

“By design, not afterthought!”

- A case study in embedding Security
& Compliance into IT Services

Michael J. Robinson

Sr. Director - Service Management,
McKesson Corporation

Core Competencies – C32



About the Speaker

Michael Robinson

Senior Director, Service Management, McKesson Corporation

- Michael brings over 18 years experience leading the development and delivery of innovative service offerings that produce tangible business results.
- McKesson Corporation
 - Currently ranked 14th on the FORTUNE 500, is a healthcare services and information technology company dedicated to making the business of healthcare run better.
 - We partner with payers, hospitals, physician offices, pharmacies, pharmaceutical companies and others across the spectrum of care to build healthier organizations that deliver better care to patients in every setting.
 - McKesson helps its customers improve their financial, operational, and clinical performance with solutions that include pharmaceutical and medical-surgical supply management, healthcare information technology, and business and clinical services.
- At McKesson, Michael's focus is on linking the Account Management, Product Management, Enterprise Architecture functions to the delivery of value to McKesson IT's customers
- Prior to joining McKesson, Michael was VP Professional Services for Third Sky, a Service Management consultancy.
- Michael's Service Management certifications include:
 - Certified ITIL® v3 Service Management Expert
 - ITIL® v3 Intermediate: Release, Control, and Validation
 - ITIL® v3 Intermediate: Service Offerings and Agreements
 - ITIL® v2 Service Manager

ITIL is a Registered Trade Mark, and a registered community Trade Mark of the Office of Government Commerce, and is Registered in the US Patent and Trademark Office. The trade mark symbol should be inferred wherever the term "ITIL" appears in these materials.



Agenda

- ITIL, COBIT, and ISO/IEC 20000 - compare & contrast
- Leveraging ITIL and COBIT for assessments of compliance with IT controls
- McKesson IT case study:
 - Shifting customer engagement from a technology-centric to a more service-centric mode
 - Including security, risk and compliance requirements when defining internal IT services



ITIL, COBIT, AND ISO/IEC 20000

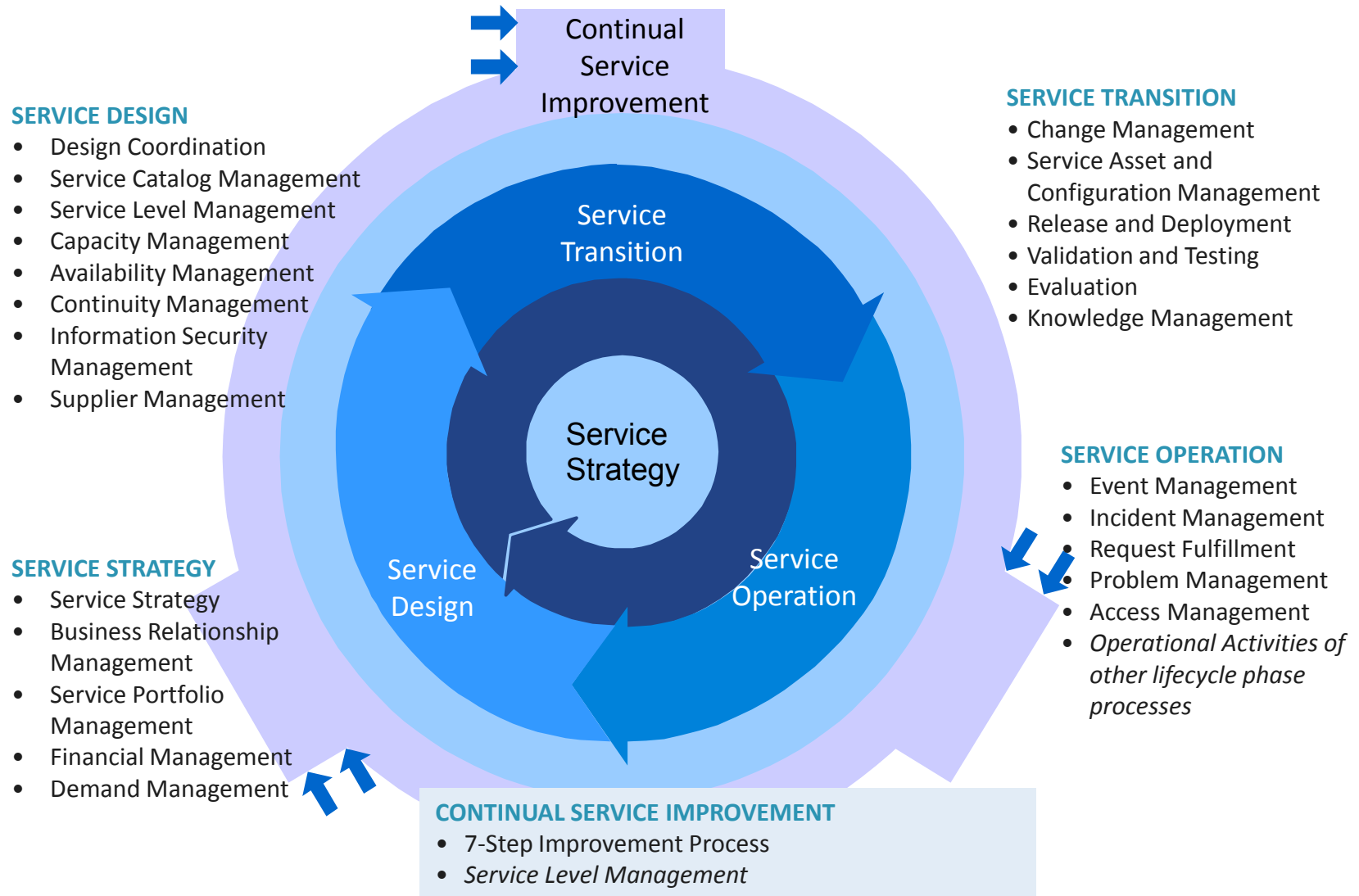
Portions of this section have been adapted from material developed with or by Third Sky, Inc.



What is ITIL®?

