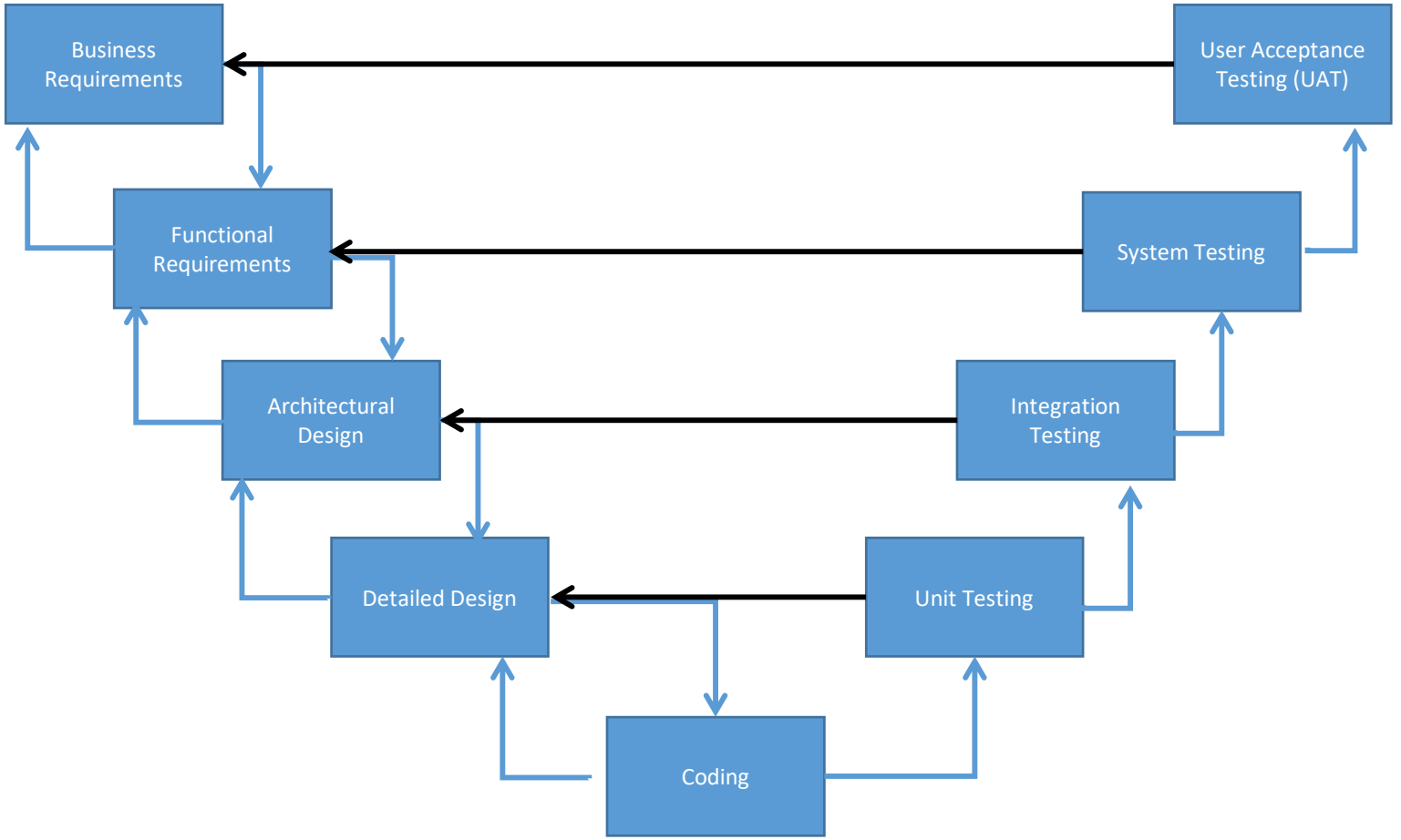
FOX | ITACS
Master of IT Auditing & Cyber Security

