



Independent Communications Authority of South Africa

Pinmill Farm, 164 Katherine Street, Sandton

Private Bag X 10002, Sandton, 2146

File Plan Reference: 8/2/P/3

INFORMATION TECHNOLOGY AND SERVICES

Application Life Cycle Policy, Procedures & Guidelines

September 2016

NOTICE

© Copyright 2016 ICASA

This document may not be copied in whole or part, in any manner whatsoever, without the express written permission of ICASA.

Handwritten initials/signature

Table of Contents

DOCUMENT CONTROL PAGE.....3

POLICY APPROVALS RECORD4

DEFINITIONS.....5

1. INTRODUCTION7

1.1 *Background 7*

1.2 *Policy statement..... 7*

1.3 *Purpose..... 7*

1.4 *Legislative mandate..... 8*

1.5 *Scope..... 8*

2. POLICY PRINCIPLES..... 9

2.1 *Principles..... 9*

2.2 *Policy implementation..... 10*

2.3 *Communication..... 10*

2.4 *Accountability..... 11*

2.5 *Reporting and monitoring..... 11*

3. COMPLIANCE..... 11

3.1 *Adherence to policy and procedure 11*

3.2 *Cross referencing..... 12*

3.3 *Review of policy..... 12*

4 ANNEXURES..... 13



4.1. *ANNEXURE A: SDLC- Procedures and Guidelines..... 13*

4.2. *ANNEXURE B – Life Cycle Phases..... 20*

Handwritten marks: a checkmark and a circled 'P' with a checkmark.

DOCUMENT CONTROL PAGE							
Document title	Application Life Cycle Policy						
Creation date	October 2006						
Effective date	1 September 2016						
Digital name	Application Life Cycle Policy, Procedures and Guidelines						
Electronic location	ICASA Intranet\Policies						
Password Protected		Yes		No	X		
Status		Draft		Final	X		
Version	V1.1						
Author title, name and contact details	IT Management Information Systems Manager, Phila Mhlakaza, PMhlakaza@icasa.org.za						
Editor title, name and contact details	Senior Manager: IT Roshan Algu ralgu@icasa.org.za						
Policy owner title, name and contact details	Senior Manager: IT Roshan Algu ralgu@icasa.org.za						
Contributors	Riaan Scheepers, Exco, ITRC and Internal Audit						
Distribution	ICASA						
Security classification Indicate with X	Restricted	X	Confidential		Secret		Top Secret
Revision Record	Versi on No	Revisio n Date	Revision Details			Revised by	
Revision frequency: Every 2 years	V1.1	May 2016	Included policy principles Moved SDLC procedures and guidelines as Annexure A and SDLC phases as Annexure B Added Post Implementation Review			R Algu	



POLICY APPROVALS RECORD		
	Approved by the Accounting Officer	Authorised by Council
Name and job title	Pakamile Pongwana Chief Executive Officer	Acting Chairperson
Signature		
Date	29/09/2016	13/10/2016
Implementation date	1 September 2016	



DEFINITIONS

For purpose of this policy, unless otherwise stated, the following definitions shall apply:

Manual	A system of approved policy statements and corresponding procedural guidelines and supporting forms that direct the Authority towards its operational goals.
Obligation	The laws, regulations, statutes, codes, policies, procedures and community standards to which ICASA should comply.
Policy	A concise, formal and mandatory statement of principle which provides a framework for decision-making and a means by which the Authority reduces institutional risk. Policies support the Authority's course for the foreseeable future and should therefore change infrequently.
Policy decision	A stated course of action with a defined purpose and scope to guide decision making under a given set of circumstances within the framework of corporate objectives, goals and management philosophies.
Policy owner	The policy owner is a management position responsible for the development, oversight and review of a policy.
Procedure	The mandatory steps required to implement and comply with a policy and meet its intent. A procedure specifies who does what and when. A procedure may be reviewed and revised more frequently than the policy it is associated with.
Process	A series of prescribed steps followed in a definite regular order which ensure adherence to the guidelines set forth in a policy or procedure to which the process applies.



Responsibility	The management position responsible for implementation of a policy and procedures, and also responsible for monitoring implementation of and compliance with the policy and its associated procedures.
Responsible Officer	Is a member of staff who is appointed by management to assist in the facilitation, monitoring and reporting of compliance within their business unit or department

Handwritten signature and initials in the bottom right corner. The signature appears to be 'W' and the initials are 'W'.

1. INTRODUCTION

This policy is part of a set of policies which its main aim is to provide a Systems Development Life Cycle (SDLC) methodology to be used to ICT application acquisition, enhancement and development.

1.1 Background

- 1.1.1. This policy provides a framework for the implementation of Applications/Business Solutions. The SDLC methodology is intended to provide controls over the processes of acquiring and maintaining application software resulting in decreased risk of project or system failure. The SDLC methodology includes oversight processes to ensure that all aspects of the development lifecycle are consistently and effectively managed.
- 1.1.2. The aim of this Application Life Cycle Policy is to prescribe the application of measures necessary to assure the continued delivery of services in order to meet ICASA's legislative mandate and the requirements of corporate governance.

