**XXXX IT Policies and Procedures**

**Document Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version/Revision | Description |
|  |  |  |  |

**Author Role Signature/Date**

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Reviewed By:**

**Name Role Signature/Date**

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Concurrence and Approvals**

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Signature/Date** |
|  |  |  |

### **Table of Contents**

[1. IT Governance Framework 7](#_Toc528827972)

[2. Applications Management 26](#_Toc528827973)

[3. Infrastructure Management 45](#_Toc528827974)

[4. IT Policy and Procedure Management 50](#_Toc528827975)

[5. Change Management 52](#_Toc528827976)

[6. Configuration Management 60](#_Toc528827977)

[7. Service Management Framework 62](#_Toc528827978)

[7.5.1 Overview 66](#_Toc528827979)

[7.5.2 Objectives 67](#_Toc528827980)

[7.5.3 Scope 67](#_Toc528827981)

[7.6 Reactive Availability Management Activities 67](#_Toc528827982)

[7.7 Proactive Availability Management Activities 67](#_Toc528827983)

[7.8 Availability Plan 68](#_Toc528827984)

[7.9 Availability Testing 68](#_Toc528827985)

[7.10 Risk Management 68](#_Toc528827986)

[7.11 Availability Reporting 68](#_Toc528827987)

[7.12 Activation Criteria and Procedures 68](#_Toc528827988)

[7.12.1 Incident Response 69](#_Toc528827989)

[7.12.2 Localized Activation 69](#_Toc528827990)

[7.13 Activation Procedure 69](#_Toc528827991)

[7.14 Service Continuity Requirements Management 69](#_Toc528827992)

[7.14.1 Activation Criteria and Procedures 69](#_Toc528827993)

[7.14.1.1 Incident Response 69](#_Toc528827994)

[7.14.1.2 Localized Activation 69](#_Toc528827995)

[7.15 Activation Procedure 70](#_Toc528827996)

[7.15 Roles and Responsibility for Service Continuity Process 70](#_Toc528827997)

[7.16 Roles and Responsibility for Availability Process 71](#_Toc528827998)

[8. Incident Management Framework 72](#_Toc528827999)

[9. Service Request Management Framework 76](#_Toc528828000)

[10. Problem Management Framework 77](#_Toc528828001)

[11. IT Device Naming Convention 81](#_Toc528828002)

[12. IT Backup Policy 83](#_Toc528828003)

[13. Collaboration Service: User Access Policy 90](#_Toc528828004)

[14. Service Level Management Framework 93](#_Toc528828005)

[15. Business Relationship Management Framework 95](#_Toc528828006)

[16. Service Complaints Management Framework 97](#_Toc528828007)

[APPENDIX 103](#_Toc528828008)

[A.1 Project Documentation Checklist 103](#_Toc528828009)

[A.2 Requirements Specification Template 104](#_Toc528828010)

[A.3 Functional & Technical Specification Template 108](#_Toc528828011)

[A.4 Test Script Template 110](#_Toc528828012)

[A.5 Change Request Template 111](#_Toc528828013)

[A.6 IT Service Business Impact Grid 114](#_Toc528828014)

[A.7 Change Request Priority Table 118](#_Toc528828015)

[A.8 Change Categories Guide 118](#_Toc528828016)

# 1. IT Governance Framework

#### 1.1 Introduction

In the 21st century, Information Technology lies at the core of all profitable organizations; this among other factors such as increased use of alternate transaction channels and social media has created new regulations and revisions of existing policies. This evolution and demand for more oversight globally means organizations can no longer afford to have IT governance by default or bad IT governance by design.

It is however, impossible to set the right context for IT governance without relating it to overall Enterprise Governance. The most comprehensive framework for Enterprise Governance is that defined by the Chartered Institute of Management Accountants (CIMA), which stipulates that there are two dimensions of Enterprise Governance: conformance and performance. In general, the conformance dimension is approached in the ex post (retrospective) view, while the performance dimension is approached in the ex-ante (prospective) view.

Corporate Governance, as the conformance dimension of Enterprise Governance, has had significant coverage following the various series of world scandals. The aftermath of such scandals has been new regulations globally to strengthen the role of Corporate Governance. Amongst such regulatory recommendations in most markets is that companies that are traded on open markets provide a coherent and descriptive statement covering the key elements of Corporate Governance rules and practices in their annual report and on their web site.

In direct terms Corporate Governance is the way in which business corporations are directed and controlled. It specifies the distribution and share of rights and responsibilities among different parts of the corporation, such as the board, management, shareholders and other stakeholders, spelling out the rules and procedures for making decisions on corporate affairs. By so doing, it provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance.

The importance of good Corporate Governance is recognized worldwide. It must lead to improved responsiveness to shareholder interest by attempting to balance the CEO’s power with the board’s ability to act as genuine custodians of the organization.

Business Governance, as the performance dimension of Enterprise Governance, focuses on the board’s role in making strategic decisions, risk assessment and understanding the drivers for business performance.

The attention to Corporate Governance also raises the question of whether the technology used for supporting business processes is adequately controlled. Because, technology is an integral part of business operations, IT Governance is consequently also an integral component of Corporate Governance.

#### 1.2 Objective

The objective of the XXXX IT Governance Framework is to provide an insight to the approach and standards adopted in the design of the governance framework.

When read with any other document referenced herein, an individual’s gets a very clear and concise view of how the IT department of the XXXX is run and controlled to ensure that all technology investments yield the maximum value/return on investment and all foreseeable risk are mitigated and ultimately meets all the requirements of the overall XXXX’s Enterprise Governance standards.

#### 1.3 Scope

The scope of this section of this policy document includes the definition of the term IT Governance, and the design and operating model of the IT Governance Framework of XXXX.

Its scope however does not include the documentation or design of the actual IT processes and policies, which however when referenced in conjunction with this document gives a more complete and balanced view of the effectiveness and quality of the XXXX’s IT Governance.

This Policy document will be reviewed once every year and sign off if there are changes during the review process.

**1.4 What is IT Governance?**

IT Governance has been defined in many ways, depending on the literature or publication being consulted:

* IT governance at its most basic is the process of making decisions about IT. By this simple definition, every organization has some form of IT governance. Good IT governance ensures that IT investments are optimized, aligned with business strategy, and delivering value within acceptable risk boundaries — considering culture, organizational structure, maturity, and strategy.
* IT Governance is a framework of decision processes and underlying accountabilities that align the management of the IT department to business objectives.
* This framework defines the leadership, roles, responsibilities and processes that align decision-making and performance measurement in the IT department with business strategies and direction.
* How IT decisions are made, sponsored, enforced and how the overall IT performance and IT investment outcomes are tracked
* IT Governance is the system by which IT within the enterprise is directed and controlled. The IT Governance structure specifies the distribution of rights and responsibilities among different participants, such as the board, business and IT managers, and spells out the rules and procedures for making decisions on IT. By doing this, it also provides structure through which the IT objectives are set, and the means of attaining those objectives and monitoring performance.

Table 1.1, below compares the most important characteristics of Corporate Governance,

Business Governance and IT Governance within Enterprise Governance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Corporate Governance** | | **Business Governance** | **IT Governance** | |
| Separation of ownership and control | | Direction and control of the business | Direction and control of IT | |
| Ex post | | Ex ante | Ex ante |  |
| * Duties of Directors/Leaders * Legislative/Fiduciary   Compliance & Control   * Shareholder Rights * Ethics & Integrity * Business Operations, Risks & Control | | * Business Goals & Objectives * Business Strategy & Planning * Business Activities & Processes * Innovation & Research capabilities * Knowledge & Intellectual Capital * Information & its Management | * IT Objectives * Alignment with   Objectives   * IT Resources * Information   Management   * IT Strategy & Planning | Enterprise  Knowledge |
| * Financial Accounting   Reporting   * Asset Management * Risk Management | & | * Human Resource Management * Customer Service & Relationships * In-and External Communication * Performance Control | * IT Acquisition & Implementation * IT Operations, Rights & Control * IT Asset Management * IT Risk Management | |

*Table 1.1 Governance characteristics*

Strong IT Governance will provide the mechanism for focusing IT on business alignment and investing in appropriate initiatives. It ensures that IT is properly organized and controlled, provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives.

