change initiative...'
3	Creating a vision	'...without a sensible vision, a transformation effort can easily dissolve into a list of confusing, incompatible projects that can take the organization in the wrong direction, or nowhere at all...' '...an explanation of 5 minutes should obtain a reaction of "understanding" and "interest".
4	Communicating the vision	'...without credible communication, and a lot of it, the hearts and minds of the troops are never captured.' '...make use of all communications channels.' '...let managers lead by example ...' "walk the talk".'
5	'Empowering' others to act on the vision	'...structures to underpin the vision ... and removal of barriers to Change.' '...the more people involved, the better the outcome.' '...reward initiatives...'
6	Planning for and creating quick wins	'...real transformation takes time ... without quick wins, too many people give up or join the ranks of those opposing Change.' '...actively look for performance improvements and establish clear goals...' '...communicate successes.'
7	Consolidating improvements and producing more Change	'...until Changes sink deeply into the culture new approaches are fragile and subject to regression...' '...in many cases workers revert to old practice.' '...use credibility of quick wins to tackle even bigger problems.'
8	Institutionalising the Change	'...show how new approaches, behaviour and attitude have helped improve performance.' '...ensure selection and promotion criteria underpin the new approach.'

Source: ITIL V3® Continual Service Improvement

Stages of Organizational Change

Source: The Art of Stress Free IT Service Management – Art of Service

The Importance of Measurements



"If you can not measure it, you cannot improve it."

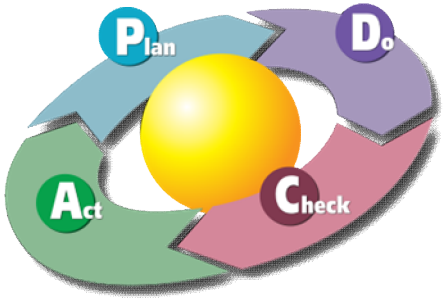
Lord Kelvin (Sir William Thompson, 1824-1907)

ITSM Processes

- Objectives (Process, Service)
- Critical Success Factors
- KPIs
- Assessments and Gap Analysis
  - Service Improvement Plans to address gaps

Audits

- Control Objectives
- Continuous monitoring of key controls
- Analytical Reviews for trends and patterns
- Audit Findings
  - Corrective Action Plans address findings and control weaknesses



Measurement is the key to the continuous improvement cycle

(Plan – Do – Check – Act)