1.2 Policy statement

- 1.2.1. The objective of the policy is to establish a structured process to plan, design, build, deploy, operate, maintain and (if necessary) dispose applications which are no longer adding value to the business needs of ICASA.

1.3 Purpose

- 1.3.1. To establish an Application/Business solution and associated Life Cycle Policy to meet ICASA's changing and expanding business needs. Life cycle in this context refers to the "cradle to grave" activities associated with the application, spanning the complete process from the business need through eventual replacement, with all stages in between including selection, deployment, operation, maintenance and enhancement. Refer to Annexure A for phases of the Systems Development Life Cycle (SDLC).

- 1.3.2. Software has an expected life just like IT hardware and infrastructure. System software and back-office applications (e.g. word processing software, specialized business applications i.e. off-shelf and custom solutions) normally gets upgraded or replaced at the time of replacement of the hardware, i.e. every three to five years.
- 1.3.3. Application or business solution software also has a useful life, but because of the cost involved on the one hand, and an architecture that allows enhancements (up to a point) on the other, they tend to have life cycles that typically last between five and ten years, sometimes longer.
- 1.3.4. This policy defines the application life cycle in the ICASA context and documents the key decisions and processes affecting applications at every stage in its life cycle (Refer to Annexure B).

1.4 Legislative mandate

- 1.4.1 ICASA is required to manage its information and records within a legislative framework.
- 1.4.2 This policy provides a framework for the implementation of Applications/Business solutions to the entire ICASA.
- 1.4.3 The South African National Archives and Records Service, in terms of its statutory mandate, requires governmental bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. All information records created and received by ICASA shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996. (see ICASA Records Management Policy)

1.5 Scope

- 1.5.1. This policy applies to the following individuals and entities:
 - 1.5.1.1. Council

1.5.1.2. All employees of ICASA

1.5.1.3. All contractors and consultants delivering a service to ICASA, including their employees who may interact with ICASA;

2. POLICY PRINCIPLES

2.1 Principles

2.1.1 Divisional Managers who need new application and business solutions to support their business processes shall work with the Senior Manager IT & Services to select such applications and business solutions that conforms to the framework provided in this policy.

2.1.2 Each System Project must have a Program Sponsor: To help ensure effective planning, management, and commitment to information systems, each project must have a clearly identified program sponsor. The program sponsor serves in a leadership role, providing guidance to the project team and securing. from senior management, the required reviews and approvals at specific points in the life cycle.

2.1.3 A Single Project Manager must be appointed for each project: The Project Manager has responsibility for the success of the project and works through a project team and other supporting organisation structures to accomplish the objectives of the project.

2.1.4 A project charter is required for each system project: The project charter is a pivotal element in the successful solution of an information management requirement. The project charter must describe how each life cycle phase will be accomplished to suit the specific characteristics of the project. The project charter is a vehicle for documenting the project scope, tasks, schedule, allocated resources, and interrelationships with other projects. A project plan is used to provide direction to the many activities of the life cycle, and must be refined and expanded throughout the life cycle.



- 2.1.5 Each system project deliverable must undergo formal acceptance: The program sponsor (or business owner) formally accepts the system by signing a User Acceptance Testing signoff.
- 2.1.6 Each IT project should comply with these established guidelines: The SDLC methodology includes phases during which defined ICT work products are created or modified, providing a full sequential SDLC work pattern. The phases of the SDLC are expanded in Annexure A.

2.2 Policy implementation

- 2.2.1 Accountability and responsibility for the implementation of this policy is set out below:
 - 2.2.1.1 Senior Manager: IT and Services
 - 2.2.1.2 Divisional Line Manager(s), Senior Managers and General Managers
 - 2.2.1.3 Manager: MIS

2.3 Communication

- 2.3.1 The Senior Manager: IT shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with ICASA. The CEO will further ensure that the Application Life Cycle Policy and directive prescriptions are enforced and complied with.
- 2.3.2 Communication of the Application Life Cycle Policy will be by means of a program conducted as follows:
 - 2.3.2.1 distribution of memos and circulars to all employees; and
 - 2.3.2.2 access to the policy and applicable directives on the ICASA intranet.

2.4 Accountability

- 2.4.1 The Senior Manager: IT is responsible to establish and enforce a policy to assure that the implementation of Application/Business solution is made in a controlled way, minimising the impact and risk to the users of the ITS facilities;
- 2.4.2 The Senior Manager: IT is responsible to identify, investigate and recommend to Council and other Divisional Managers, applications and business solutions that support ICASA's business strategy and changing business needs;
- 2.4.3 The Manager: MIS is responsible to implement and maintain the applications and business solutions according to the Life Cycle elements of this policy;
- 2.4.4 All IT staff and contractors, who have a mandate to support the IT Applications/Business Solutions and therefore may have a need to work according to the Application Life Cycle Framework;
- 2.4.5 Upon approval of the Application Life Cycle Policy, the Senior Manager IT delegates responsibility and associated authority to implement and execute the policy to the Manager: MIS.