IT Governance integrates and institutionalizes best practices of planning, organizing, acquiring, implementing, delivering, supporting, and monitoring IT performance, to ensure that the enterprise’s information and related technology support its business objectives. It enables the enterprise take full advantage of its information, thereby maximizing benefits and capitalizing on opportunities, thus leveraging competitive advantage.

Establishment of a Governance process drives significant value for the enterprise:

|  |  |
| --- | --- |
| **IT Value** | **Business Value** |
| * Clarifies the roles and responsibilities of IT and business leadership in delivering value from IT * Provides coordinating framework for key corporate IT management process * Focuses appropriate business unit   support for IT initiatives   * Ensures consistency of IT policies | * Ensures better alignment of the IT strategy with business objectives * Corporate priorities drive IT   investment and delivery   * Ensures strategic IT issues are resolved by appropriate cross-   functional leadership |

A key aspect of effective IT governance is direct linkage between business objectives and IT behaviors to support those objectives and the metrics to track realization. See illustration below:

|  |  |  |
| --- | --- | --- |
| **Objective** | **Behavior** | **Metric** |
| Deliver great customer service | Service, customer focused | Measured customer satisfaction |
| Stable and incremental improvement | Process excellence | System stability, availability |

#### 1.5 Governance Framework

IT is essential to manage transactions, information and knowledge necessary to initiate and sustain economic and social activities. These activities increasingly rely on globally cooperating entities to be successful. In many organizations, IT is fundamental to support, sustain and grow the business.

While many organizations recognize the potential benefits that technology can yield, the successful ones also understand and manage the risks associated with implementing new technologies. Among the enterprise's challenges and concerns are:

* Aligning IT strategy with the business strategy
* Cascading strategy and goals down into the enterprise
* Providing organizational structures that facilitate the implementation of strategy and goals
* Insisting that an IT control framework be adopted and implemented
* Measuring and optimizing IT's performance

Effective and timely measures aimed at addressing these top management concerns need to be promoted by the governance layer of an enterprise. Hence, the Board and Executive Management need to extend governance, already exercised over the enterprise, to IT by way of an effective IT governance framework that addresses strategic alignment, performance measurement, risk management, value delivery and resource management.

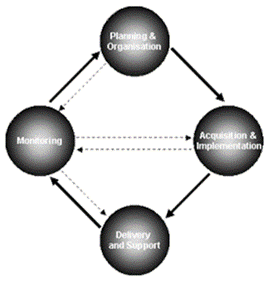
Simply put, IT governance and the effective application of an IT governance framework are the responsibilities of the board of directors and executive management. IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

IT governance framework and standards, such as Control Objectives for Information and related Technology (COBIT), the IT Infrastructure Library (ITIL) and IT Service Management (ISO 20000) can be critical elements in ensuring proper control and governance over information and the systems that create, store, manipulate and retrieve it.

 COBIT is a model for control of the Information Technology function. The model was originally developed by the Information System Audit and Control Foundation (ISACF®), the research institute for the Information System Audit and Control Association (ISACA®). In 2003 ISACF changed its name to the IT Governance Institute (ITGI®). Therefore, all marks formally held by the foundation are now held by the IT Governance Institute.

COBIT supports IT Governance by providing a comprehensive description of the control objectives for IT processes and by offering the possibility of examining the maturity of these processes**.**

It helps in understanding; assessing and managing the risks together with the benefits associated with information and related IT. COBIT provides an IT Governance instrument that allows managers to bridge the gap with respect to control requirements, Information Systems (IS) & Information Technology (IT) issues and business risks, to communicate that level of control to stakeholders. It enables the development of clear policy and good practice for the control of IT throughout organizations



#### Figure 1.2 COBIT Process Domains

For each of the domain a number of processes have been identified. These are listed in the table below:

|  |  |  |
| --- | --- | --- |
| **Planning & Organization (PO)**  This domain covers strategy and tactics and is concerned with the identification of the way IT can best contribute the achievement of business objectives. | | PO1: Define a Strategic IT Plan  PO2: Define the Information Architecture  PO3: Determine Technological Direction  PO4: Define the IT department & Relationships  PO5: Manage the IT Investment  PO6: Communicate Management Aims & Direction  PO7: Manage Human Resources  PO8: Ensure Compliance with External Requirements  PO9: Assess and Manage Risks  PO10: Manage Projects  PO11: Manage Quality |
| **Acquisition & Implementation (AL)**  In order to realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business processes. In addition to making sure that the life cycle is continued for existing systems, this domain covers changes in and maintenance of these systems. | | AL1: Identify Automated Solutions  AL2: Acquire & Maintain Application Software  AL3: Acquire & Maintain Technology Infrastructure  AL4: Develop & Maintain Procedure  AL5: Install & Accredit Systems  AL6: Manage Changes |
| **Delivery & Support (DS)**  This domain is concerned with the delivery of required services, which range from traditional operations over security and | | DS1: Define & Manage Service Levels  DS2: Manage Third-Party Services |
| continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the processing of data by application systems, which is classified under application controls. | often | DS3: Manage Performance & Capacity  DS4: Ensure Continuous Service  DS5: Ensure Systems Security  DS6: Identify & Allocate Costs  DS7: Educate & Train Users  DS8: Assist & Advise Customers  DS9: Manage the Configuration  DS10: Manage Problems & Incidents  DS11: Manage Data  DS12: Manage Facilities  DS13: Manage Operations |
| **Monitoring (M)**  All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses management oversight of the organization’s control process and independent assurance provided by internal and external audit or obtained from alternative sources. | | M1: Monitor the Processes  M2: Assess Internal Control Adequacy  M3: Obtain Independent Assurance  M4: Provide for Independent Audit |

 ITIL is a best practice framework for IT Service Management and is the de facto global standard in this area.

ITIL consists of a series of books giving best practice guidance for service management, with guidelines describing what rather than how. Service management is tailored to the size, the internal culture and the requirements of the company. An important focus is the provision of quality IT services

Best known ITIL books (figure 1.3) are the Service Support book which describes the Service Desk and the Incident Management, Problem Management, Configuration Management, Change Management and Release Management processes, and the Service Delivery book, which describes processes for Capacity Management, Financial Management for IT Services, Availability Management, Service Level Management and IT Service Continuity Management.

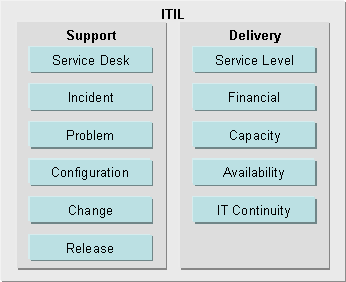


Figure 1.3

* ISO20000 is the International Organization for Standardization (ISO) standard for IT Service Management. This standard specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an IT Service Management System.

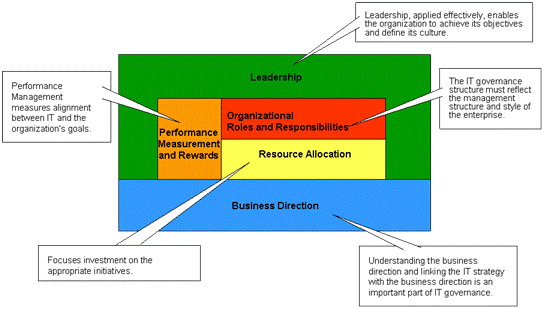
The requirements include the design, transition, delivery and improvement of services to fulfill agreed service requirements.