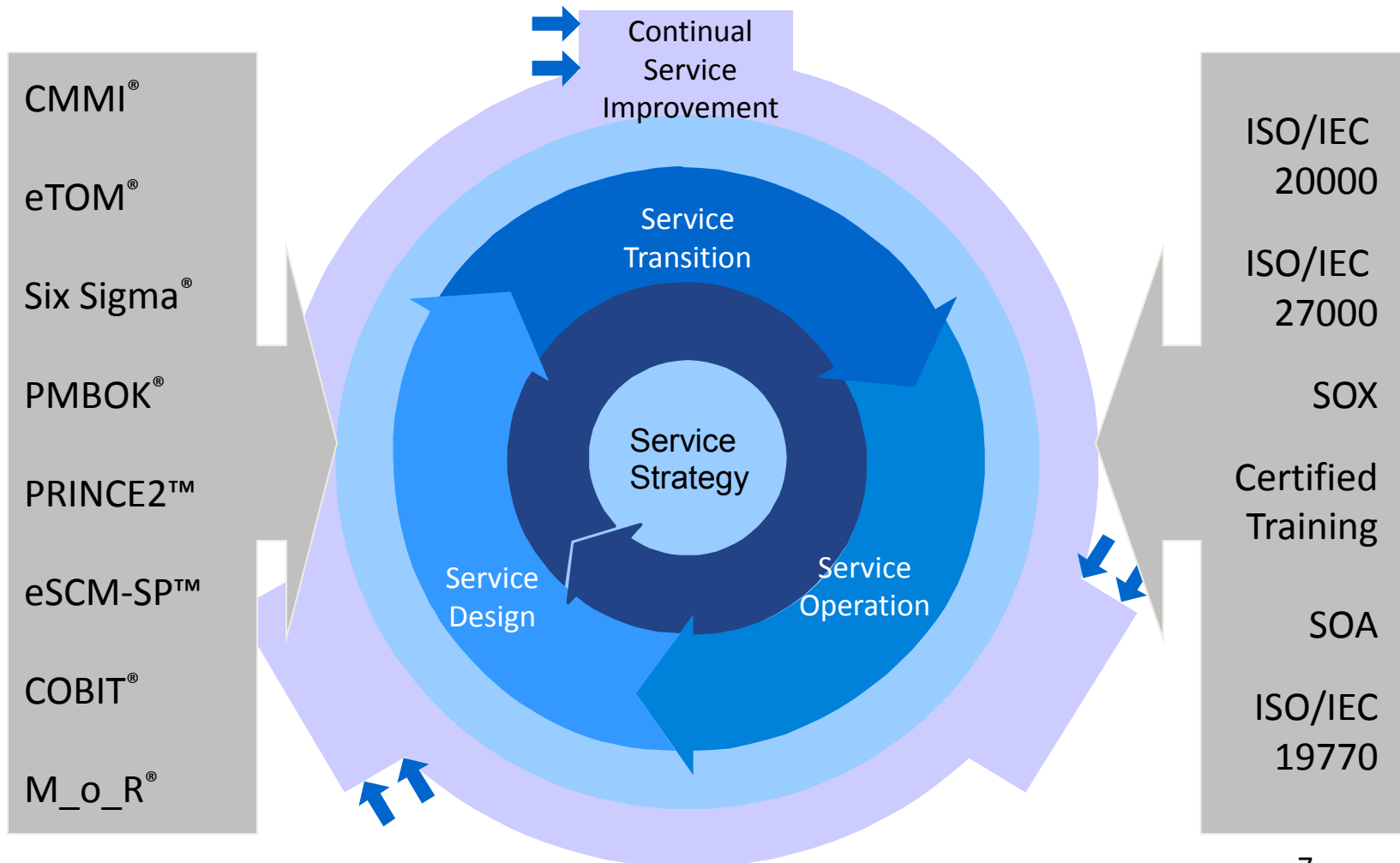
- ITIL® = Information Technology Infrastructure Library
 - A set of best practices and guidelines that define an integrated, process-based approach for managing information technology services
 - Built on good practices that were observed around the world and compiled by the British Government’s IT organization– formerly the Central Computer and Telecommunications Agency (CCTA), now the Office of Government Commerce (OGC)
- ITIL is a Framework, not a Methodology, that provides:
 - Good practice guidelines for a set of Service Management processes, and
 - A focus on the services that are delivered to the Service Provider’s customers
- Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.
- ITIL is about integrating the Service Provider with the needs of its business customers
 - Improving service quality
 - Decreasing the costs of Service delivery and support
- The current version of ITIL (“v3”) was published in 2007 and updated in August of 2011

The Core of ITIL: A Service Lifecycle

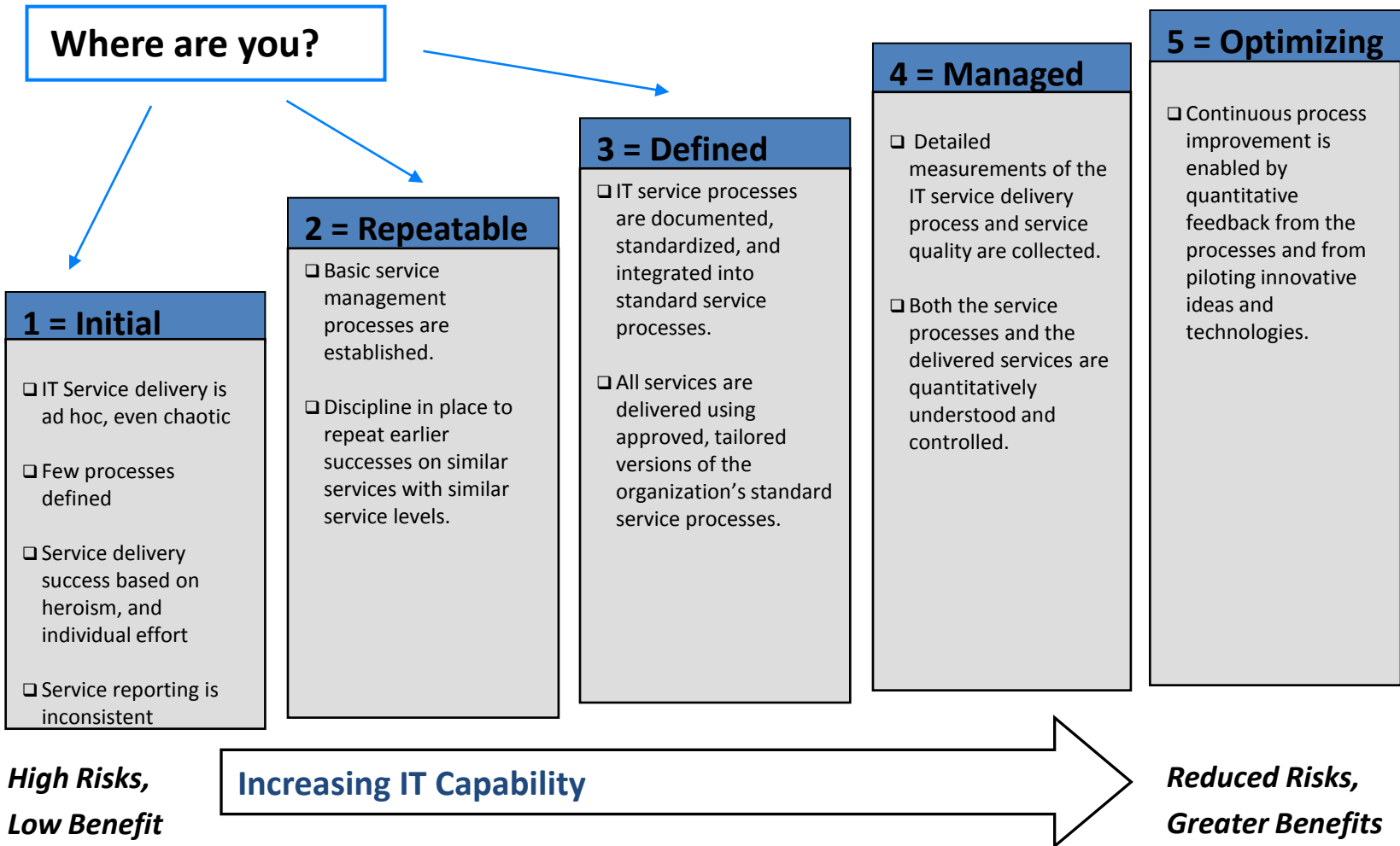


Convergence: ITIL integration with other frameworks

ITIL can be used in concert with other sources of good practice, including other frameworks and/or standards, to help organizations achieve their goals.

