

IT Governance Models & Good Practice Frameworks

Ian Inglis MBCI PMP



What is IT Governance?

The IT Governance Institute* defines IT Governance as

“an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives”

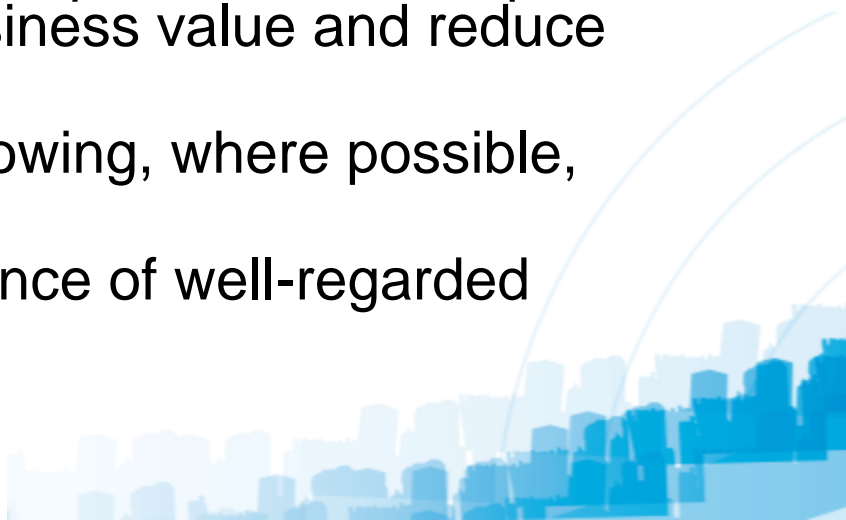
* The IT Governance Institute. URL : <http://www.itgi.org/>

IT Governance

Whatever the definition of an individual framework states, in essence they all cover:

- Control of the work
- Co-ordination between different pieces of work
- Measurement of outcome
- Compliance with internal policy or regulation
- Justification of spending
- Accountability and transparency
- Connecting with the needs of customers, the broader organisation, and other stakeholders

Business Drivers for the adoption of IT Best Practice

- Business demanding better returns from IT investment
 - Concern over increasing level of IT expenditure
 - The need to meet regulatory requirements for IT controls
 - The selection of service providers and the management of service outsourcing and acquisition
 - Increasingly complex IT-related risks, such as network security
 - IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities to increase business value and reduce business risk
 - The need to optimise costs by following, where possible, standardised approaches
 - The growing maturity and acceptance of well-regarded frameworks
- 

IT Governance Critical success factors

- Clear Purpose
- Senior Management Commitment
- Management of Business Change
- Minimise complexity
- Focus, execute and enforce
- Phased approach works best
- Develop realistic KPI's & Metrics

Control of Business Information and related Technology - COBIT

The IT Governance
Institute's (ITGI) definition of
IT Governance:

“the leadership and
organisational structures
and processes that ensure
that the organisation's IT
sustains and extends the
organisation's strategies
and objectives”