ISO20000 is the complimentary certifiable standard compatible with IT Service Management best practice (ITIL). It supports continual improvement and shows the organization’s commitment to delivering best practice in IT Service Management.

ISO20000 enables full over-sight in IT Governance and strategic direction within the organization.

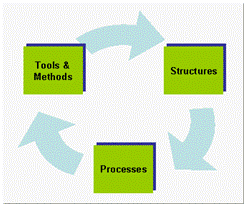
#### 1.6 XXXX IT Governance Framework

The IT Governance Framework to be adopted by XXXX is made of 5 key capabilities, Leadership, Business Direction, Organizational Roles & Responsibilities, Resource Allocation and Performance Measurement & Rewards. It incorporates and leverages both the COBIT and ITIL Governance framework standards, and is depicted by the schematic below:



#### Figure 1.4 XXXX IT Governance Framework

The XXXX IT Governance Framework will in turn be operationalized through three key components as shown below:



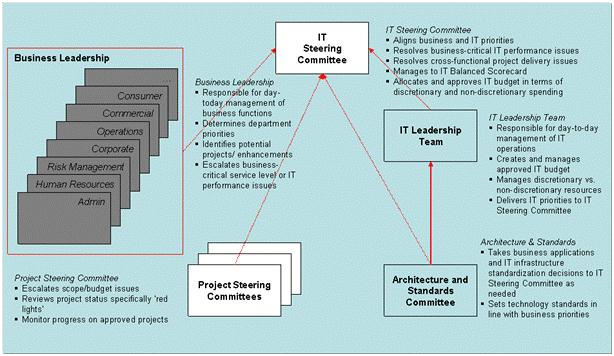
#### Figure 1.5: IT Governance Operational Model

The table below captures a summary of the IT Governance Framework:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Capability** | | **Key Attributes Addressed** | | **Operationalized** | |
| Leadership | | * Values-driven leadership (i.e., behaviors of leaders embody values of the firm) * Strong, commonly understood culture   focused on value creation   * Effective decision-making bodies (structure) and mechanisms | |  IT Governance Structure | |
| Business Direction | | * Clear business value creation focus * Specific guidelines on target markets (products and geographies), customers, and channels * Clear enterprise growth targets * Defined profitability objectives | |  IT Governance Processes | |
| Organizational Roles & responsibilities | | * Structure reflects business strategies * Responsibilities consistent with   accountabilities   * Execution effectiveness guaranteed by   standardized and institutionalized processes | |  IT Governance Processes | |
| Resource Allocation | | * Value creation is the primary driver to   prioritize IT initiatives   * Balanced long-term and short-term views * Joint IT/business prioritization processes * Clear guidelines on resource acquisitions * Comprehensive view of resources (across functions/organizational boundaries) * Effective measurement and tracking * Continuous feedback and adjustment | | * IT Governance Processes * IT Governance Tool Set | |
| Performance  Measurement  Rewards | and |      | Clearly understood mechanisms  Clearly established risk, reward, and performance criteria  Tight alignment with business objectives |    | IT Governance Processes  IT Governance Tool Set |

##### 1.6.1 IT Governance – Structures

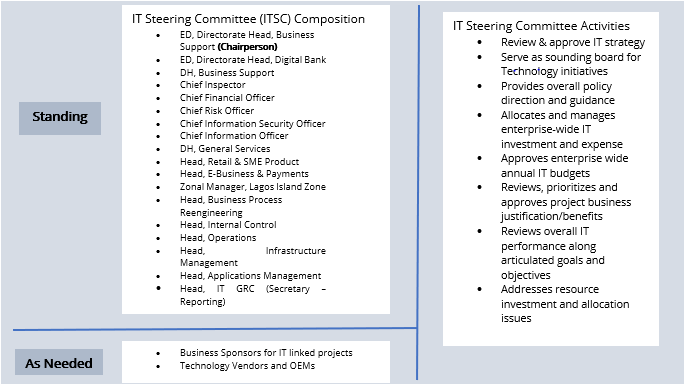
The IT Governance structures for XXXX will interact with business functions and IT functions, this is key to achieving a perfect fit and alignment between the XXXX’s business goals & objectives and IT objectives and initiatives. The schematic below depicts the proposed IT Governance Structures for the XXXX:



##### 1.6.2 IT Steering Committee

The schematic below captures the Proposed IT Steering Committee Participants and

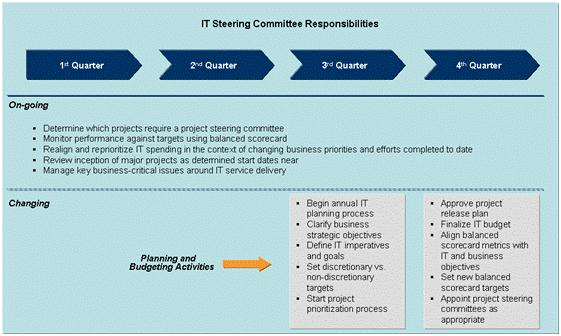
Responsibilities:



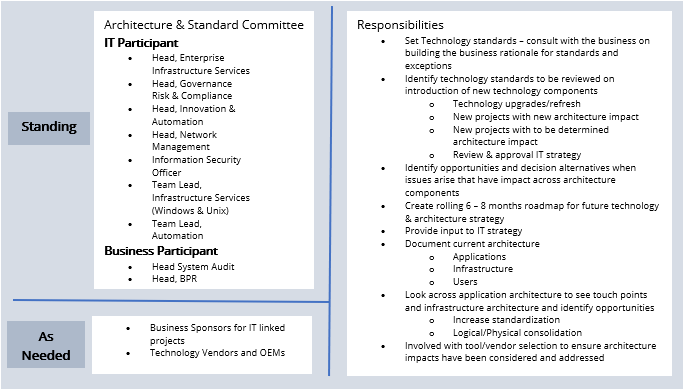
IT Steering Committee participants will have specific roles within the committee to ensure achievement of their charter as shown in the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Participants** | | **Role** | **Highlights** | |
| ED, Directorate Head, Business Support | - | Committee  Chairman | * Provides overall policy direction and guidance * Develops overarching business direction and objectives * Accountable for ensuring alignment of IT SC outcomes with business direction and objectives * Ultimate decision authority for cross-function business and IT issues that cannot be resolved by lower decision-making bodies | |
| CFO |  | Finance Lead | * Reviews IT budget prior to IT SC approval * Drives the budgeting process * Sets IT spending and capital constraints | |
| ED Directorate Head, Digital XXXX  Chief Inspector  DH, Business Support  DH, Retail & SME Product  DH, General Services  Head, E-Business Payments  Head, Internal Control  Head, Operations  Head, Business Process Reengineering  Zonal Manager, Lagos  & Island Zone    Chief Risk Officer | | Business  Representation | * Clarify specific BU strategies and tactics * Ensure IT agenda aligns with and enables articulated business goals * Presents list of potential capabilities and IT projects to ITSC for review * Alerts ITSC to business-critical IT performance issues * Raise relevant legal and regulatory issues | |
| Chief Information Security Officer | | Information Security Control |  | * Confidentiality this means considers what needs to be done to ensure sensitive data and information stays private. * Integrity is focused on the life cycle of the data and ensuring that it is always accurate. * Availability means that your hardware and software systems have constant uptime and that everything is maintained properly. |
| Chief Information Officer  Head Enterprise Infrastructure Services  Head Automation & innovation  Head, IT Governance Risk & Compliance | | IT Operations |  | * Responsible for effective and efficient delivery of IT services * Accountable for IT operational results * Manages approved projects * Delivers IT priorities to ITSC |
| IT Governance Risk & Compliance | | IT Strategy |  | * Determines IT implications of near- and long-term business strategies |
|  | |  |  | * Scans market place for relevant new technologies and informs ITSC |
|  | |  |  | * Sets and enforces overall IT standards |
|  | |  |  | * Ensures IT initiatives and new IT capabilities align with existing architecture standards |