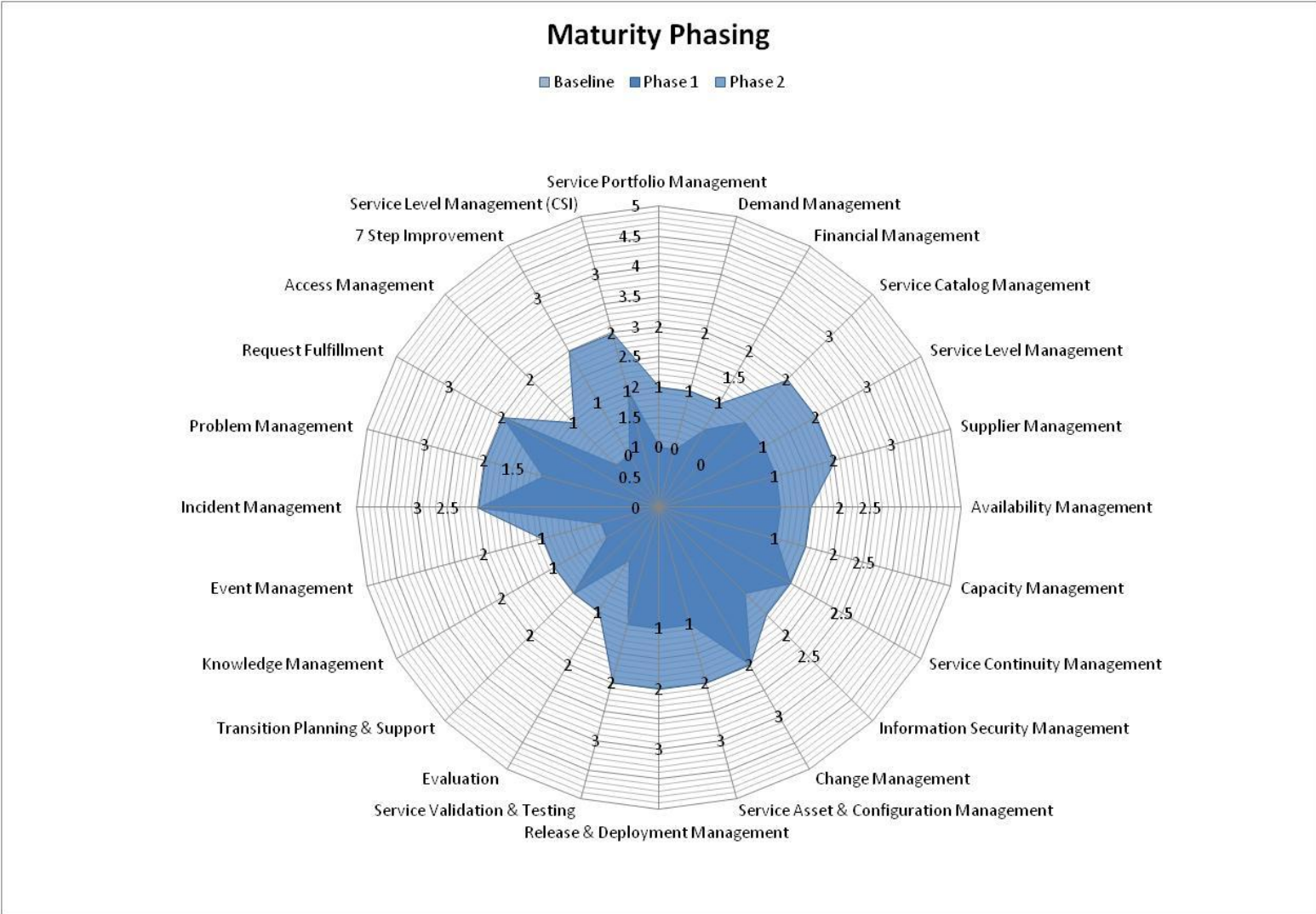


IT Service Capability Maturity Model



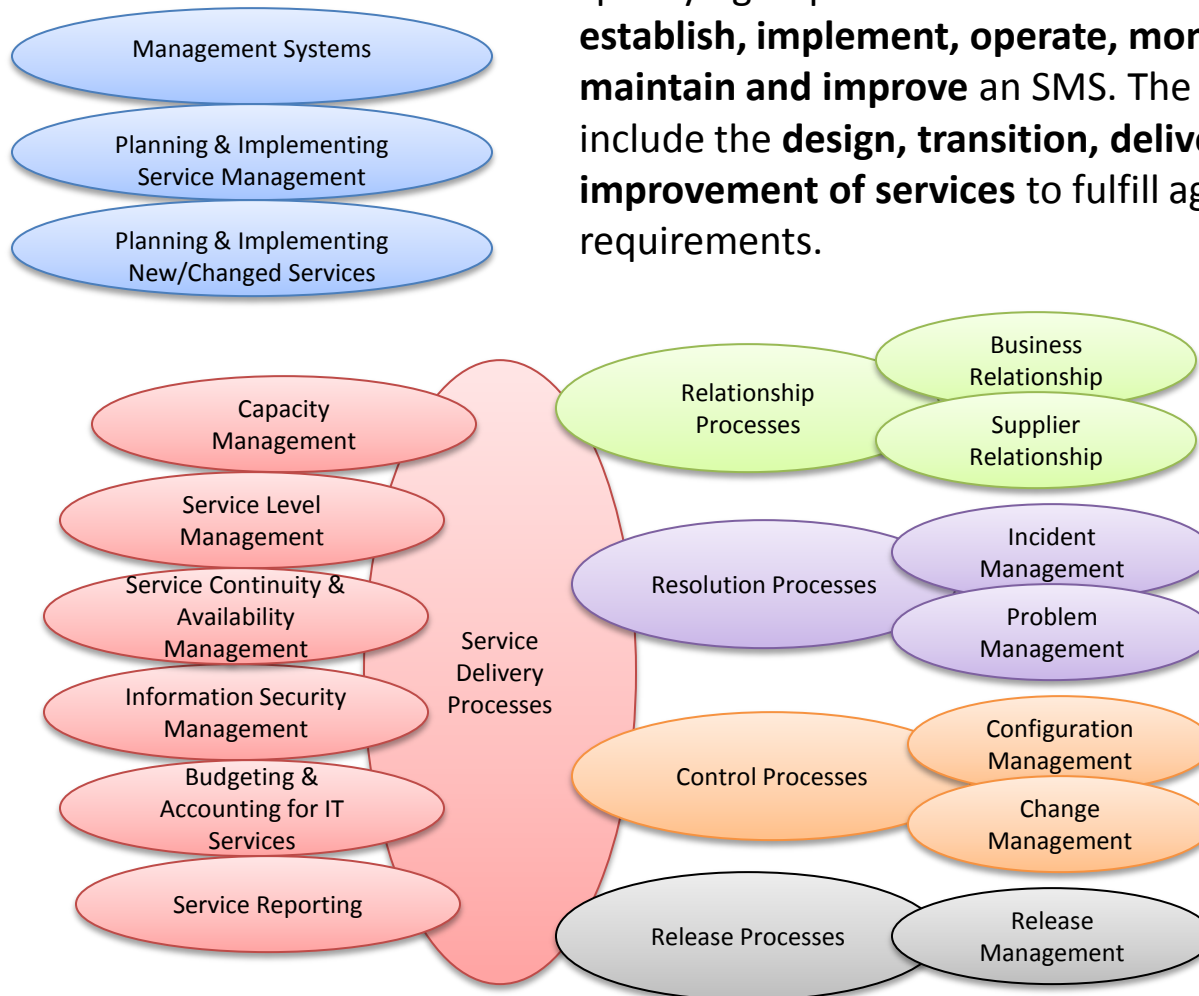
Source: Third Sky experience and "The IT Service Capability Maturity Model" by Frank Niessinka, Viktor Clerca, Ton Tjinkink, and Hans van Vlietb

Improvement Roadmaps: Examples of high-level visualization



What is ISO/IEC 20000 ?

A **standard for a service management system (SMS)**, specifying requirements for a service provider to **plan, establish, implement, operate, monitor, review, maintain and improve** an SMS. The requirements include the **design, transition, delivery and improvement of services** to fulfill agreed service requirements.