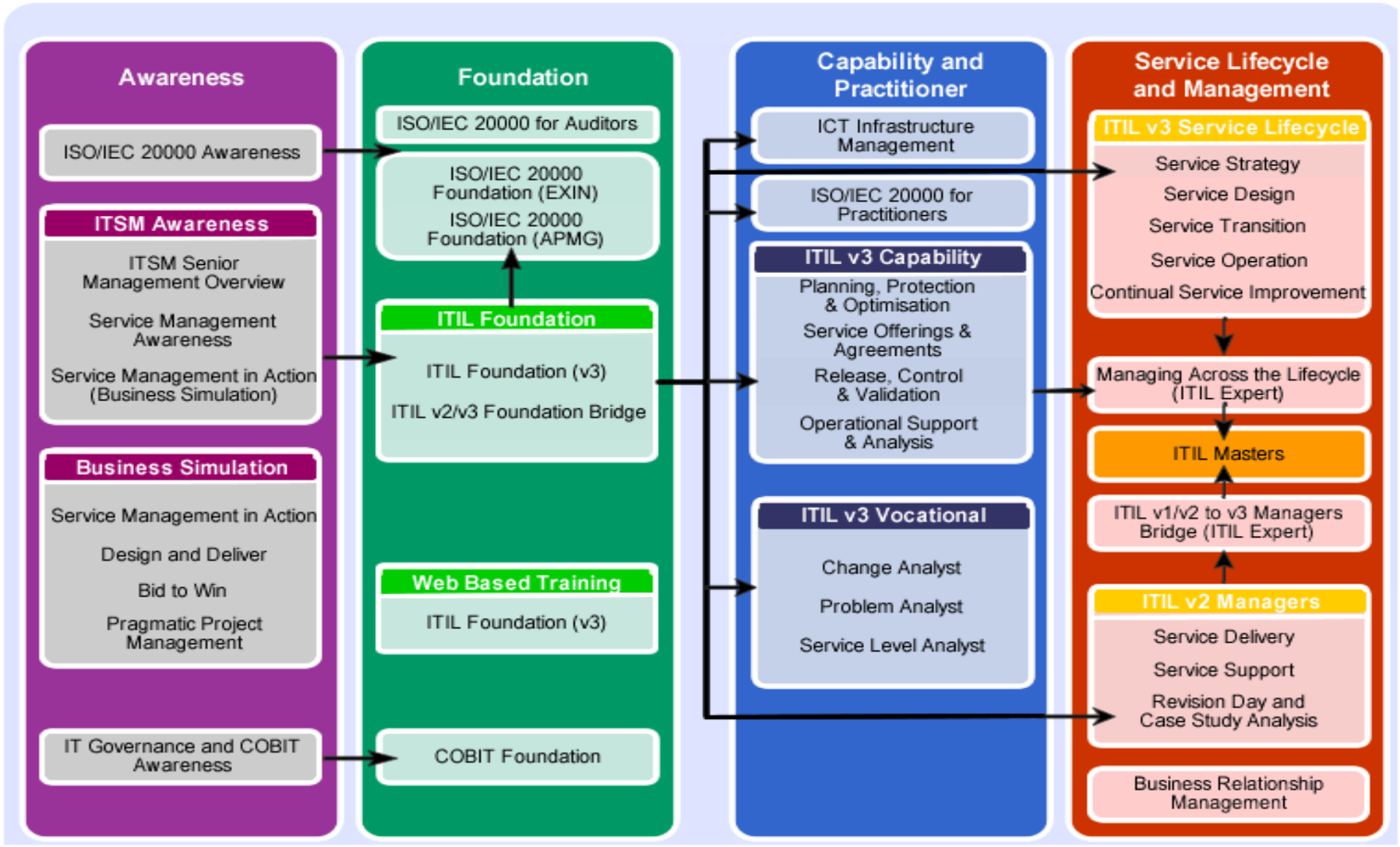
W. Edward Deming, 1900-1993

Coordination is Key to Success

Operating Model Office
ITSM Compliance Function's Vision Statement

To institutionalize compliance/control best practices into the ITSM process environment and culture while supporting/enabling ITSM adoption and expansion.

Certifications/Certifications



Source:
Fox IT Website: http://www.foxit.net/pages/education/routemap.shtml

QUESTIONS

"The Total Control Package"