2.5 Reporting and monitoring

- 2.5.1. The breaches of Application Life Cycle policy will be reported in line with the requirements of Legal and Risk Division.

3. COMPLIANCE

3.1 Adherence to policy and procedure

- 3.1.1 It is the responsibility of the relevant delegation to make appropriate provision for establishing controls to ensure adherence to this policy and procedure.

- 3.1.2 No deviations to this policy and procedure are permitted. Any incident where this policy and procedure has been breached should be monitored and reported to the Compliance Officer in the Legal and Risk Division.
- 3.1.3 Any disciplinary action taken in terms of non-compliance with this policy and its associated documents will be in accordance with the disciplinary procedures of the Authority.

3.2 Cross referencing

- 3.2.1. The following policies and procedures should be read in conjunction with this policy;
 - 3.2.1.1. Information Security Policy
 - 3.2.1.2. IT Infrastructure Change Management Policy
 - 3.2.1.3. IT Project Management Policy
 - 3.2.1.4. IT Facilities Internet and E-mail Usage Policy
 - 3.2.1.5. IT Asset Policy
 - 3.2.1.6. ICASA Supply Chain Management Policy/PFMA
 - 3.2.1.7. ICASA disciplinary code

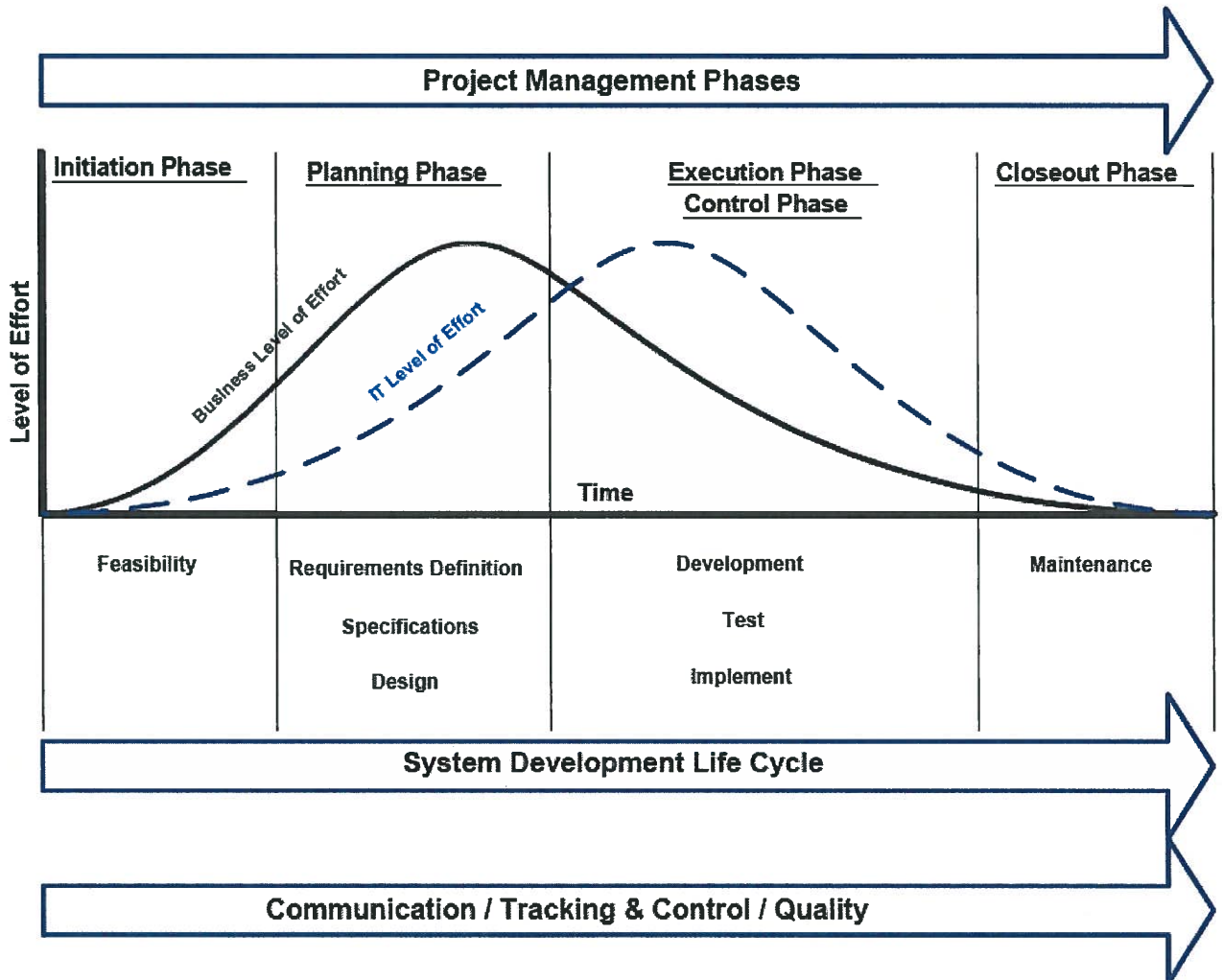
3.3 Review of policy

- 3.3.1 The policy owner shall initiate a review of this policy, its procedures and associated documents every two (2) years. Significant amendments that result in a change in practice shall go through the approval and authorisation process specified in the Policy and Procedure Review Framework.