When to pursue ISO/IEC 20000 Certification?

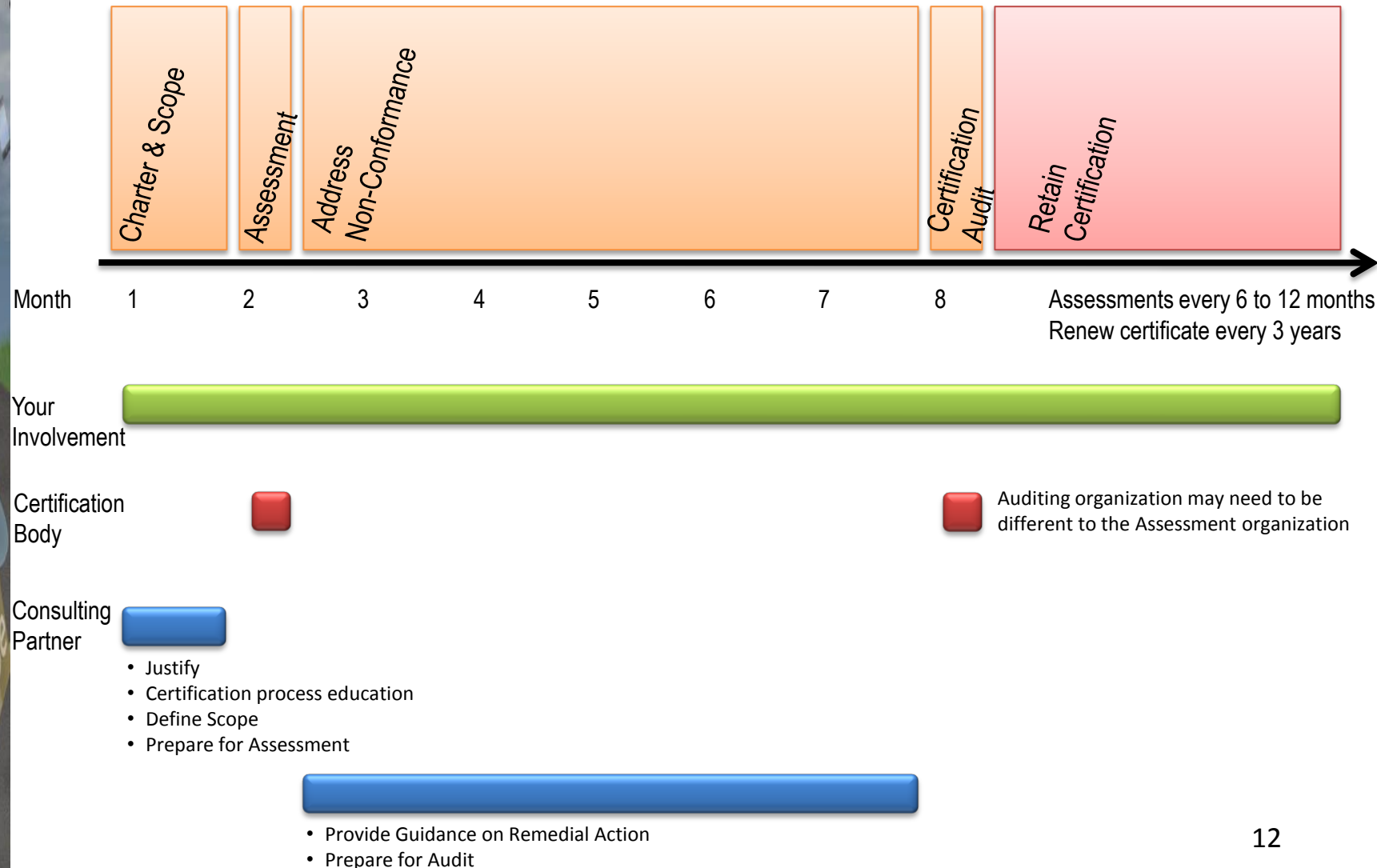
Pursue certification when there is a need to....

- Provide assurance to internal customers
- Provide competitive differentiation to external customers
- Provide assurance within your own organization (IT) that you have met a global standard, not just leveraged guidance
- Enable “apples to apples” comparison with peers

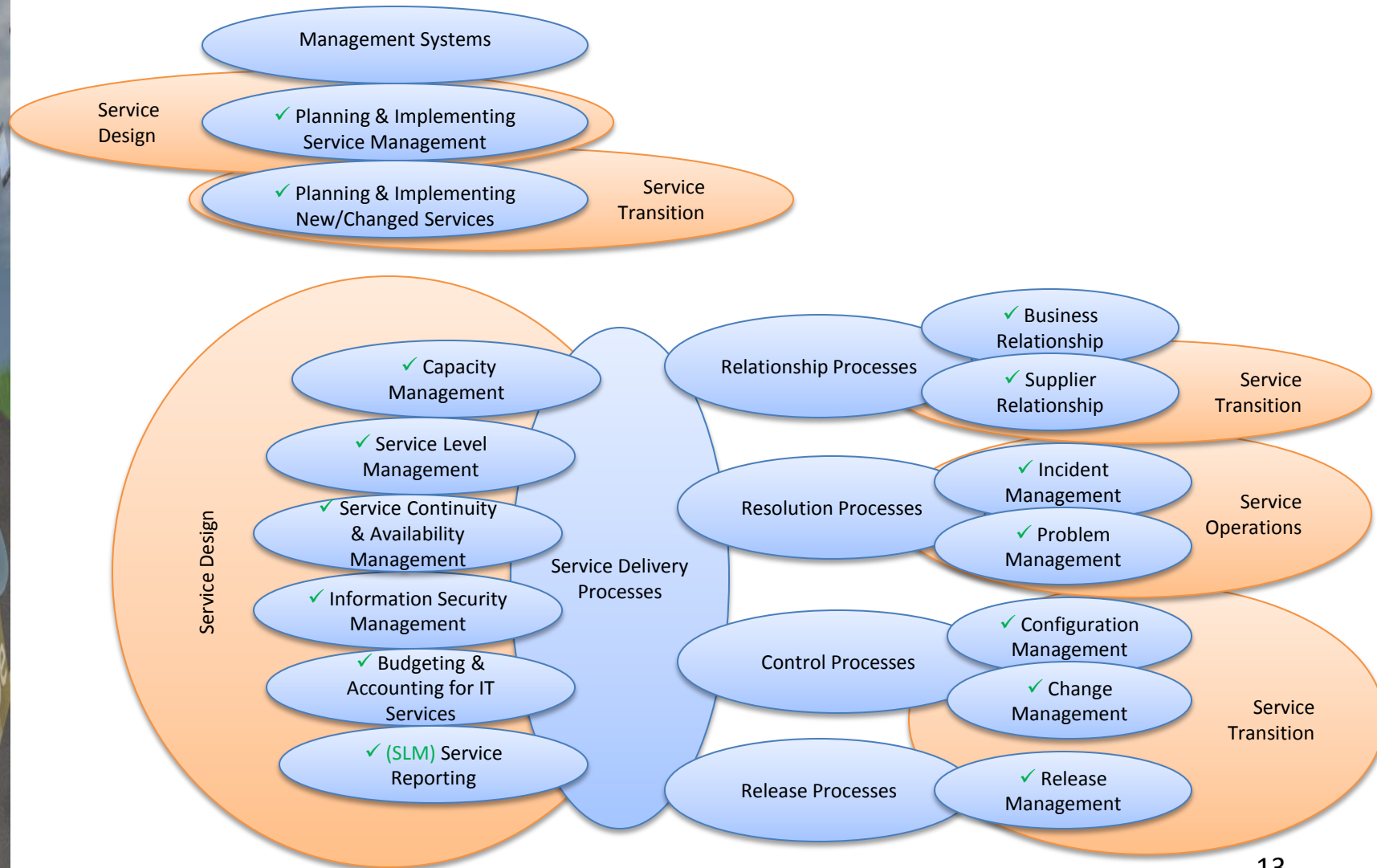
Do not pursue certification when you have....