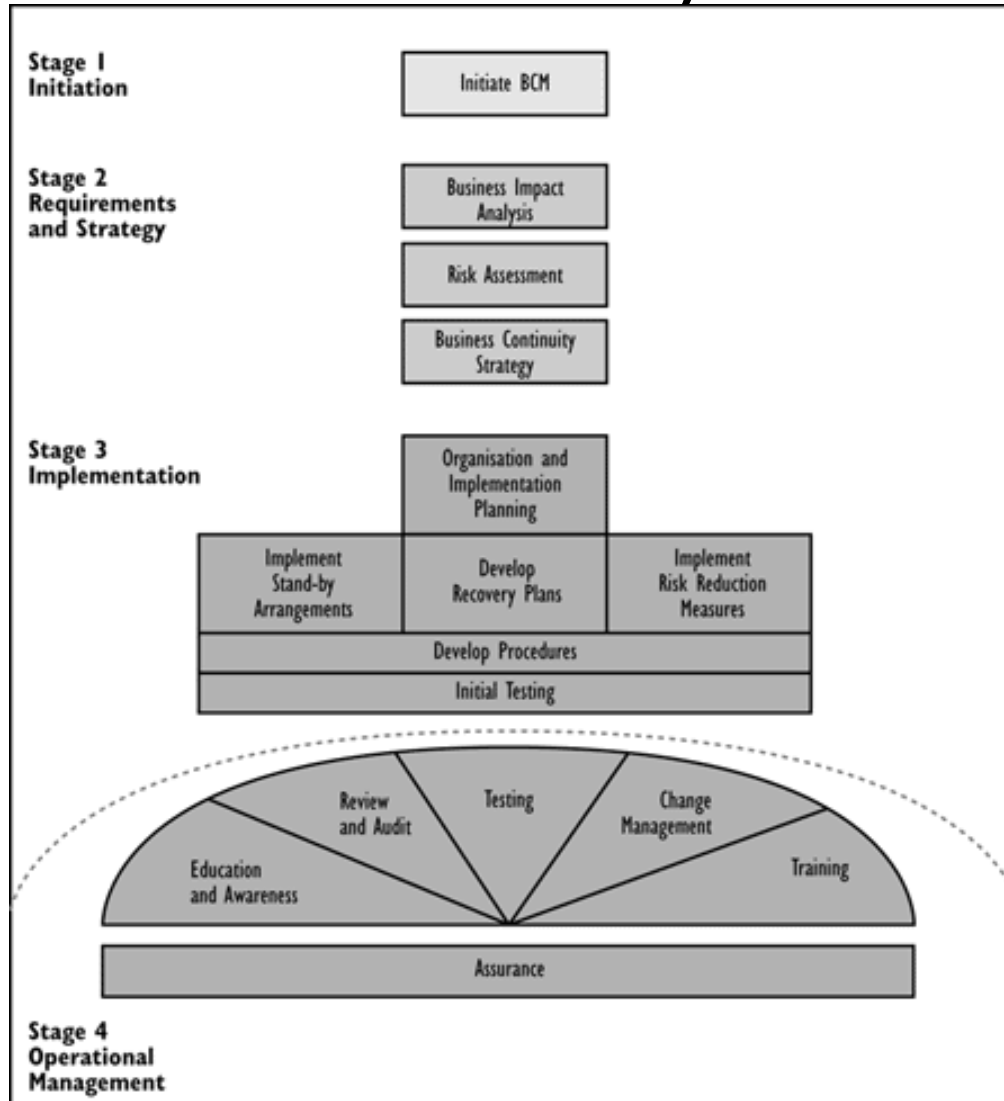


IT Infrastructure Library (ITIL)