4 ANNEXURES

4.1. ANNEXURE A: SDLC- Procedures and Guidelines

4.1.1. IT projects consist of applying the people, process, and tools to initiate, plan, execute, control, and close out projects relating to computer-based information systems. IT deliverables are normally created using what is referred to as the System Development Life Cycle (SDLC). The SDLC is a very detailed and specific set of procedures, steps, and documents that carry a project through its technical development. It is intended as a guide to assist in deciding on what project management concepts must be applied during the SDLC development of an IT product to ensure that a quality deliverable meets or exceeds customer expectations. ICASA Business units and sub-units should follow established informational processing system methods:



4.1.2. SDLC is broken down into five phases:

- a. Initiation Phase
- b. Planning Phase
- c. Execution Phase
- d. Control Phase
- e. Close-out Phase

4.1.3. Within these phases, several SDLC processes are performed (e.g., requirements definition, design, development, testing, and operations). These processes have been created and are maintained at an operational level.

4.1.4. Details on each phase of SDLC

4.1.4.1. **Initiation Phase:**

4.1.4.1.1. Information technology projects must have a starting point. Once a need has been recognized for a new IT product or service, several processes must take place for the project to be defined more clearly and approved. Within the Systems Development Life Cycle, a Feasibility Study Document will be completed. The creation of this document interrelates with the project manager's responsibilities of putting together a product description, synthesizing a business analysis, and drafting a Project Concept Document and a Project Charter.

4.1.4.1.2. Major activities of Initiation Phase:

- i. Support Establishment of:
 - Goals & Objectives
 - Possible Approach
 - Resource Needs
- ii. Product Description
- iii. Project Feasibility
- iv. Concept Document
- v. Project Charter
- vi. Project Manager Skills and Responsibilities

4.1.4.1.3. Key Products of the Initiation Phase

- i. Feasibility Study

4.1.4.2. **Planning Phase:**

4.1.4.2.1. Project Planning is the most important phase of information technology projects. It is during this phase that the document baseline and processes that will be used to guide all the work to be done in the project will be created. Being able to manage communication, budgets, risk, and the other assorted project management competencies is of infinite importance because these processes create the infrastructure that allows technical project staff to commit themselves to producing quality documents and deliverables.

4.1.4.2.2. Major activities of Planning Phase:

- i. Project Scope
- ii. Work Breakdown Structure
- iii. Cost Benefit Analysis
- iv. Resource Plan
- v. Schedule Development
- vi. Risk Planning
- vii. Quality Planning
- viii. Communications Planning
- ix. Project Budgeting
- x. Planning Summary

4.1.4.2.3. Key Deliverables of the Planning Phase:

- i. Work Statement
- ii. Requirements Documents
- iii. Solutions Documents
- iv. Specifications Documents
- v. Design Schedules
- vi. Technical Specifications
- vii. Project Plan

4.1.4.3. Execution Phase:

4.1.4.3.1. During the execution phase the SDLC the actual information technology project is developed. Testing is the actual test of the products or processes created within the Development Phase. Implementation involves putting the tested and approved products into an operational environment for use by the customer. Documentation includes the creation of written operations manuals, standards, systems outputs, and performance reports that document the requirements and use of the product. All of these components combined provide the basis for the SDLC within the Execution Phase.

4.1.4.3.2. Major activities of Execution Phase:

- i. Contract Administration
- ii. Project Administration/ Weekly and Monthly reports
- iii. Risk Management

4.1.4.3.3. Key Deliverables of the Execution Phase:

- i. Development
- ii. Testing
- iii. Implementation
- iv. Documentation

4.1.4.4. Control Phase:

4.1.4.4.1. Control is vital for keeping projects within scope, cost, schedule and within acceptable quality because there are so many variables that may come into play. IT projects often deal with unknown or unproven technologies that make these projects difficult for the project manager to baseline the scope, schedules, and costs during the Planning Phase.

4.1.4.4.2. Project control in information technology is a combination of formal and informal processes that work together to keep a project moving forward while evaluating changes, redefining planning efforts, and making decisions that could affect the outcome of the project as a whole.