- No need for external differentiation or internal confidence building via a “standard”
- An approach to adopt and adapt ITIL guidance over time (i.e. a roadmap of continual improvement), rather than pursuing an all-or-nothing achievement of a standard
- Budget / resource limitations

How to attain ISO/IEC 20000 Certification ?



Mapping ISO/IEC 20000 to ITIL v3



Contrasting ITIL and ISO/IEC 20000

ITIL

- Used by organizations worldwide to establish and improve capabilities in Service Management.
- Can be adopted in whole or in part, per the needs of the organization.
- Offers a body of knowledge useful for achieving the ISO/IEC 20000 standard.
- Certification is for the individuals

ISO/IEC 20000

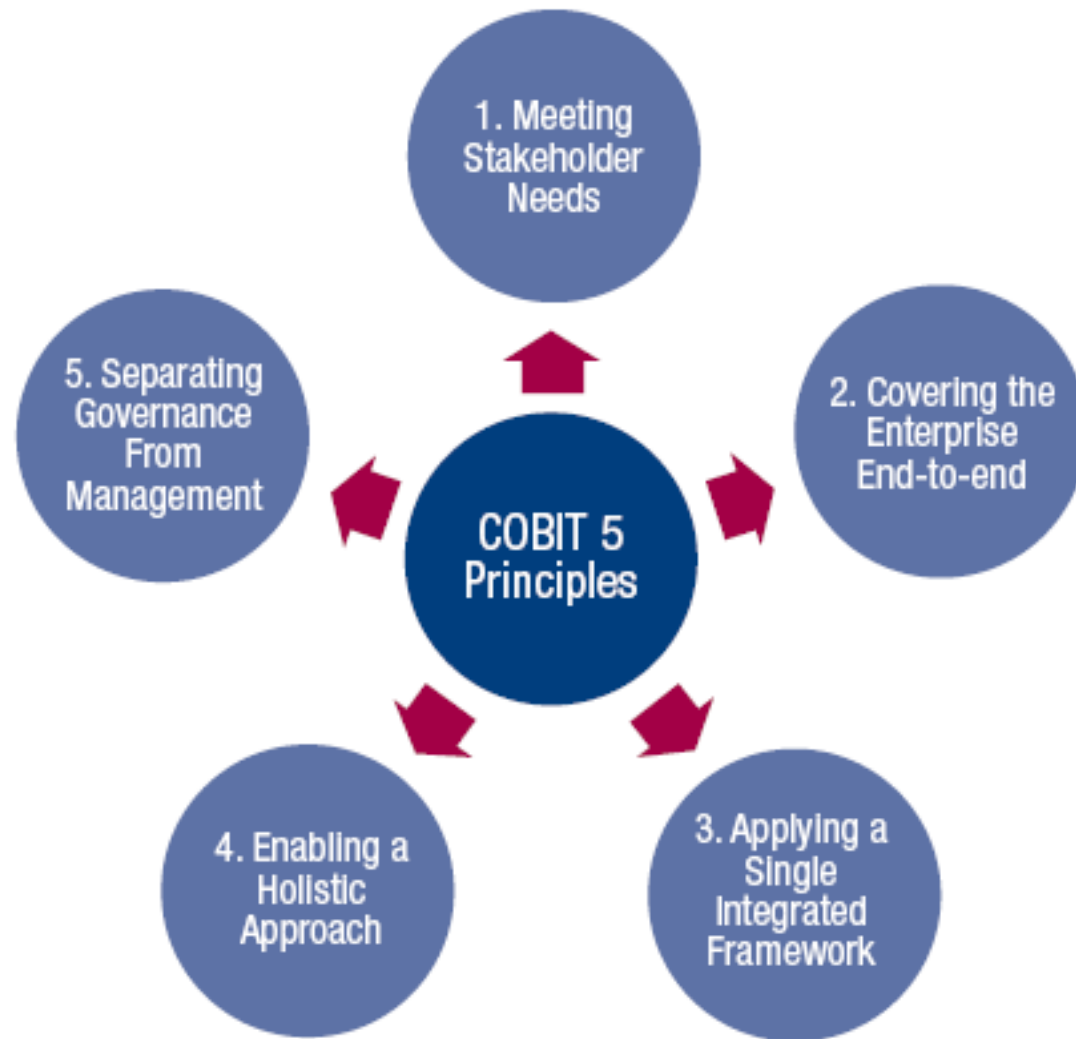
- Provides a formal and universal standard for organizations seeking to have their Service Management capabilities audited and certified.
- A standard to be achieved and maintained
- Emphasizes a formal and structured IT governance model (echoing COBIT)
- References ISO/IEC 17799 (Information Security Management) as a compliance requirement.
- Underpins ISO 9000 for IT



What is COBIT?

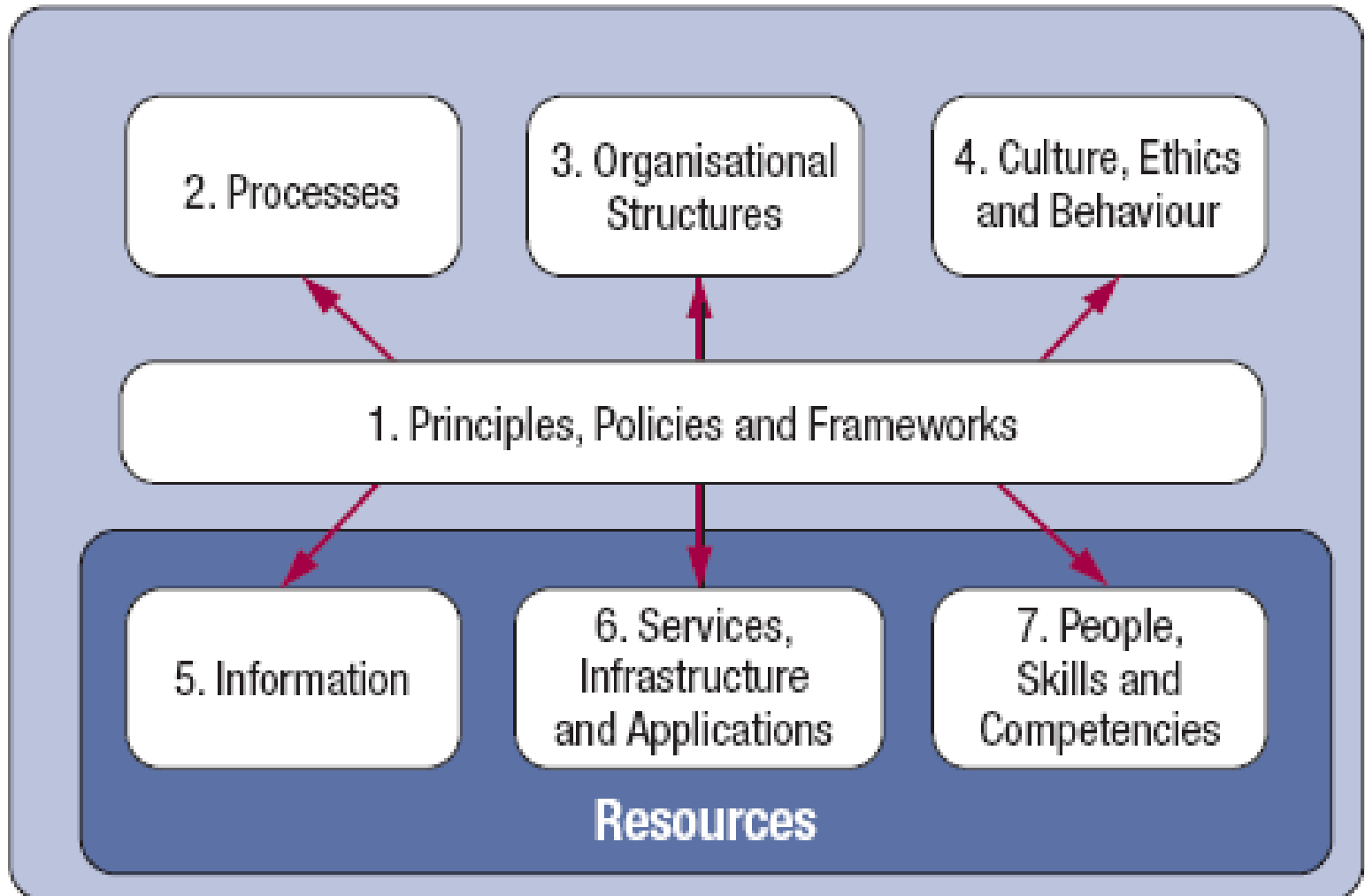
- COBIT is a business framework for the governance and management of enterprise IT.
- COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including:
 - ISACA’s Val IT and Risk IT
 - Information Technology Infrastructure Library (ITIL®)
 - Related standards from the International Organization for Standardization (ISO).
- COBIT 5 brings together:
 - Five principles that allow the enterprise to build an effective governance, and
 - Management framework based on a holistic set of seven enablers that optimizes information and technology investment and use for the benefit of stakeholders.