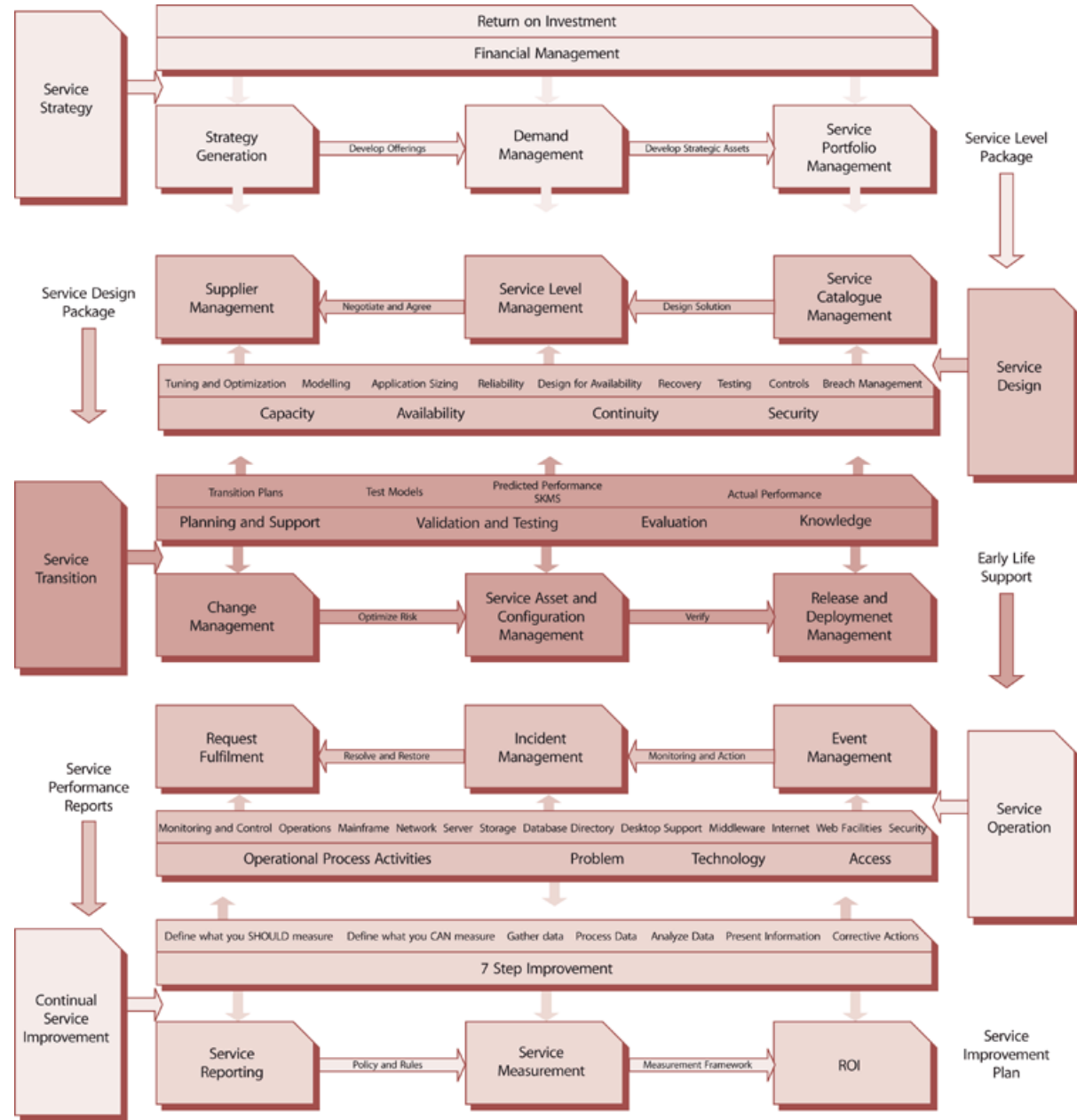
- Currently 2 versions in use:
 - V2 Focus on Service Management & Continual Service Improvement
 - V3 Builds on V2 by introducing Strategic planning concepts, reinforcing business linkage and general updates to reflect changing IT landscape



ITIL v2 – Service Continuity Lifecycle

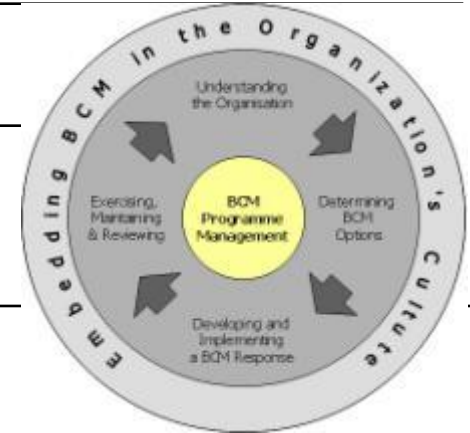


ITIL V3 Process Model



BCM Governance Structure

BS25999



- Identification of the necessary structure to control, measure and monitor BCM within the environment:
 - Federated approach
 - Success criteria for the BCM Programme
 - Metrics & KPI's for ongoing management
 - Issue/risk reporting & escalation
 - Links & association with IT and enterprise risk management
 - BCM status tracking and reporting
 - Integration of BCM into company culture and methods
 - Integration & association of BCM with Security management
- Work with Compliance/Legal functions to identify high level legal, regulatory and statutory requirements for BCM
- Identify key methods, criteria and process for benchmarking development and status of BCM across the Group