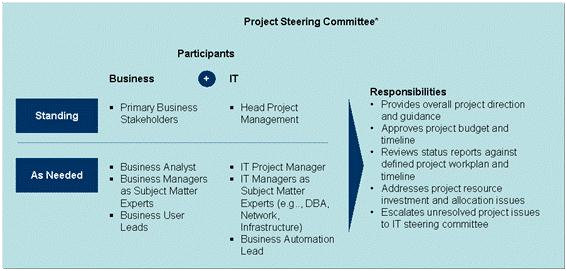
The IT Steering Committee responsibilities and corresponding meeting agendas will change throughout the fiscal year, but the schematic below shows a generic guideline for the affairs of the committee for a whole year:



Below are the identified participants and responsibilities of the Architecture and Standards Committee:



Whilst below is a typical listing of participants and responsibilities of a Project Steering Committee. [At the discretion of the IT steering committee, depending on scope, project steering committees will be created for approved typical projects or capability releases. Primary business stakeholders will be selected based on project scope].



\* Project Steering Committee is an Ad-hoc Committee setup based on need.

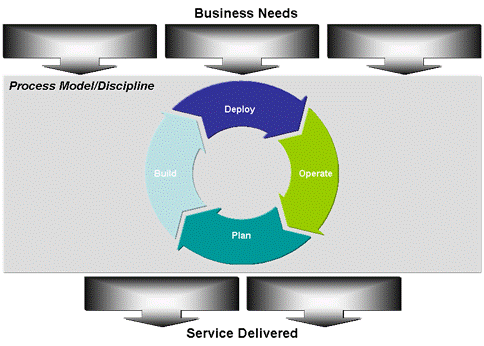
##### 1.6.3 IT Governance – Processes

Today’s business environment places increasing demands (rapid change, financial constraints, security and reliability concerns, global interconnectedness) on IT departments in order to meet the expanding needs of a wide variety of stakeholders.

In delivering an effective portfolio of IT services to the business, IT operations and project teams must focus on three key objectives:

* Understand the business and operational needs for the service and create a solution that delivers these within the specified constraints
* Effectively and efficiently deploy the solution to users with as little disruption to the business as the service levels specify
* Operate the solution with excellence in order to deliver a service that the business trusts

The process component of the XXXX IT Governance Framework will be driven by the model depicted in the schematic below:



The logic of the above figure is that once business needs have been well articulated and prioritized and used to pick IT initiatives; if passed through this process excellence model, superior service will continuously be delivered.

The process model above leverages the two standards on which the XXXX IT Governance Framework is built; COBIT and ITIL. The table below shows the mapping of the above the domains of both COBIT and ITIL process framework:

|  |  |  |
| --- | --- | --- |
| **XXXX IT Process Model** | **COBIT** | **ITIL** |
| Plan | Planning & Organization | Service Strategy |
| Build | Acquisition & Implementation | Service Design |
| Deploy | Delivery & Support (DS) | Service Transition  Service Operation & Continual Service Improvement |
| Operate | Monitoring (M) |

##### 1.6.4 IT Governance – Tools & Methods

The XXXX’s IT Governance Framework will utilize two basic tools & Methods for it to be effective and continually improving:

* A tailored IT Balanced Scorecard
* Decision Criteria

###### 1.6.4.1 IT Balanced Scorecard

A Balanced Scorecard directs one to look at performance from four equally important perspectives. It supplements traditional financial measures with three additional perspectives –Client/Customer Value, Growth, and Operational Excellence. And emphasizes balance across multiple dimensions of performance so that good performance in one area is not offset by poor performance elsewhere

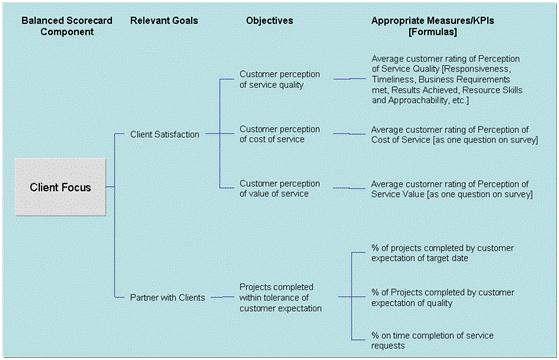
For our purpose, a tailored balanced score card that allows for a balanced view and measurement of the IT department is what is required. Measuring its compliance with standards, pro-activeness in mitigating risk, its ability to guarantee seamless continuous service availability, and ultimately its ability to exceed expectations of all its stakeholders – external customers, internal customers, regulatory authority, auditors (internal & external), management, board and shareholders in general.

The schematic below presents the tailored scorecard to be applied to the IT department as part of the operationalization/execution of the XXXX IT Governance Framework:

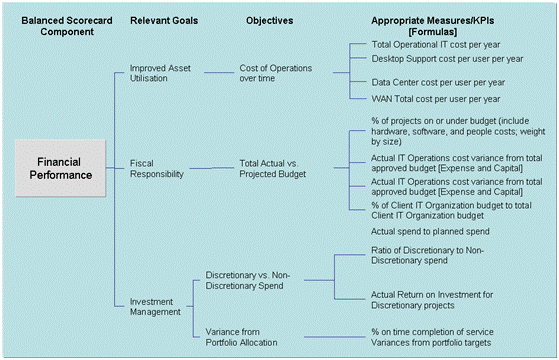


Whilst as identified in the guidelines for the running of the affairs of the IT Steering Committee, balanced scorecard targets shall be moving targets. The new couple of diagrams present a baseline for future updates:

1.6.4.1.1 Balanced Scorecard –Client Focus Component

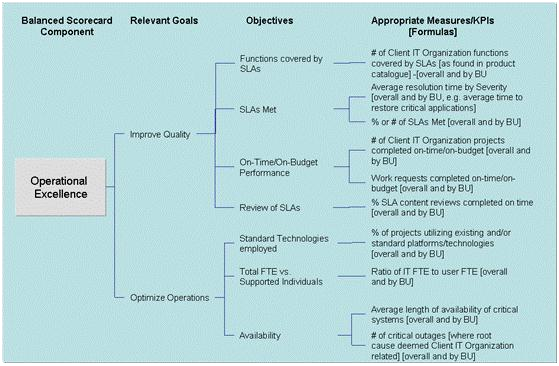
Goals, objectives, and measures/KPIs are identified for the Customer Focus component of the tailored Balance Scorecard to serve as a baseline as shown in the schematic below: 

1.6.4.1.2 Balanced Scorecard –Financial Performance Component

Goals, objectives, and measures/KPIs have been identified for the Financial Performance portion of the tailored Balance Scorecard to serve as a baseline as shown in the schematic below: 

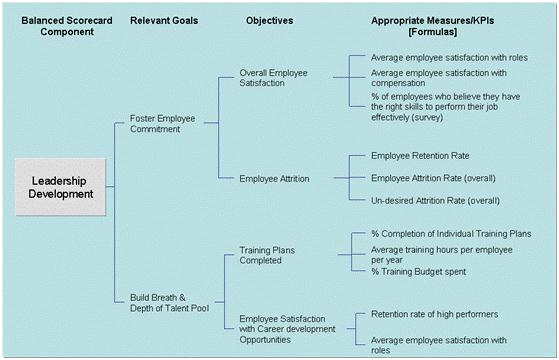
1.6.4.1.3 Balanced Scorecard – Operational Excellence Component

Goals, objectives, and measures/KPIs have been identified for the Operational Excellence component of the tailored Balance Scorecard to serve as a baseline as shown in the schematic below:



1.6.4.1.4 Balanced Scorecard – Leadership Development Component

Goals, objectives, and measures/KPIs have been identified for the Leadership Development component of the tailored Balance Scorecard to serve as a baseline as shown in the schematic below:



###### 1.6.4.2 Decision Criteria

A disciplined Demand Management/Prioritization process and accepted prioritization criterion focuses IT investments on high value and priority projects.