4.1.4.4.3. Major activities of Control Phase:

- i. Scope Control
- ii. Schedule Control
- iii. Cost Control
- iv. Quality Control
- v. Risk Control
- vi. Contract Administration
- vii. Configuration Management

4.1.4.4.4. Key Deliverables of the Control Phase:

- i. Develop
- ii. Test
- iii. Implement
- iv. Document

4.1.4.5. **Closeout Phase:**

4.1.4.5.1. The intent of the Project close-out process is to bring closure to the activities that have been carried out in the Execution and Control Phases. The process for Information Technology projects is basically the same as for non-Information Technology projects. The MIS: Manager or the Project Manager is responsible for ensuring that the common close-out processes are carried out while the developed Business Application/solution systems are rolled-over into maintenance mode.



4.1.4.5.2. Major activities of Closeout Phase:

- i. Project Administrative Closure
- ii. Project Financial Closure
- iii. Project Audit

4.1.4.5.3. Key Deliverables of the Closeout Phase:

- i. Maintenance
- ii. Service Level Agreements

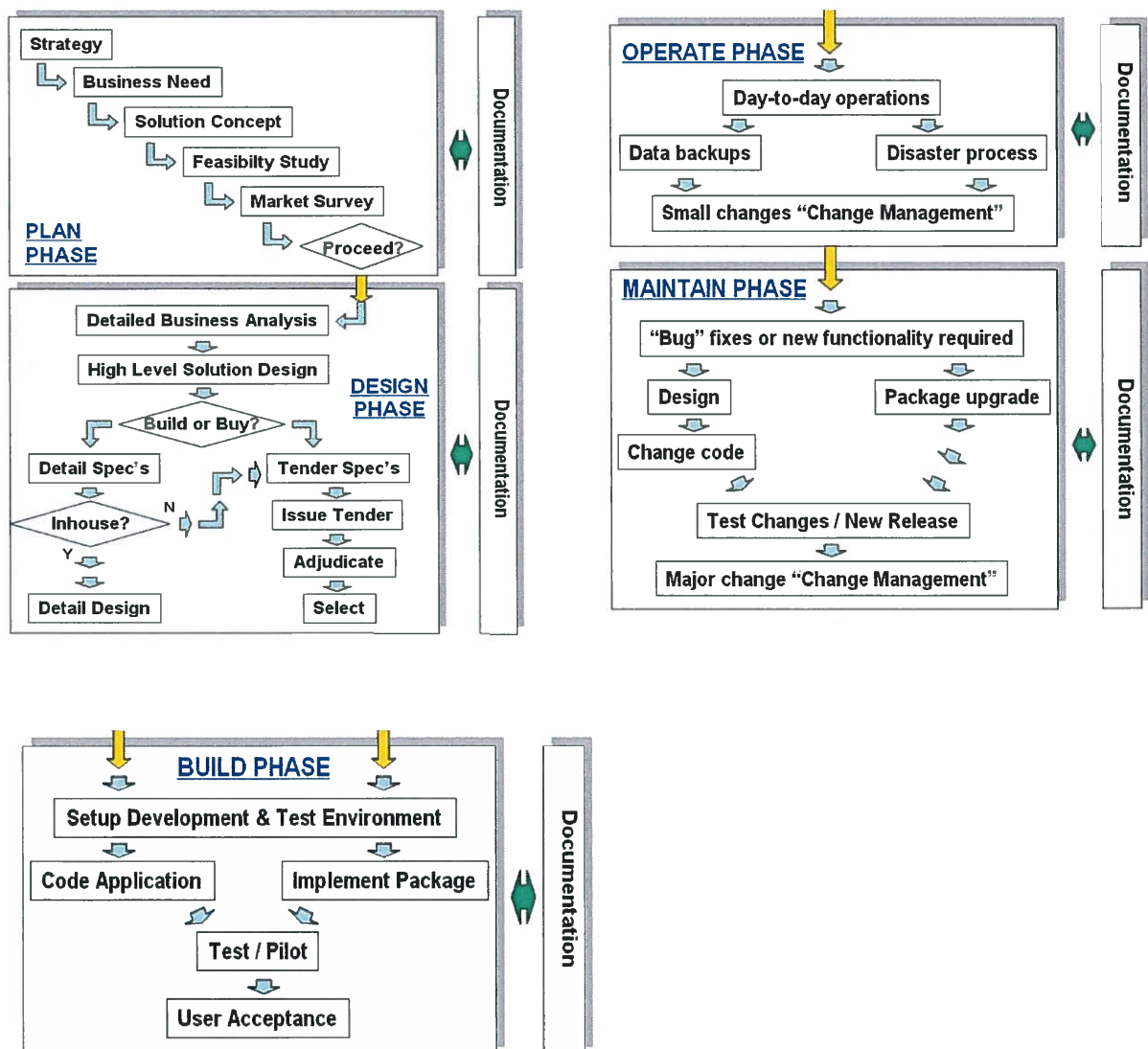
4.2. ANNEXURE B – Life Cycle Phases

4.2.1. LIFE CYCLE PHASES

Different sources use different names for the phases, but in essence a life cycle contains the following phases:

PLAN -> DESIGN -> BUILD -> DEPLOY -> OPERATE -> MAINTAIN > DISPOSE

The following diagram summarizes the major components of an application life cycle:



4.2.2. Documentation

Note that every phase and every step within a phase require that comprehensive documentation be created and filed, e.g. design specifications, contracts, project plans, minutes, operations guides etc.