IT Audit Process

Michael Romeu-Lugo MBA, CISA

March 20, 2017

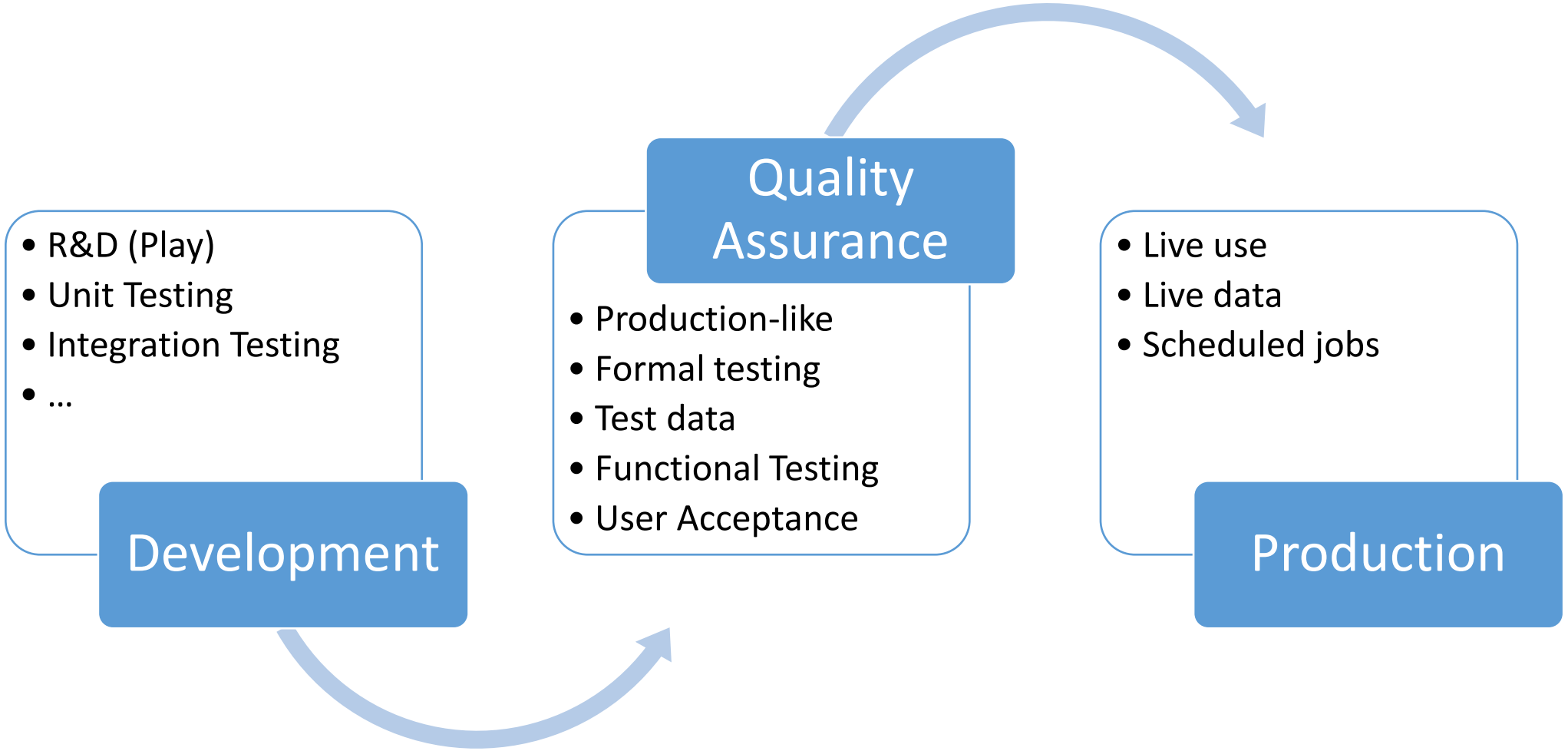
Development V&V



SDLC Life Cycle Controls – Activities and Documentation

Justification	Planning	Development	Testing	Implementation	Operation	Retirement
• Business Requirements • Feasibility Study • Business Case	• Scope Management • Time Management • Cost Management • Quality Management • Human Resources Management • Communications Management • Risk Management • Procurement Management • Stakeholder Management	• Business Requirements • Functional Requirements • Architecture Design • Detailed Designs • Coding	• Unit • Integration • System • User Acceptance	• Data Migration • Rollout Schedule • Training • Support Transition	• Incident Management • Problem Management • Change Management • Access Management	• Decommissioning Plan • Data/Records Archival