Key benefits of effective and efficient decisioning criteria include:

* Maximize business value generated by investments in information technology
* Reduce or eliminate spending on information technology initiatives that are not aligned with the business priorities
* Reduce or eliminate spending on redundant and/or overlapping systems across functions and regions
* Prioritize investments based on business value creation
* Develop enterprise-wide agreement on major IT investment priorities
* Manage demand for key IT resources more effectively

Increase accountability for and build organizational commitment to realizing business results from IT investments

* Generic guidelines for prioritizing initiatives include:
  + Prioritization criteria should be based on strategic, financial, organizational priorities and balanced against risk
  + Prioritization criteria and project evaluation guidelines should be well defined, documented and communicated
  + Accountability for accuracy of initiative estimates and realization of planned benefits should be built into the process
* The steps recommended as part of the IT Governance Framework standard for deciding on which initiatives to kick-start/prioritize are (assumption is all initiatives have passed through the filtering process of the review of the IT Strategy):
* Confirm business merit, strategic alignment and risk
* Force rank on scoring
* Review initiatives against resource constraints
* Finalize adjustments to meet goals and targets
* Recommend Project Sequencing

# 2. Applications Management

#### Overview

This addresses the control over the IT process of procuring and developing automated solutions that satisfy the business requirement of ensuring an effective and efficient approach to satisfy the XXXX’s customers.

It is also supported by an objective and clear identification and analysis of the alternative possibilities and measured against business requirements and takes into consideration

* Knowledge of solutions available in the market
* Acquisition and implementation methodologies
* Required user involvement and buy in
* Available development resources
* Alignment with Enterprise IT Architecture
* Integration with heterogeneous systems
* Minimum application requirements (developed or custom made)
* Data storage and information sharing requirements definition
* Feasibility study (costs, benefits, alternatives, etc.)
* Functionality, operability, acceptability and sustainability requirements
* Cost-effective security and control
* Supplier responsibilities and support

#### 2.1 Application Acquisition and Development

##### 2.1.1 Policy Statement

*IT shall at all points in time adopt the most a system development methodology which best fits to the overall cultures, standards and expectations of our customers and this methodology shall govern the process of developing, acquiring, implementing and maintaining computerized information systems and related technology.*

##### 2.1.2 Development Methodology Standard

The chosen system development methodology shall

* Be appropriate for the systems to be developed, acquired, implemented and maintained
* Provide standards covering test requirements, verification, documentation and retention for testing individual software units that interface with the XXXXing application as part of every information system development or modification project.
* Require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g., user ID’s and passwords) against discovery and misuse.
* In the event of major changes to the XXXX’s existing information technology, management shall ensure that this system development methodology is observed, as in the case of the acquisition or development of new technology.
* Provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.
* Provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.
* Provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.
* Provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.
* The XXXX’s system development methodology shall provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.
* Ensure that security is built into applications forming a business requirement for systems to be acquired.

##### 2.1.3 PROCEDURE 1: Application Development Framework

* Project Definition:

o A project will be initiated by a project manager, sponsor or user by requesting for a service or product

o Each project shall be defined and documented in a project charter or notes

* Requirements Definition
* A requirements definition will be jointly undertaken by Users of the technology and the technology group.
  + - The User Requirements definition will be drawn up and documented and will form development details from the customer perspective; specific requirements desired, expected business benefits, value proposition, detailed functionality and reports and development details from an IT perspective documenting functional requirements, application architecture, presentation and project scope. Refer to the Appendix for a Requirements Specification template
    - There should be risk assessment and mitigation measures documented by Operational Risk Management team in every Project Initiation Document.
    - The requirements specification document is signed off by the project manager, sponsor and a representative of IT.
    - The approved requirement specification document serves as the Project Initiation Document (PID). The PID will be circulated for sign off by the requesting unit.

This document will be referenced from the beginning to the end of the project and shall form the basis of development

* Feasibility Analysis
  + A feasibility analysis depending on the scope of the project will be performed from a technical and functional perspective.
  + This analysis will include a comparison of available options and a decision on if to custom build a solution or procure an off the shelf application. The functional/business feasibility analysis will include
    - * Total Cost Impact
      * Impact on existing Business Process and Process requirements
      * Required Standard Operating Procedures
      * Who is to have access to the application, and what infrastructure investment is required to deliver the solution to them.
      * Can the solution be easily extended to additional business units of external stakeholders
      * Training required for the application
      * Does a similar solution exist within the Enterprise and can it be customized for this need.
  + The Technical feasibility will include an analysis of:
    - * Hardware and software requirements
      * Development platform
      * Database platform
      * Connectivity between client and server
      * Software architecture (e.g. 2-tier (fat client) or n-tier (thin client with middleware) Client/Server, Web-based development
* Project Mandate
  + Each project requiring specific development (software programming) to meet a line function or staff function need will require the concurrence of the Head, IT
* Systems Design and Development
  + System design will be the responsibility of the application development team within the technology group of the XXXX, but must be in line with pre-defined standards and methodologies.
  + The developers must understand the business environment and processes. Training should be provided if there is a knowledge gap

It is also important to asses existing processes and procedures that support the system in development to make sure that these are optimized.

* + At the end development, a test release plan should be produced in conjunction with the business.
  + A Technical Specification should be produced.
  + A training plan should be produced along with end user manuals and/or job cards where applicable. Refer to Appendix for complete project documentation checklist.
  + Control measures and procedures for the protection of programs and data shall be built in, tested and audited to ensure that data and programs cannot be changed (amended/updated) without authorization, destroyed or subjected to sabotage and/or espionage due to negligence or on purpose.
  + Collaboration should occur during the project between the developer and project stakeholders to reduce iterative cycle times and provide more insight into business needs and also reduce the required learning curve on the side of the user.
  + Design changes should be implemented immediately, so as to manage the deviation and the magnitude/importance of the change.
  + All changes should be coded, tested and deployed immediately.
  + All Applications developed must go through the software quality assurance stage as stated in the application security standards 2.0 which must be satisfactorily tested to an acceptable level of risk (if fundamental system functionalities exist) by the testing team and approved by the Head of Quality Assurance/Test or his/her delegation before calling for UAT.
  + All applications developed/modified must go through Team Foundation Server and subsequently no developer must be able to access the build version after development.
  + All Deployment must be done through the Team Foundation Server
  + Where a completed module can be deployed for demonstration purposes, it should be. This allows the users to interact with the application at the earliest possible opportunity.
  + When developing reports the users should be involved in the design of the reports, keep in mind that a group of users will only interact with the application via the reports. They should be self-explanatory and easy to use.
  + Reports should be accessible in real-time over the Corporate Intranet, and should be server-based.
  + Except in those cases where the security features of the operating system are required as an additional measure, security for the application should be built into the application itself.
  + Facilities to update the application settings and data should be built into the application itself. All applications should be web based and centrally controlled and updated.
  + Application change control will be managed using IT change request forms to be filled in by the user, and counter-signed by the user’s line manager and coordinated through IT Architecture and Strategy
* Commercial Off-The-Shelf Purchase (COTS)
  + COTS shall be considered to meet customer requirements after the options of in house development by the application development team or the option of contract application programming
  + In such a case IT management, will issue a tender for contract software development based on the standards set by the XXXX.