COBIT 5 Principles



Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 Enablers



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

Mapping COBIT to ITIL

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor



Align, Plan and Organise



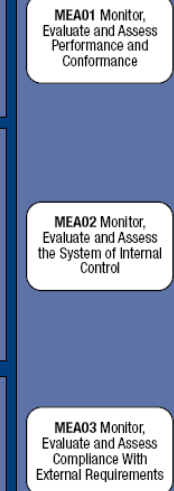
Build, Acquire and Implement



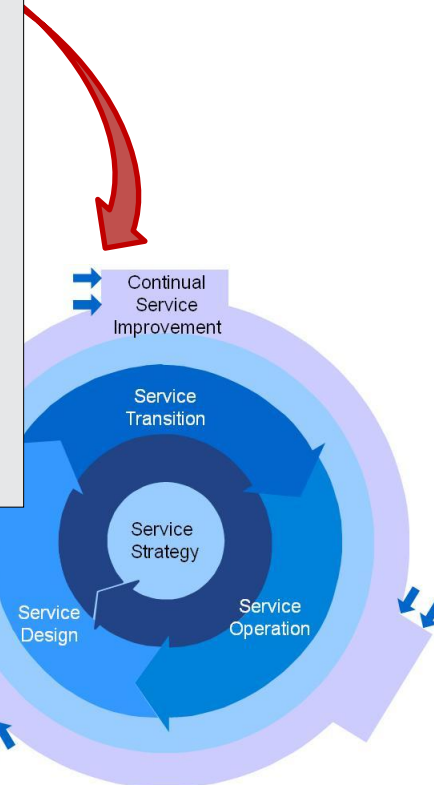
Deliver, Service and Support



Monitor, Evaluate and Assess

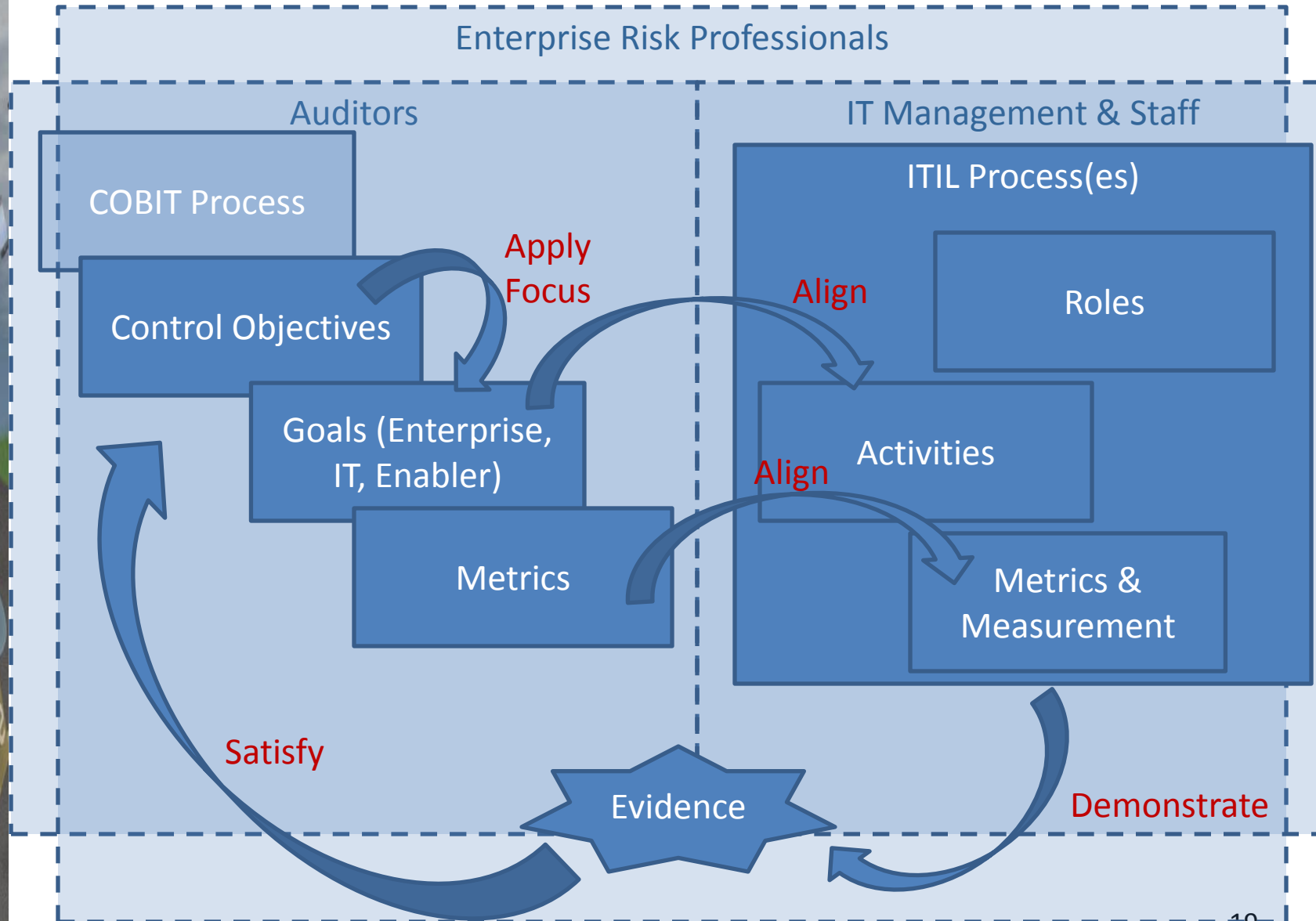


Processes for Management of Enterprise IT



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

Leveraging ITIL & COBIT



Using COBIT & ITIL with Unified Compliance Framework(s)