APPENDIX

Why A Total Control Package?
Multiple Drivers *Require* a Multifaceted Solution

Business Drivers

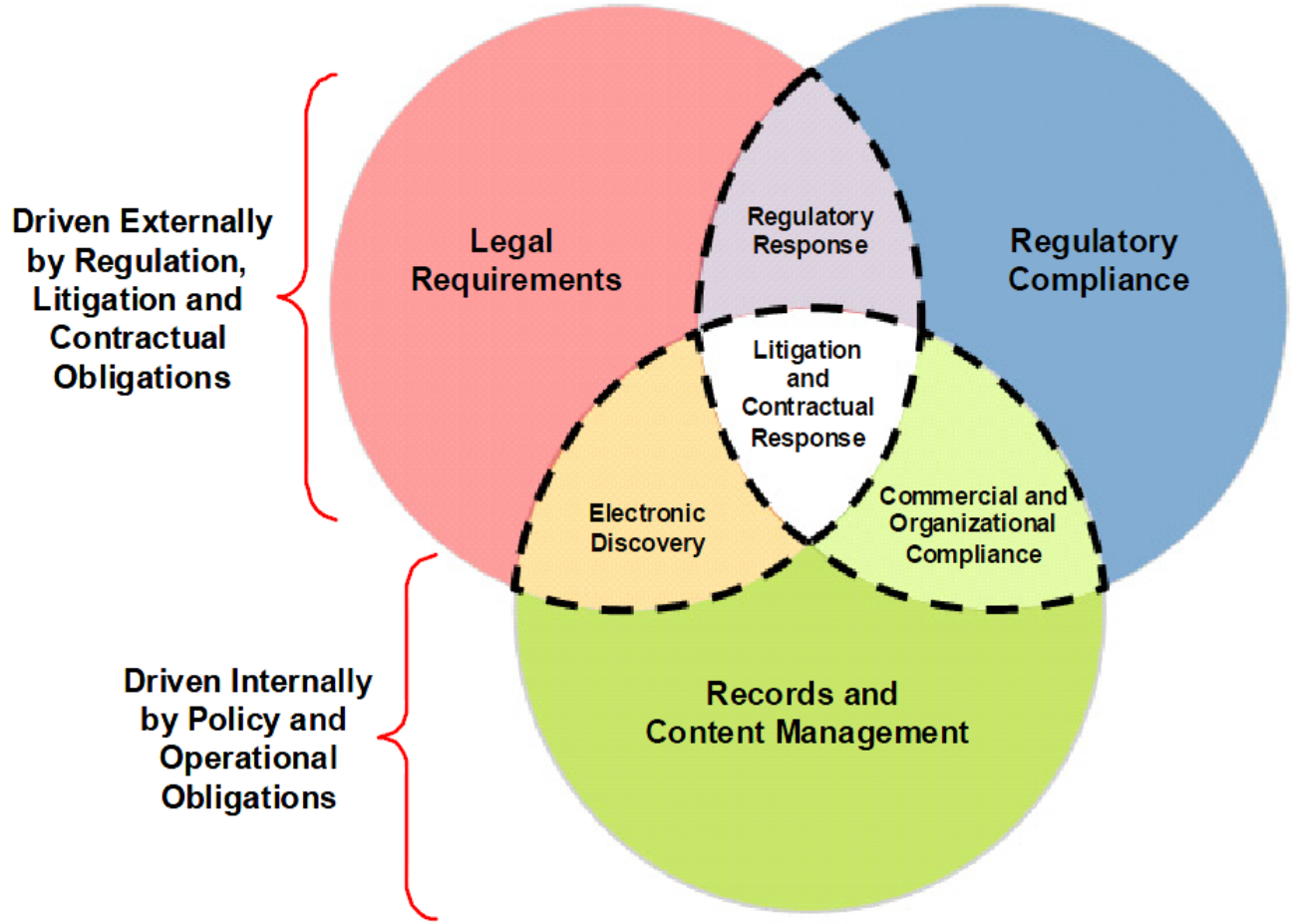
Financial
- Enhance shareholder value
- IT cost control/reduction
- Pressure to outsource IT
- Reduce auditor & consulting costs
- IT Risk Management

Business Reputation
- Manage network security threats
- Business continuity
- System Availability
- Governance and compliance
- Maintain competitive edge (ISO Certifications, SSAE 16)

IT Value
- Align IT Services with business goals
- Customer satisfaction
- Effective system implementation
- Continual Service Improvement
- Achieve SLA targets

Reference: COBIT 4.1

Regulatory Compliance Drivers



Source: Gartner (October 2009)

Gartner for IT Leaders Overview: IT Compliance, Audit and Legal Professionals
15 October 2009 ID:G00169524

Key ITSM Components

Processes

- Processes are coordinated sets of activities designed to accomplish a specific objective.
- Attributes of processes include:
  - Measurable
  - Specific Results
  - Customers
  - Respond to Specific Events

Functions

- Functions are organizational units specialized to carry out one or more processes or activities and are responsible for specific outcomes.

ISO 20000 Organizational Certification (Ex. Methodology Approach & Roadmap)

Planning/ Pre-Assessment

- Business Justification
- Executive approval
- Executive endorsement
- Awareness of cert. initiative
- Project Team & Organization
- Identify goals & initial scope
- Develop project metrics
- How certifiable are we?
- Go/No go Decision
- Consultant Required?
- Initial gap analysis
- Go/No Go Decision
- Gap remediation
- Select Certification Body
- Develop plan & charter
- Project Plan Sign Off
- Communicate to stakeholders