Development methods for contractors should follow the general guidelines detailed in “Systems Design and Development”

* Contract Application Programming
  + Contract Application Programming will only be considered once technology group cannot provide the application development service or are unable to deliver the service in the required time frame. And that there are no cost-effective COTS that will meet the customer needs
  + In such a case IT management, will issue a tender for contract software development based on the standards set by the XXXX.
  + Development methods for contractors should follow the general guidelines detailed in “Systems Design and Development”
* System / Program Testing
  + Before acceptance of a system, an audit of the set control and security measures shall be done by IS Control who must oversee the implementation of all controls during development of the system. All security audit actions shall be documented. The testing of the security measures shall be continued during the system life cycle to ensure that the security objectives are met and that controls operate as intended.
  + All emergency maintenance programs (e.g. backdoors) shall be removed before a system is installed. Systems shall be audited before installation and implementation.
  + System and program testing is undertaken by the application testing and quality assurance team in conjunction with selected officials of the user group.
  + No application / program / module will be released for production purposes until signed off by the Head, Applications Management as error-free. o The results of the test must be documented and retained with IS Control
* Conversion Planning and Parallel Testing
  + Where applications / modules are to be converted, the user department and the development team will plan, agree on and document the conversion process.
  + Once conversion development is complete the development team will test the application using data copied from the live system. Where possible, parallel testing will be undertaken, but only where sufficient human resources exist to do so.
* Final Acceptance and Post Implementation Review
  + Following the successful deployment of an application or module, a post implementation review will be held one month after the successful deployment in order to finalize the project
  + **Step 1: Review the project performance**
* To start, we need to determine how the project performed against each of the targets defined during the Initiation phase. We should identify whether the project:
* Delivered the business benefits in the Business Case Requirement as contained in the Project Initiation Document (PID)
* Achieved the objectives specified in the Project Initiation Document (PID)
* Remained within the scope defined in the Project Initiation Document (PID)
* Produced the deliverables as contained in the Project Initiation Document (PID)
* Met the quality targets defined in the Quality Plan in the Project Initiation Document (PID)
* Completed within the planned project schedule

**Step 2: Review the project conformance**

Next, identify the extent to which the project has conformed to the following management processes initially defined:

* Time Management
* Cost Management
* Quality Management
* Change Management
* Risk Management
* Issue Management
* **Step 3: Identify project achievements**

Next, list the major achievements for the project and describe the positive effect that each achievement has had on the customer’s business.

* **Step 4: Identify project failures**

List any project failures and describe the effects they have had on the customer’s organization.

* **Step 5: Identify lessons learned**

Describe the lessons learned from undertaking this project and list any recommendations for similar projects in the future.

* All changes or alterations to the application will then be processed in line with the Change Control Policy.
* Systems Documentation.

o Refer to the Appendix for complete documentation checklist

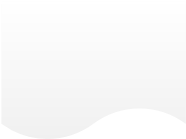
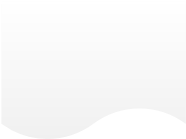
#### 2.2 Portfolio Management

##### 2.2.1 Policy Statement

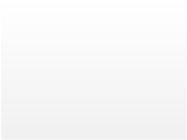
*The Business Automation team shall deliver all projects within agreed timelines and to business specifications and agreed development methodology.*

##### 2.2.2 Request Management Process

All projects initiation from within or outside the IT department are approved and managed using the defined business process flow which ensures requests are duly documented and approved. Information on expected due diligence and documentation required for project initiation and approval is outlined in the project documentation checklist (Refer to Appendix)



**User Request**



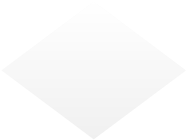
**Request**

**complete**

**documentation**

**and Supervisor**

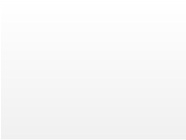
**Approval**



**Document**

**complete**

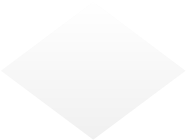
**?**



**Filter request**

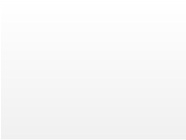
**through**

**selection criteria**



**High Priority**

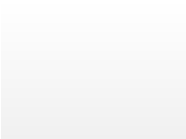
**?**



**Pipeline and**

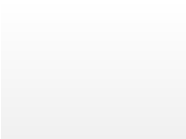
**Schedule for**

**Later Date**



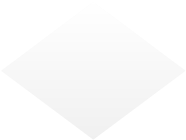
**Resource**

**Yes**



**Start**

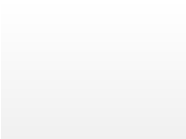
**Development**



**Take on**

**request**

**?**



**Weekly Portfolio**

**Review**

**No**

**Yes**

**Yes**

**No**

**No**

Figure 2.1: Request Management Workflow

##### 2.2.3 Selection Criteria

Requests will be approved and prioritized based on the following selection criteria.

* Direct Financial Impact
  + - Does the request have direct financial impact on the XXXX as a whole and can this be measured in terms of increased revenue or reduced costs?
    - Each high priority request must be justifiable in terms of fiscal benefits while holistically factoring in potential investments required to achieve the automation in terms of infrastructure procurement or resourcing.
* Direct Customer Service Impact
  + Does the request have direct impact on customer service in terms of new or existing product or service delivery or improvement?
  + Customer service directly and indirectly translates to fiscal benefits for the XXXX so projects which have direct significant impact on customer service delivery through any of our service outlets is considered high priority subject to other projects which are currently pipelined.
* Regulatory Requirements o Is the request based on regulatory requirements?

o Requests which are made based on the need for compliance to regulatory requirements are classified as high priority based on available timelines or deadlines from the regulatory body.

* Exceptions
  + This applies to requests which do not fall into any of the listed categories but based on business exigencies need to be prioritized.
  + Requests in this category will be handled based on available resources locally or using contract application programming Contract Application Programming

##### 2.2.4 Billing

All requests will be billed based on the following parameters

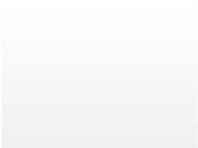
* Effort to Complete
  + The number of days and staff required from the development team and the IT department to complete the project.
  + The estimated cost per day for effort to complete is determined by the industry average obtainable for development skills moderated by the remuneration model within XXXX for the grade band of each development and IT management roles.
* Skill Requirements
  + The level of complexity and scope of the project will determine the grade and skill level of the developer(s) assigned and the number of developers assigned.
  + In addition, the scope of the project will determine if any supervisory and project management skills are required. All these factors largely impact on the overall cost of the delivering on the request.
* Infrastructure Requirements
  + This refers to all required hardware and software infrastructure ranging from Servers to Software, Operating systems or Drivers.
* Standard Billing Template

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **# Working Days** | **Developer** | **Senior Developer** | **Lead Developer** | **IT Project Mgt** | **Total** |
| 5 |  |  | X |  |  |
| 10 | X |  |  | X |  |
| 15 |  |  |  |  |  |
| 20 |  |  |  |  |  |
| 25 |  |  |  |  |  |
| **Resourcing Total** | |  |  |  |  |
| **Infrastructure** | **Model** | **Quantity** | **Purpose** | **Unit Price** | **Total** |
| Server |  |  |  |  |  |
| Desktop |  |  |  |  |  |
| Laptop |  |  |  |  |  |
| Printer |  |  |  |  |  |
| Software/Driver |  |  |  |  |  |
| Modem |  |  |  |  |  |
| Routers |  |  |  |  |  |
| Switch |  |  |  |  |  |
| Others |  |  |  |  |  |
| **Infrastructure Total** | |  |  |  |  |
| **Grand Total** | |  |  |  |  |

##### 2.2.5 Pipeline Management

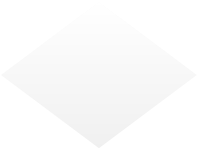
Project requests are initiated and managed using a development pipeline based in project priority, impact, scope and available resources.