4.2.3. Planning Phase

4.2.3.1. Strategy

4.2.3.1.1. The process starts with the ICASA business strategy, and is aimed at providing the business solutions needed by ICASA to meet its business mission and objectives.

4.2.3.1.2. The process is triggered "top-down" when major changes in the ICASA strategy occurs, e.g. prompted by legislative changes, market condition changes or strategic policy changes needed to enable a competitive and socially responsive communications environment that is manageable.

4.2.3.1.3. It may also be triggered "bottom-up" by IT&S or any of the ICASA business units when new solutions or technology becomes available that can increase effectiveness and/or efficiency of any part of the ICASA business operations.

4.2.3.1.4. IT&S shall balance the potentially conflicting Business Need. The business need is normally expressed in the form of a formal business case that is presented for approval.

4.2.3.2. Solution Concept

4.2.3.2.1. The Solution Concept is a business description of the functionality required to meet the business need, and is the DoA (Document of Understanding) between the business unit / users and IT&S.

4.2.3.3. Feasibility & Impact Study

The feasibility study covers four aspects:

- 4.2.3.3.1. Strategic - The solution and/or technology may potentially have no positive impact on ICASA and even have negative ROI, but its implementation is justified on the basis of industry credibility, i.e. practice what they preach.
- 4.2.3.3.2. Financial - This is a ROI projection, and should meet or exceed ROI standards for new investments as determined by the CFO and Council. Note that in order to do this part of the feasibility study, it will be necessary to reasonably accurately determine the costs associated with the solution. These costs not only cover acquisition costs, but ongoing operational costs as well as potentially hidden costs as per the Technology and Process areas below.
- 4.2.3.3.3. Technology - Technology: Will the solution and/or technology fit into the current standards, skills and processes of ICASA, or will it cause a small "revolution" in these areas? Will ICASA be able to obtain possible scarce or esoteric skills to implement, maintain and operate it?
- 4.2.3.3.4. Process - Will the solution and/or technology fit into the existing business process processes, or will it change business processes? How wide will the impact be – confined to one department, or ICASA wide?

4.2.3.4. Market Survey

- 4.2.3.4.1. Once the feasibility of the solution has been confirmed, a market survey is recommended to determine where the solution or similar solutions is successfully deployed, preferably in a similar (regulatory) environment. Depending on the cost and impact of the solution, this can be a simple web-based research or may, in exceptional cases, involve site visits to other users of the solution to verify the conclusions reached during the feasibility study, and to learn about possible pitfalls in the deployment of the solution.

4.2.3.5. Decision to Proceed

- 4.2.3.5.1. Armed with all this information, the business case is updated and presented for approval to Council. If approval is granted to proceed, the budget is allocated and the next phase – Design - initiated as a project.
- 4.2.3.5.2. Note that if at any stage during the Design Phase, any of the assumptions of the business case are changed or proved wrong, or if any new information becomes available that affect any one of the feasibility study components, including the projected cost, the business case has to be updated and referred back to the Council and or CEO and the General Manager/Head of Division concerned.

4.2.4. Design Phase

- 4.2.4.1. The Design Phase is run as a formal project a project plan should be defined, resources allocated and progress and results monitored in line with the adopted ICASA IT&S Project Management Framework (PMBOK).

4.2.4.2. Detailed Business Analysis

- 4.2.4.2.1. Up to this stage, the business need and solution concept was at a high level. This step will determine business needs down to the business process, transaction and information level, as well as interfaces to other applications, business units and external information.

4.2.4.3. High Level Solutions Design

- 4.2.4.3.1. The high level solution design, or solution architecture, is intended to document the output of the business analysis in a way that will enable a decision to build (i.e. develop a unique or bespoke solution) or buy (i.e. acquire, install and

customise an existing software package). ***Build or Buy (Bespoke Solution or Off-the Shelf Package)?***

4.2.4.3.2. In principle, any organization should only revert to build if any of the following conditions hold true:

(a). The solution is unique or leading edge and no package exists.

(b). The solution affects a "line" function and is unique to an organization or enables competitive differentiation or a competitive edge.

(c). The organization has the capability to develop and maintain, throughout the projected life cycle, bespoke applications.

4.2.4.3.3. Most organizations will maintain a limited in-house development capability only to meet relatively small business unit requirements. In the event where they need a major custom application, development will be contracted to a professional development shop which has the skills, tools and methodologies to develop, test and maintain complex custom application solutions.

4.2.4.3.4. It is acknowledged that ICASA does not have the need for complex, custom applications at this stage, and will follow the route of outsourced custom development should the need arise.

4.2.4.3.5. The remainder of the Design Phase therefore focuses on identification and selection of an appropriate packaged solution, or the identification and selection of a custom development business to develop the bespoke solution.