IT Environments



SDLC Life Cycle Controls – Activities and Documentation

Operation

- Incident Management
- Problem Management
- **Change Management**
- Access Management

Process for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organize

AP001 Manage the IT management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Innovation

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Innovation

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configurations

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Controls

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Process for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organize

AP001 Manage the IT management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Innovation

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Innovation

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configurations

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Controls

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

BAI06 Manage Changes

pp 24

BAI06 Manage Changes	Area: Management Domain: Build, Acquire and Implement
Process Description Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.	
Process Purpose Statement Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.	

BAI06 Manage Changes: Process Goals and Metrics

pp 149

Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Authorised changes are made in a timely manner and with minimal errors.	• Amount of rework caused by failed changes • Reduced time and effort required to make changes • Number and age of backlogged change requests
2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

RACI Charts

(R)esponsible	• Who is getting the task done? • Fulfilling activity listed/creating the intended outcome
(A)ccountable	• Who accounts for the success of the task? • Where the buck stops
(C)onsulted	• Who is providing input? • Key roles that provide input
(I)nformed	• Who is receiving information? • Informed of achievements and/or deliverables of task

BAI06 Manage Changes: RACI

BAI06 RACI Chart																									
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

BAI06 Manage Changes: RACI - Responsible

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

BAI06 Manage Changes: RACI - Accountable

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

BAI06 Manage Changes: RACI - Consulted

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

BAI06 Manage Changes: RACI – Informed

pp 149

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

Change Management Process – Roles and Responsibilities

Role	Responsibilities
Business Process Owners	• Evaluate, prioritize and authorize change requests • Track and report change status • Close and document changes
Project Management Office	• Close and document the changes
Chief Information Officer	• Evaluate, prioritize and authorize change requests • Manage emergency changes • Close and document the changes
Head of Development Head of IT Operations	• Evaluate, prioritize and authorize change requests • Manage emergency changes • Track and report change status • Close and document changes
Service Manager	• Evaluate, prioritize and authorize change requests • Manage emergency changes • Track and report change status • Close and document changes

BAI06.01 Evaluate, Prioritize and Authorize Change Requests

pp 150

Management Practice	Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.

Input	Process	Output
Integrated and configured solution components	**Evaluate, Prioritize and Authorize Change Requests**	Impact assessment
Approved service requests		Approved request for change
Proposed solutions to known errors		
Identified sustainable solutions		Change plan and schedule
Approved changes to the plan		
Root cause analyses and recommendations		

BAI06.01 Evaluate, Prioritize and Authorize Change Requests

pp 150

Activities
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.
6. Plan and schedule all approved changes.
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.

BAI06.02 Manage Emergency Changes

pp 149

Management Practice	Carefully manage emergency changes to minimize further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.

Input	Process	Output
	Manage Emergency Changes	Post implementation review of emergency changes

Activities
1. Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change.
2. Verify that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.
3. Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.
4. Define what constitutes an emergency change.

BAI06.03 Track and report change status

pp 151

Management Practice	Maintain a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.

Input	Process	Output
	Track and report change status	Change request status report

Activities
1. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.
4. Maintain a tracking and reporting system for all change requests.

BAI06.04 Close and document the changes.

pp 151

Management Practice	Whenever changes are implemented, update accordingly the solution and user documentation and the procedures affected by the change.

Input	Process	Output
	Close and document the changes	Change request status report

Activities
1. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.
4. Maintain a tracking and reporting system for all change requests.

BAI06 Manage Changes