Pipeline Process Flow

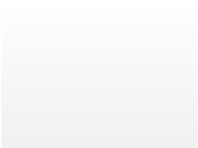


**Approved**

**Request**



**High Priority**

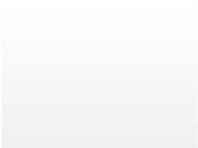


**Development**

**/**

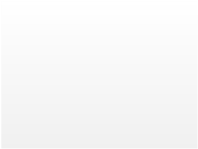
**Work In**

**Progress**

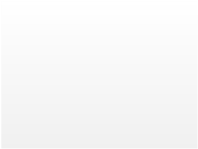


**User Acceptance**

**Testing**

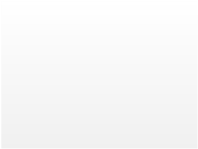


**Deploy**



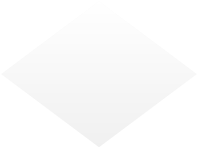
**Queue for Later**

**Date**



**Weekly Portfolio**

**Review**



**Take On**

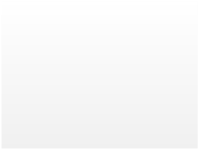
**?**

**Yes**

**No**

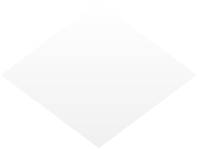
**Yes**

**No**

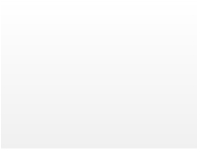


**Request for**

**Change**

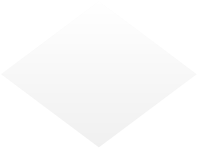


**Modifications**



**Review and**

**define Priority**



**Show**

**Stopper**

**?**

**Yes**

**No**

**No**

**Yes**

##### 2.2.6 Periodic Portfolio Review

On a periodic basis, all on-going projects, pending projects or projects put on are reviewed to analyze compliance to set timelines for delivery, review pending requests vis-à-vis available resources and determine which requests should be taken on next.

Selected requests are then moved into development to become work in progress based on resourcing availability or priority.

For reporting purposes, all requests will be identified using the following identifiers

* Open
  + Projects which are in development and for which definite timelines have been

communicated.

* User Acceptance Testing o Projects for which development has been concluded and is ready for UAT
* Change Request
  + Projects for which change requests have been formally made and are

undergoing modification.

* Closed o Projects which have been developed, tested and successfully deployed
* Pending o Projects which have been approved and scheduled to begin later
* On Hold
  + Projects which were reprioritized based on changed user or business needs. Requests which fall in this category after a portfolio review can be reclassified as “Open” or terminated.
* Terminated
  + Projects for which the business need no longer exists. Requests in this category will not be pipelined and can only be re-initiated.

#### 2.3 Updating the System Development Methodology

##### 2.3.1 Policy Statement

*Management shall implement a periodic review of its system development methodology to ensure that its provisions reflect current generally accepted techniques and procedures.*

##### 2.3.2 PRODECURE 2: Updating the Software Development Lifecycle

* Change Request will be made from the IT Architecture and Strategy Unit in conjunction with the Business Automation team
* The request will be analyzed and approved by the Head, IT
* Changes will be made to the framework and policy documents updated accordingly.
* Documented changes will be duly communicated to all affected parties.

#### 2.4 User Reference and Support Materials

##### 2.4.1 Policy Statement

*IT Management must ensure that adequate user reference and support manuals for all applications developed and acquired are prepared and available for use preferably in electronic format.*

#### 2.5 Software Selection and Acquisition

##### 2.5.1 Policy Statement

*Management shall ensure that all application acquisition done within the Enterprise are done with the input of the IT Department and confirm to documented technology guiding principles in the IT Strategy.*

##### 2.5.2 Software Selection Guiding Principles/Standards

Technology guiding principles

|  |  |
| --- | --- |
| **Guiding Principle** | **Decision** |
| IT Investment Perspective | •XXXX will adopt an IT Value Model that is driven by real business needs and value realizable by the organization (as against cost incurred)  •Business application investment at XXXX will be business led with proper business justification, and with support from the IT function  •IT Infrastructure investment at XXXX will be made at the enterprise  level |
| Technology Position | •Technology will be viewed as a business enabler; thus XXXX will seek to quickly deploy all tested and proven technology.  •Always seeking a first adopter and industry leadership advantage – where reasonable  •XXXX will deploy and manage Infrastructure that is robust, scalable, and will enable significant value creation |
| IT Resource Distribution | •XXXX will centralize the operation of its enterprise applications. |
|  | •XXXX will support high value-added operations in-house and will seek to out-source non-core operations.  •Application development will be primarily outsourced to reputable development organizations whilst IMS will build minimal capabilities to enhance core applications |
| IT Processing Distribution | •XXXX Administrative/Operations processes will be centralized  •XXXX transactional data will reside centrally |

##### 2.5.3 PROCEDURE 3: Software Selection and Acquisition

* Critical Assessment
  + IT management shall assess the XXXX’s critical success factors e.g. effective cost control, delightful customer service, operational excellence, governance, or responsiveness to customers and then decide how the IT can drive these
  + Consider critical functional requirements which must be captured at the requirements definition stage of the software development methodology. These needs should include provisions for security.
  + The functional needs will be included in the RFP and sent out to vendors
  + Vendors will be screened based on pre-defined vendor selection criteria
* Demonstration Phase

o All affected stakeholders shall be involved in the selection process.

* + On-Site demonstration is preferable
  + Only shortlisted vendors will be given the opportunity to demonstrate the product
* Selection
  + The results of the selection process shall be presented to the IT Steering Committee, the MD and the board through the program management office.
* Acquisition

o The IT steering committee will append recommendations for purchase.

o Purchase of software shall be done centrally and managed by the IT Department

* Implementation

o All implementation must be certified by the IS Control unit

#### 2.6 Application Security Considerations

##### 2.6.1 Policy Statement

*IT management shall seriously consider security in the development and choice of application.*

##### 2.6.2 Security Standards

* All security requirements and considerations, including the need for fallback arrangements, shall be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system. The business case should also detail the deliverables, possible risks and information on how the risks will be mitigated. These deliverables will be used to measure the performance of the project.
* Where software development is outsourced, the following security points should be considered:

o Licensing arrangements, code ownership and intellectual property rights

o Certification of the quality and accuracy of the work carried out

o Rights of access for audit of the quality and accuracy of work done

o Testing before installation to detect malicious code.

#### 2.7 Contract Application Programming

##### 2.7.1 Policy Statement

*The provision that the procurement of contract programming services must be justified with a written request for services from the Head, IT*

##### 2.7.2 Contract Application Programming Standards

* The contract must stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance.
* In addition, IT shall require that the end products of completed contract programming services be tested and reviewed according to the related standards by the IT function and other concerned parties (such as users, project managers, etc.) before payment for the work and approval of the end product.
* Testing to be included in contract specifications should consist of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the entire system to avoid unexpected system failure.

##### 2.7.3 PROCEDURE 3: Contract Application Programming

* After the decision to award contract for programming RFPs will be sent out to contract application developers
* Vendors will be screened by pre-defined criteria and choice is made
* The contract is then awarded by the appropriate unit in Human Capital Management advising vendor to follow stated development methodology

#### 2.8 Assessment of New Software

##### 2.8.1 Policy Statement

*IT Management must ensure that all newly purchased software are assessed for impact and integration to the Enterprise IT Architecture*

##### 2.8.2 Software Assessment Standards

* Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.
* The Assessment shall include

o Performance and computer capacity requirements

o Error recovery and restart procedures, and contingency plans

o Agreed set of security controls in place

o Effective manual procedures o Business continuity arrangements

* Evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end
  + Evidence that consideration has been given to the effect the new system has on the overall security of the organization
  + Training in the operation or use of new systems.