- Examples of compliance requirements include:
 - Regulatory requirements
 - HIPAA
 - PCI and the related PCI - Data Security Standards
 - Standards for Attestation Engagements (SSAE) No. 16, “Reporting on Controls at a Service Organization”
- The Unified Compliance Framework (UCF) is an IT compliance framework that seeks to:
 - Define the smallest possible list of controls necessary to meet all compliance requirements, and
 - Organize them for easy implementation, testing, and monitoring
- The ISO/IEC 27000 series specifies a information security management system to bring information security under explicit control, by:
 - Systematically examining the risks
 - Designing & implementing an information security strategy and coherent and comprehensive suite of information security controls and/or other forms of risk treatment
 - Adopting an overarching management process to ensure the controls continue to meet the organization’s information security needs on an ongoing basis
- Audit, Risk and Compliance professionals can use COBIT 5 to:
 - Define and publish the control framework for their Service Provider organization
 - Enable the independent evaluation of the effectiveness of those controls
- IT professionals can use ITIL to:
 - Leverage a framework for managing the continual improvement of process maturity
 - Not only advance operational objectives, but also provide evidence of IT Service Management process maturity and the meeting of control objectives



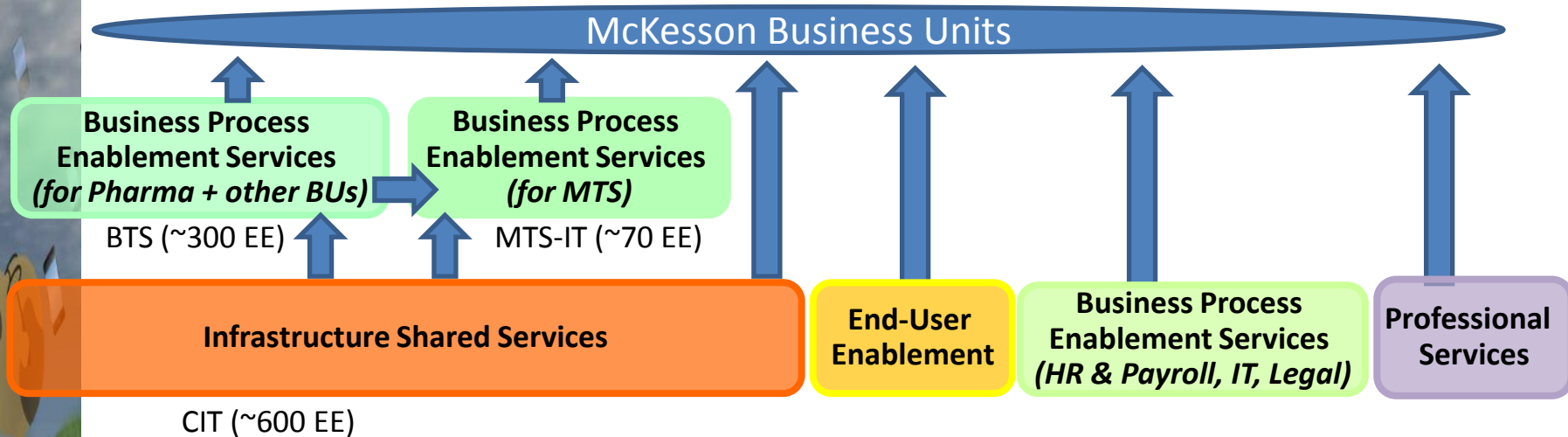
Some key COBIT Control Objectives for the Service Lifecycle

- APO05 Manage portfolio
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- EDM02 Ensure Benefits Delivery



MCKESSON IT CASE STUDY

Background: A consolidated McKesson IT Service Delivery Model



- Reduce Costs
 - Overall Reduction in Total Cost of Ownership (TCO) for Technology & Communication Services
 - Reduce duplication
- Improve Quality & Enable New Outcomes
 - Combine the application and infrastructure strengths of 3 IT organizations – building on 5 years of accomplishments and efficiencies gained separately
 - Close gaps in engagement and provide a single face to the Customer
 - Create integrated IT function that can be a more strategic Full-Service provider for its Customers

McKesson IT Integrated Business Service Portfolio

Infrastructure

Delivered (on a subscription basis) to McKesson's BU CIOs and other technology buyers to provide them with the infrastructure they need to support their own technology products and services.

Key Example:

- Hosting

End User Enablement

Delivered (on a subscription basis) to McKesson's corporate, distribution, and technology business units to help them enable their users' personal productivity across all business processes.

Key Examples:

- Voice Communications
- Mobile Communications
- Collaboration
- End User Computing

Business Process Enablement

Delivered (on a subscription basis) to McKesson's corporate, distribution, and technology Business Functions / Business Process Owners to support their business processes operations.

Key Examples:

- Sales Order Entry
- **Order Pre-Processing**
- Order Pricing & Processing
- **Regulatory Compliance Reporting**
- **Expense Management**
- **AP Processing**

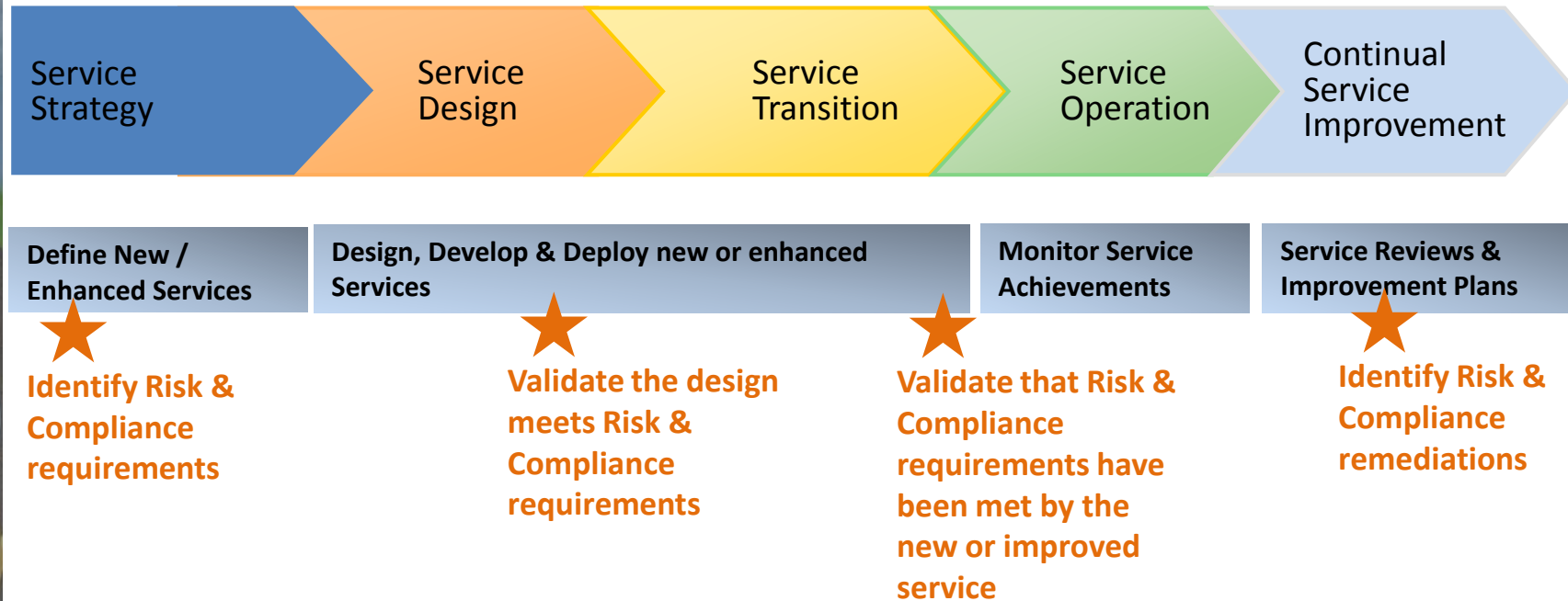
Professional Services

Delivered (on a time & materials / SOW basis) to McKesson's BU CIOs and other technology buyers to provide advisory or point-consulting services for initiatives that will not be operationally managed by McKesson IT.