4.2.4.4. Procurement of Software Applications/Business Solution and Service

4.2.4.4.1. However, before a package or a bespoke developed solution can be issued according to the guidelines that are prescribed in the Supply Chain Management Policy/PFMA, it is imperative to create detailed requirements specifications and motivation for the BAC (Bid Adjudication Committee) where applicable. These should

include all the business functionality required, the information needs and interfaces to other systems where applicable.

4.2.4.5. Issue Tender, Adjudicate & Select solution

4.2.4.5.1. These steps are covered in other ICASA Supply Chain Management Policy/PFMA. However, it is important to note that the lifecycle of an application solution is typically 10 years – consequently the tender process should also look at the vendor’s plans to enhance and keep the software “competitive” and “current”.

4.2.5. Build Phase

4.2.5.1. This phase is controlled by a comprehensive project plan, with defined user interaction points, milestones, interim deliverables, and a formal UAT (user acceptance testing).

4.2.5.2. The SDLC framework has been accepted and is used widely within the Information and Communication Technology industry. Therefore, ICASA shall adopt this framework for the development of an Applications / Solutions Development Methodology, which shall be deployed for all applications development

4.2.5.3. The management of projects shall be governed by principles stipulated in the Project Management Body of Knowledge (PMBOK)

- Two environments shall be setup:
 - Development;
 - Pre-Production.
- Application development testing shall be conducted in the Development Environment;
- End-User application development testing shall be conducted in the Pre-Production Environment.

4.2.5.4. Set-up Development and Test Environment

4.2.5.4.1. All major application solutions need to have a dedicated development / test environment, where changes and version upgrades can be tested against a copy of the database, without having an impact on the live systems and production database, before being migrated to production. The system(s) should have sufficient capacity and power to allow meaningful testing of changes – refer to the Change Management Policy.

4.2.5.5. Code Application / Customize and Implement Package

4.2.5.5.1. All major application solutions need to have a dedicated development / test environment, where changes and version upgrades can be tested against a copy of the database, without having an impact on the live systems and production database, before being migrated to production. The system(s) should have sufficient capacity and power to allow meaningful testing of changes – refer to the Change Management Policy.

4.2.5.5.2. Note that the application solution and designated execution environment (server, storage and network) must conform to the ICASA standards (refer to the IT Assets Policy) as well as the information security requirements as documented in the Information Technology Security Policy.

4.2.5.6. Systems Test, Pilot and User Acceptance

4.2.5.6.1. This step is still a part of the formal "**Build Phase**" project, and focuses on the transition from development to deployment in production. The System Test part is performed in life-like circumstances, on a copy of the production data, and may involve user staff to capture transactions or information on the new system, in parallel to doing so in the current system or process, in order to test the system and the results. A formal "**System Test Build**" of the Application solution is to be used, and any changes

applied to this **"Build"** are to be documented through the Change Management System
 – refer to the Change Management Policy.

4.2.5.6.2. Two test environments shall be created:

- **Application Development testing**– For all application/business solution development and developer testing;
- **Pre-production testing** – For all End-Users and Systems Administrator testing.

4.2.5.7. Application Development Testing

4.2.5.7.1. The Service Provider/ Developer shall develop and test all development in the development environment;

4.2.5.7.2. The Service Provider/Developer may invite the principal end-user to do some testing during software development in the development environment;

4.2.5.7.3. The Service Provider/Developer shall make sure that all programs that are impacted on by the changes, are tested and function as per requirements;

4.2.5.7.4. The Service Provider/Developer shall give a status report to the Project Manager or Manager: MIS, where applicable, on a periodic basis;

4.2.5.7.5. The Service Provider/Developer shall correct all errors referred to from the pre-production testing environment and test the changes before requesting for re-migration.

4.2.5.8. Pre-Production Testing

4.2.5.8.1. Pre-production testing shall be done in two stages, namely, first and final acceptance.

4.2.5.8.2. First Acceptance



- The end-user shall design a test plan which shall include data required for testing the system;
- The end-user shall capture all the required data online into the Pre- Production environment;
- If the software changes require the execution of batch jobs, then the end-user shall request the Network and Operations unit to schedule and run the batch jobs;
- If any problem related to the software changes is encountered, the End-user shall report it to the Service Provider/Developer and all changes introduced shall then be reversed;
- The end-user shall peruse all reports produced and attest to the correctness of such reports.

4.2.5.8.3. Final Acceptance

- The end-user shall design a more robust test plan;
- Much more data than that used in the First Acceptance testing shall be entered;
- The end-user shall test the problem application and all other integrated applications;
- If the transactions so produced feed into the normal daily, weekly and monthly job schedules, these, too, shall be scheduled and run;
- The end-user shall peruse all reports produced and shall attest to their correctness and completeness;
- The test plan and test results must be retained for UAT and audit purposes.

4.2.5.8.4. The Manager: MIS or Manager: Network and Operations must be involved in the final acceptance testing process.

4.2.5.9. Migration / Data Migration



4.2.5.9.1. The production data from the “old” system needs to be migrated to the new system, or if none existed, the core information has to be captured in the new system. Backup copies of the data before and after the migration has to be kept for audit purposes, i.e. if there should be query regarding any possible changes to the data during the migration process.