Backup/Recovery Governance Overlap

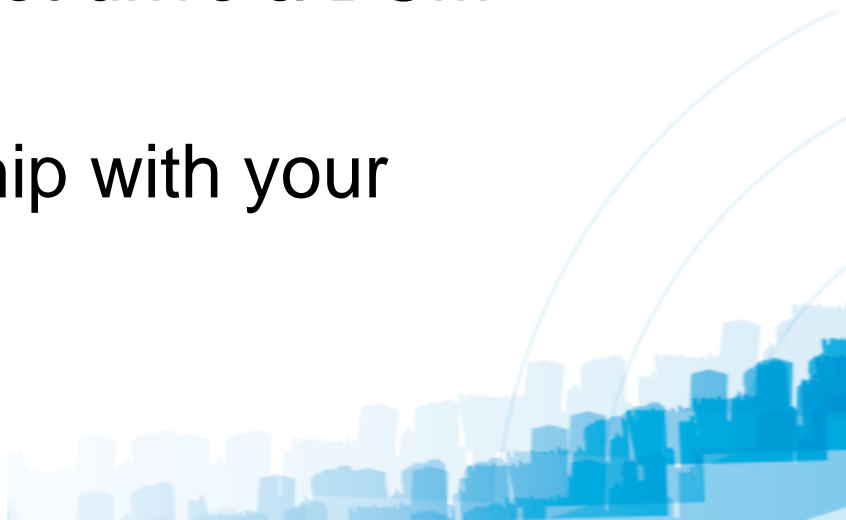
ITIL Area	SOX Objectives	Control Activity	COBIT No.	SOX	FSA	PCI*
Data Backup and Recovery	A backup plan is implemented to support the priorities and service availability requirements of the business	Appropriate personnel are verifying that backups are carried out completely according to a documented process and application requirements.	DS 11.24.6	In Scope	In Scope	
Data Backup and Recovery		Backup failures have documented rationale for the failure and follow up investigations are conducted and closed utilizing the organizations incident / problem / change management process.	DS 11.24, DS 8, DS 10		In Scope	
Data Backup and Recovery		Backups are removed off-site according to a documented procedure. This procedure directly addresses the frequency of the removal, what time of day it should occur, weekend activities, and the off-site accessibility, environmental protections, security, and off-site assessment process.	DS 11.24.7	In Scope	In Scope	3.1; 3.2; 3.3; 3.4; 3.5; 3.6
Data Backup and Recovery		Restorations are periodically tested to ensure (at a minimum) O/S usability and hardware/software compatibility, results are documented and approved by appropriate personnel.	DS 11.5		In Scope	
Data Backup and Recovery		Backup and restore procedures should consider requirements and approvals for: data retrieval, cost-effectiveness, continued integrity, encryption/authentication requirements, retention and data destruction protocols, and security requirements for legal, regulatory, and business requirements of data, archives, programs, and reports.	DS 11.25		In Scope	3.1; 3.2; 3.3; 3.4; 3.5; 3.6; 7.2
Data Backup and Recovery		Media containing sensitive information is securely stored, and, access to all backup media is restricted to authorized individuals.	DS 11.6		In Scope	3.1; 7.2; 9.10

* Payment Card Industry

SCM Governance Overlap

ITIL Area	SOX Objectives)	Control Activity	COBIT No.	SOX	FSA	PCI
IT Service Continuity		An operational risk analysis is completed and reviewed on an on-going basis and as a minimum every 6 months. The operational risk analysis considers the likelihood, impact and mitigation for risks to IT service continuity for infrastructure.	DS 4.1		In Scope	
IT Service Continuity		Documented IT Service and Continuity (including disaster recovery plans) for infrastructure should address the scope of coverage, requirements, disaster scenarios, recovery timeframes, recovery point objectives, alternative processing and recovery scenarios, outsource provider instructions, and detailed service continuity process procedures.	DS 4.2, DS 4.3		In Scope	12.9
IT Service Continuity		IT continuity plans for infrastructure should be periodically tested and the results documented and reviewed by key stakeholders and any remediation and corrective action implemented via the change management process.	DS 4.5		In Scope	
IT Service Continuity			DS 4.2, DS 4.3, DS 4.8		In Scope	
IT Service Continuity		IT disaster recovery plans for infrastructure should be periodically tested and the results documented and reviewed by key stakeholders and any remediation and corrective action implemented via the change management process.	DS 4.5		In Scope	

Summary

- There are a number of models/frameworks available
 - Framework should be moulded to fit your company's needs NOT the reverse
 - Consider an integrated Governance model
 - IT Governance alone will not drive a BCM strategy but it will help
 - Establish a good relationship with your Compliance team
- 

References

ITIL v2 Self Assessment material:

<http://www.itsmf.com/trans/sa.asp>

IT Governance Institute to download copy of COBIT:

<http://www.itgi.org>