Examples include:

- IT Service Continuity (Advisory)
- Information Security & Risk Management (Advisory)


Key integration points for Risk & Compliance in the Service Lifecycle



Business Services Drilldown – Key Examples

Ref #	IT Product	Brief Description	Product Package(s)
O2D5	Regulatory Compliance Reporting	<p>Regulatory Compliance enables McKesson to comply with mandates from the DEA and state agencies regarding the sale of controlled substances (Class II (CII) to Class V (CV); RXDA B, D, E, X), List 1 chemicals, and various potentially “dangerous” pharmaceuticals</p> <p>Controlled substance & license monitoring and manipulation of orders per compliance rules (including omits, thresholds) - Monitoring of DEA licenses, threshold compliance, state regulations for product orders; Includes DEA and State license validations; traceability of product origins to satisfy State regulations; includes e-Pedigree</p>	<ul style="list-style-type: none"> • Federal (incl. DEA – CSMP & ARCOS) • State (CSMP) • Pedigree
O2D1	Sales Order Entry	<p>Sales Order Entry automates the receipt of customer orders into McKesson. McKesson’s customers submit orders in numerous ways. Orders are received from multiple customer groups including: Retail/National Accounts; Hospitals/Pharmacies; Small/Independent Chains; and Other/Misc.</p> <p>* Includes item availability lookup (ordering & lookup)</p>	<ul style="list-style-type: none"> • Online * • EDI * • CRM • Mobile • [etc.]
O2D2	Order Pre-Processing	<p>Includes: credit check, order blocking, controlled substance license checking (customer and DC), CSOS eligibility, standard lookup, term eligibility, item eligibility for customer (order profile code), and execution of item substitution rules.</p>	<ul style="list-style-type: none"> • Distribution • Technology
O2D3	Order Pricing & Processing	<p>Accurate order pricing and processing that is consistent with customer contracts, promotions and rebates</p>	<ul style="list-style-type: none"> • Standard (includes: Drop-Ship order; Dock-to-Dock; Pre-Book; Auto-Ship; TradeCo; Stock Transfer Orders; Generics) • Central Fill • Technology Solutions Orders • Plasma Orders • Specialty Products Orders • Government

Actual operational compliance to controlled substance regulations is built into this process-oriented Product



Business Services Drilldown – Key Examples

Ref #	IT Product	Brief Description	Product Package(s)
P2P6	AP Processing	Includes invoice receipt through multiple channels; supplier submission of disputes; order matching and payment through multiple channels	<ul style="list-style-type: none"> • AP Invoice Processing • Online Dispute Management • Invoice verification - Logistics • Invoice verification - Finance • Payment Processing - Electronic • Payment Processing – Check
AFM7	Expense Management	Travel and Expense (T&E) enables McKesson employees and their managers to accurately create expense reports – classifying and submitting expenses – approve them, and initiate reimbursement for business-related travel and entertainment purchases made via corporate card or out-of-pocket payment. P-Card functions from purchases to accounting and compliance management. Includes reporting and analyses functionality.	<ul style="list-style-type: none"> • Travel & Entertainment • P-Card

Actual operational compliance for Federal Sunshine regulations is being built into these process-oriented Products



Providing evidence of the satisfaction of the controls

- Currently at McKesson:
 - IT Risk looks at the core applications and conducts risk assessments (focusing on SOX, HIPAA, PCI, ISO 27K) over time, with a view of the business process(es) that each applications supports
 - Legal & Compliance examines regulatory compliance, privacy, and security from a business perspective
- The Service-centric approach to defining & meeting Risk & Compliance requirements (as described in this case study) will help unite these two perspectives



Summary

- The architecture of an IT control framework needs to be designed collaboratively by Risk and IT professionals who can:
 - Design the process controls (Risk professional)
 - Design a method to provide the evidence to prove that the process control is operating effectively (IT professional)
- ITIL and COBIT both have their uses in defining and providing evidence of compliance to a controls framework
- Defining a unified control list is a noble objective, but most important is to understand:
 - The different controls in play
 - Who cares about each of them, and
 - On what cycle are they assessing the controls
- IT Service Provider should embed the required controls and measurement methods right into the upfront design of their services



Q&A

- Discussion
- Questions?

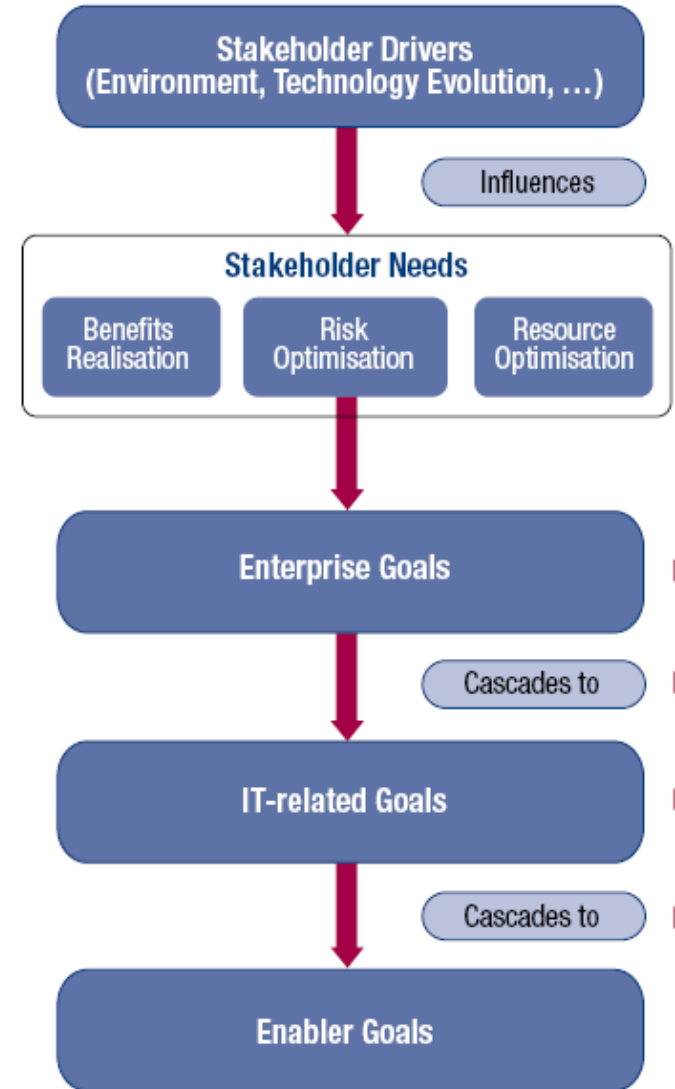
For more information, please contact:
mrobinson@mckesson.com



APPENDIX

COBIT 5 goals “cascade”

- Principle 1. Meeting Stakeholder Needs:
 - Stakeholder needs have to be transformed into an enterprise’s actionable strategy.
 - The COBIT 5 goals cascade translates stakeholder needs into specific, practical and customised goals within the context of the enterprise, IT-related goals, and enabler goals.



Stakeholder Value and Business Objectives – Balanced Scorecard

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		



Governance and Management Defined

- **Governance** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and 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).