Audit and Remediation

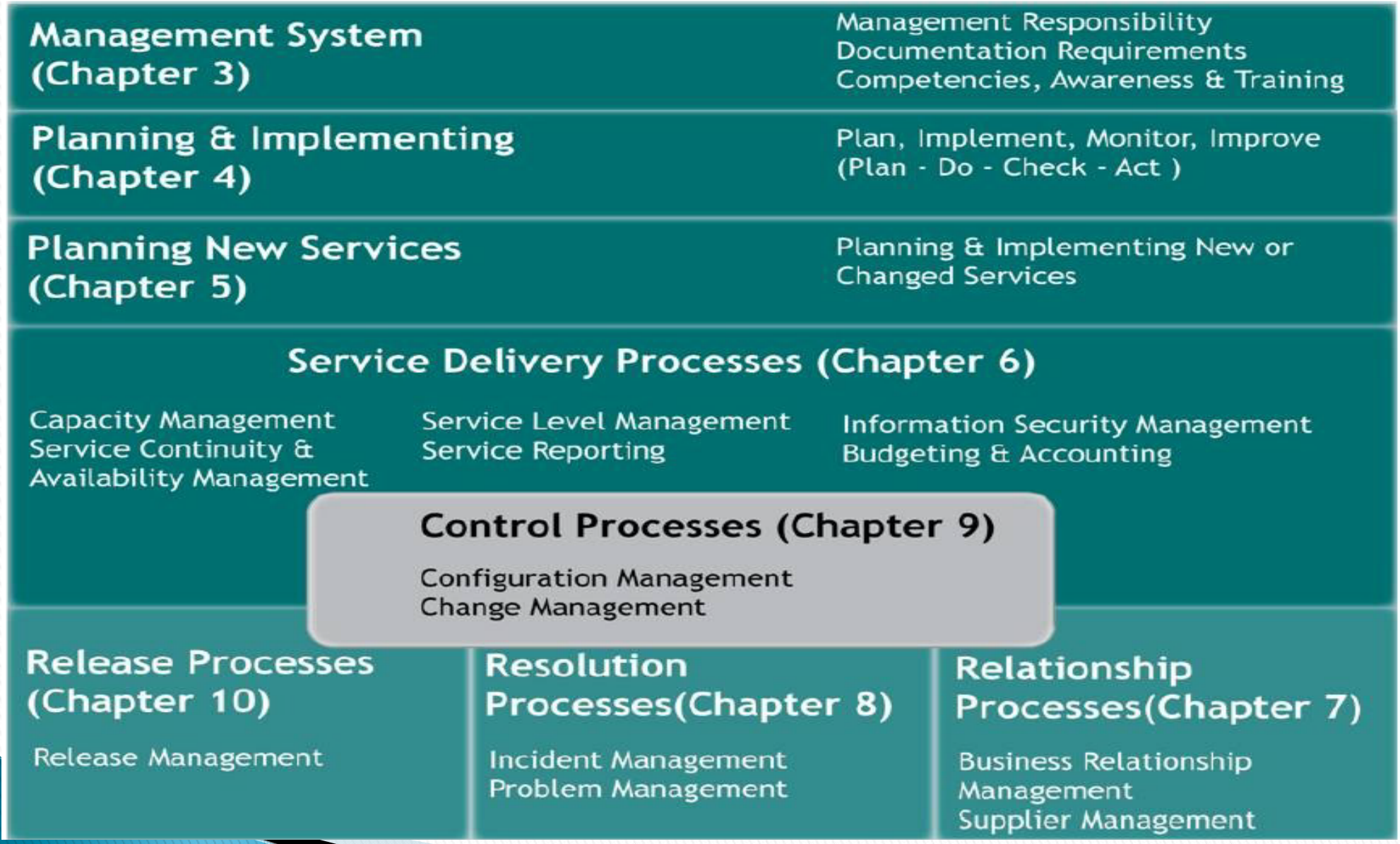
- Develop OLAs as necessary
- Start periodic status reporting
- Finalize scope
- Map mgt. system to the standards
- Revise justification as needed
- Develop "quick win" opportunities
- Go/No go Decision
- Develop service improvement plan based on mapping
- Close all remediation plan items
- Develop a service improvement plan including "quick wins"
- Initial audit
- Remediation Planning
- Go/No go Decision
- Close gaps from initial audit
- Certification audit preparation
- Certification Audit

Certification and Maintenance

- Certification Awarded
- Communicate and market certification
- Annual surveillance audits
- Re-certification every 3 years

Reference: Implementing ISO/IEC 20000 Certification itSMF International The Service Management Forum