4.2.5.9.2. This is an appropriate time to assess data quality and clean the data, e.g. archive dormant data, eliminate duplicate records, fix errors etc.

4.2.5.9.3. Data that has been migrated must be tested for accuracy, validity and completeness. Results of this must be signed off by the Business Owner and then retained for audit purposes.

4.2.5.10. User Training

4.2.5.10.1. An important and often neglected part of the implementation of a new system is user training – training manuals and materials have been developed as part of the “Build Phase” documentation.

4.2.5.10.2. Training should be completed before roll-out commences, or as part of the roll-out process, and users should be left with a summary, e.g. in the form of a reference card, which should also contain the number to call for help! There should not be a significant time lapse (i.e. more than two weeks) between training and actual commencement of using the new system.

4.2.5.10.3. The user training should be made available on request, or as part of new employees’ (who will be users of the system) induction programs.

4.2.5.11. Roll-out

4.2.5.11.1. The roll-out of the application should be supported by increased availability of support staff, help desk staff or even SWAT teams to visit users to answer questions,

resolve issues and generally ensure that the users are comfortable with the new application.

4.2.5.11.2. A second and more important component of the roll-out phase is to audit a large proportion of the transactions and the data base – if users (through misunderstanding or through lack of enforced controls in the system) enter wrong information, the data base will be corrupted. This needs to be corrected very quickly through training or, preferably, through a system change that will detect and / or prevent the entry of incorrect information into the system.

4.2.6. Operate Phase

4.2.6.1. Activities of this phase have essentially been covered in other IT policies and Procedures.

4.2.6.2. **Day-to-day Operations** - Normal operational procedures to assure availability of the system to the users, handle queries.

4.2.6.3. **Changes to System** - Covered in the IT Infrastructure Change Management Policy. "Small Change" Change Management, refers to adding / removing users, password reset etc. i.e. the changes that do not affect the "Production Build" implementation of the application solution, i.e. the code, database or deployment (server).

4.2.6.4. **Data Back-ups** – The systems administrator to ensure that the development, QA and production environments are included in the backup schedule. Full recovery of new systems from backups must be included in the next schedule DR test.

4.2.7. Maintenance Phase

4.2.7.1. Maintenance will be required regardless of whether the application was custom developed or acquired as a standard package. The most important aspect is to have a

maintenance agreement (SLA) with the developer of the system / vendor of the package.

4.2.7.2. Fixes, New Functionality

4.2.7.2.1. "Fixes" refer to resolving problems, errors or incorrect results (vis-à-vis the specifications) of the system, while "new functionality" refers to a requirement stemming from a new or changed business need.

4.2.7.2.2. Note that a Package may not offer the required "new functionality" or that it may only offer it as an option (i.e. at an additional cost!). Whether it is a problem fix or new functionality, the process will affect the "Production Build." Depending on the scope of the fix or upgrade, a project should be launched to develop / implement the proposed changes and take it through a comprehensive test cycle before releasing and deploying a new "Production Build."

4.2.7.3. Test

4.2.7.3.1. This aspect is extensively covered above as well as in the IT Infrastructure Change Management Policy. Note that depending on the scope of the change, it may require another complete "deploy" process, as detailed earlier in this policy.

4.2.7.3.2. This step is especially essential if the infrastructure is changed, e.g. a new version of the server operating system, database management software of any aspect of the hardware (delivery platform) or network.

4.2.7.4. Major Change / Change Management

4.2.7.4.1. This aspect is extensively covered in the IT Infrastructure Change Management Policy.

4.2.7.4.2. ICASA should be aware that it is not recommended to implement two (or multiple) major changes simultaneously, e.g. a new version of the application software AND a new version of the server operating system. It is always better to implement and stabilise one major change or upgrade, and only then proceed to the next one.



4.2.7.5. Disposal-Phase

- 4.2.7.5.1. The disposal of the Application/Business solution would entail move, sanitise, dispose, archive of information, software and hardware, where applicable.
- 4.2.7.5.2. All documentation including approved change control forms and evidence of disposal and archives must be retained for record and audit purposes

4.2.7.6. Post Implementation Review

- 4.2.7.6.1. The Post Implementation Review (PIR) is conducted after a project has been completed. The purpose of the PIR is to evaluate how successfully the project objectives have been met and how effective the project management practices were in keeping the project on track. The outcomes of the PIR should be documented in a Post Implementation Review Report (also known as a Close-Out Report).
- 4.2.7.6.2. Review the Project Charter to evaluate how closely the project results match the original goals, objectives, and deliverables. This review should also include a gap analysis between the planned requirements, schedule, and budget and what was actually delivered, when and for how much.
- 4.2.7.6.3. Conducting a timely and thorough PIR will help identify lessons learned which will assist in planning, managing, and meeting the objectives of future projects.