ISO 20000 Prior to 2011 Revision

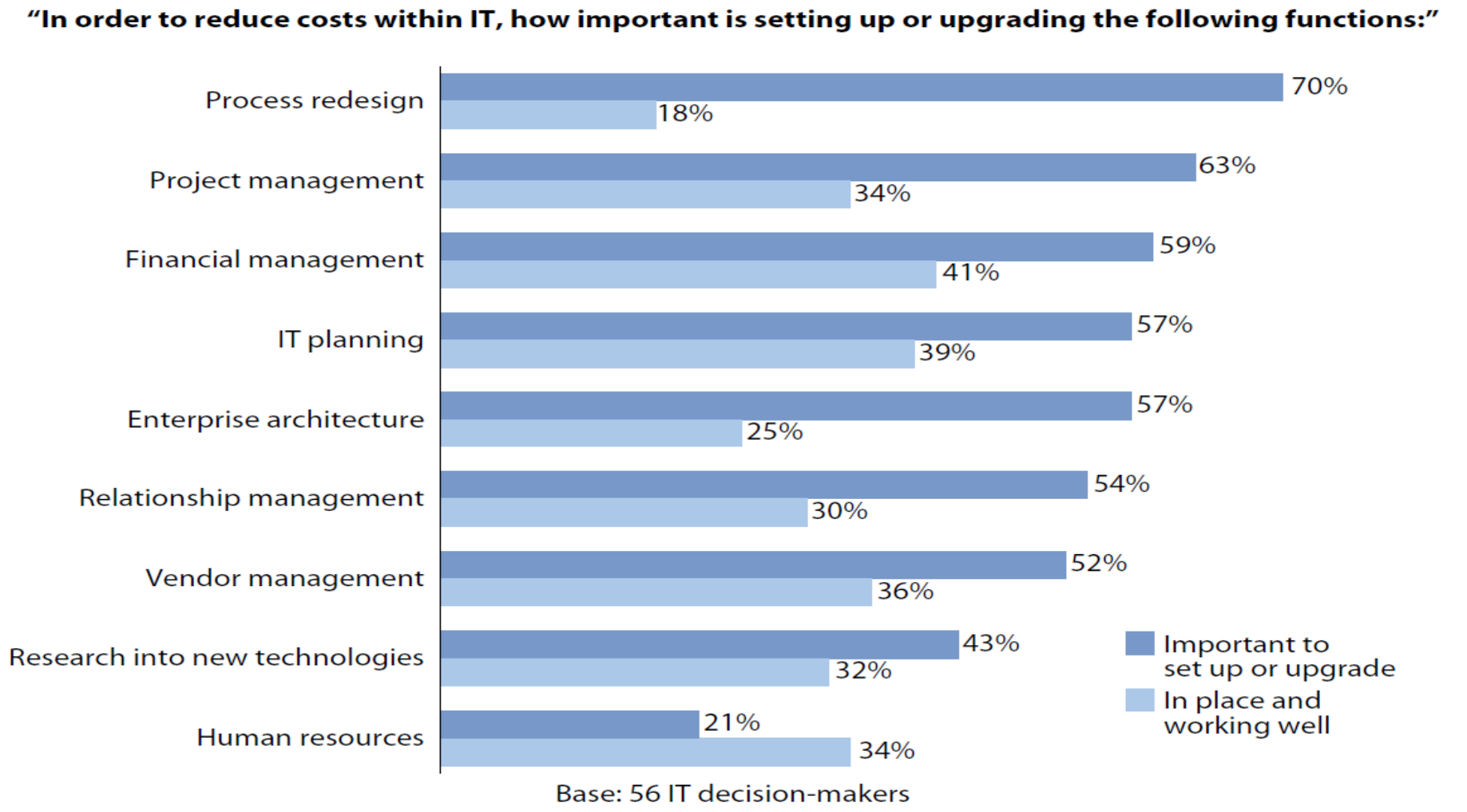


Major Revisions to ISO 20000 in 2011

- Closer alignment to ITIL V3
- Closer alignment to ISO 27001
- Introducing the term Service Management System
- Clarification of governance over 3rd party providers
- Scope clarification of SMS & how PDCA relates to SMS
- New requirements for the design and transition of new/changed services

Source: Final Draft International Standard ISO/IEC FDIS 20000-1

Cost Reductions Could Impact The Control Structure?



Source: July 2009 Global IT Cost Reduction Online Survey

56627

Source: Forrester Research, Inc.

REFERENCES AND RESOURCES

- http://www.itil-officialsite.com/home/home.aspx
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-5-Exposure-Draft.aspx
- http://www.isaca.org
- http://www.isaca.org/Search/Pages/DefaultResults.aspx?k=Mapping%20COBIT%20to%20ITIL%20V3&s=Site Content&start1=0&ct=Site&cs=Research-Deliverables
- http://20000.fwtk.org/
- http://www.iso.org/iso/home.html
- http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Documents/jpdf094-implementing-the-ISOIEC.pdf