#### 2.9 Application Testing and Quality Assurance

##### 2.9.1 Policy Statement

IT Management must ensure that all newly purchased software is tested for compatibility and assessed for compatibility with existing systems and Enterprise IT Architecture

##### 2.9.2 Application Testing Standards

* Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.
* All software testing shall be done on a test server before actual deployment to production

#### 2.10 Software License Management

##### 2.10.1 Policy Statement

*IT Management must ensure that all newly purchased software and all software used within the Enterprise Network is adequately licensed.*

##### 2.10.2 Software License Standards

* It is the XXXX’s policy not to allow copying or use of unlicensed software within the XXXX
* All software packages that do not require specific licenses (such as shareware, freeware, etc.) must be accompanied by supporting documentation certifying same
* Each staff is individually responsible for adhering to all licenses, notices and agreements in connection with software which he or she acquires copies, transmits or uses.
* The IT support function will not be extended to equipment that have illegally acquired software
* IS audit shall annually review all software on systems for adequate licensing
* XXXX employees learning of any misuse of software or related documentation within the XXXX shall notify the technology group and IS control unit immediately.

Duplication of copyrighted software should only be for backup or archival purposes.

##### 2.10.3 Software License Guidelines

* The unauthorized copying or use of copyrighted software can expose the XXXX to significant risks by damaging the XXXX’s reputation in the market place, risks of litigation against the organization and even risks of criminal penalties against individual officers and staff.
* Manufacturers and distributors of software are aggressively protecting their rights and interests in their products. Users of illicit copies are prosecuted to the full extent that the law allows, and penalties can be grave for each offence.
* The software user should follow the one software package/one computer rule or when available the user should follow the licensing agreement with the software provider. This means that an equivalent number of software packages/license should be purchased for every piece of hardware on which the software is used or stored on.
* XXXX recognizes that software theft is an illegal and a criminal act and thus strives to ensure that all software in use within the XXXX are legally obtained and is covered by a software license and corresponding agreement.
* Each employee should understand that use of unlicensed software is illegal, against XXXX’s policy, and subject to strict disciplinary procedures including dismissal. It is the responsibility of the User to ensure that all software installed on his/her PC is licensed.

##### 2.10.4 PROCEDURE 6: Software License Review

* Carry out an inventory of all software licenses or installation CDs held within the XXXX.
* Use System Center Configuration Manager to verify the applications installed all machines on the network and raise any exceptions discovered
* Conduct a review on a periodic basis

#### 2.11 Application Release

##### 2.11.1 Policy Statement

*An implementation and release plan must be prepared, reviewed and approved by IT affected stakeholders.*

##### 2.11.2 Release Plan Guidelines

The implementation plan should address areas like infrastructure acquisition (when needed) and installation, user training, installation of operating software changes, implementation of operating procedures and data conversion (where applicable).

* All releases for the production rollout is only approved and implemented following successful testing of releases. Issues of new releases must be closely coordinated with customers and users as well as IT operating staff. It is imperative that the varying expectations be skilfully managed in order to avoid potential irregularities following deployment.
* A release schedule is maintained for all software releases or patches. This will set out details of the releases to be deployed.

#### 2.12 System and Data Conversion

##### 2.12.1 Policy Statement

*IT Management must ensure that, as part of every application development or modification, all necessary elements from the legacy system are converted to the new one according to a pre-established plan.*

##### 2.12.2 Data Conversion Standards

* Tests to be performed must include comparison of database structures, static data and overall compatibility of legacy data with the new system.
* The conversion plan should include details about methods of collecting and verifying the data to be converted and identifying and resolving any errors found during conversion.

#### 2.13 Enterprise Software Installation

##### 2.13.1 Policy Statement

*Enterprise Servers and Desktop shall ensure that all applications are accurately installed and validated.*

##### 2.13.2 Software Installation Standards

All system software installation must be done to pre-defined specification as determined by Enterprise Servers and Desktop.

##### 2.13.3 PROCEDURE 11: System Software Installation

* On procurement of any new infrastructure asset, the asset is configured to a predefined standard as specified by the owning unit (Enterprise Servers and Desktop, Network and Communications, Power and Telecoms)
* For applications installed on laptops and desktops, media is retrieved from Head,

Enterprise Servers and Desktop and sign off on possession

* Install using configuration baselines specifications
* Configure system following the standard configurations Test system for ideal functionality

#### 2.14 System Software Maintenance – Update & Upgrade

##### 2.14.1 Policy Statement

*All enterprise wide upgrades (new versions, patches etc.) shall be initiated and managed centrally by the IT Group.*

##### 2.14.2 System Software Maintenance Standard

* System software changes must be in line with the XXXX’s change management procedures.
* System software shall never be upgraded or changed without the formal advice of the software vendor
* All changes will be carried out according to defined change control procedures.
* All software requisitions can only be done through the IT Service Desk
* All patches should be tested in a lab environment to ensure no adverse effect or impact on system performance or security before deployment enterprise-wide

##### 2.14.3 PROCEDURE 12: Upgrading / Updating System Software

* Request

o A request must be formally made to IT via IT Service Desk

* + If the affected application is a third-party application, the vendor will be contacted
  + If the software is an operating system, the request will be analyzed by the Enterprise Servers and Desktop team
  + The request must be accompanied with a justification report and how the planned update is in line with business objectives
* Approval

o The request must be approved by the Chief Technology Officer (CTO) or a designate

* + If approved, the request is forwarded to the owning team for execution
* Software Procurement

o When applicable and within budget provisions, the upgrade software shall be purchased from the vendor

* Scheduling

o On receipt of the approved request, the change will be scheduled and this schedule approved by the CTO

* + The change schedule will be done based on resource availability and other requirements like hardware requirements and user training
* Testing and Implementation

o Testing is done on a test server and results analyzed and approved by IS control before deployment

* + All changes should go through a test phase and user acceptance test.
  + No software testing shall be carried out on the production server without adequate user acceptance testing and associated documentation.
  + Tests must be done on a backup machine or a test machine where a similar environment exists to ensure adequate results. Software testing should be fully documented.
  + The test shall be under conditions similar to the application environment and in the manner in which the system will be run in a production environment.
  + After testing, the solution can be deployed to production

#### 2.15 System Risk Assessment

##### 2.15.1 Policy Statement

*IT shall conduct periodic risk assessments of all applications and infrastructure to ensure alignment with application and technology architecture and prevent adverse impact on Enterprise network.*

##### 2.15.2 Risk Assessment Standards

* All application, hardware and communications infrastructure shall undergo periodic risk assessments carried out by IT.
* Independent assessments can also be carried out over different IT domains.
* Applications such as Internet XXXXing which are transactional and are accessed over the internet shall undergo certification and risk assessment by an independent body

#### 2.16 Application Deployment

**2.16.1 Policy Statement**

*Only tested and validated applications can be deployed to a production environment.*

##### 2.16.2 Application Deployment Standards

* All application deployment on core XXXXing systems must be signed off by the Head, Applications Management
* Before the old system is discontinued, the new system will have successfully operated through all daily, monthly and quarterly production cycles.
* The respective operating environments should be segregated and properly protected.
* Thorough testing procedures shall be followed and the system must be predictable before it can be promoted to production

#### 2.17 Post Implementation Review

##### 2.17.1 Policy Statement

*Management shall require that a post-implementation review of all operational applications be conducted to assess whether the users’ needs are being met by the system.*

# 3. Infrastructure Management

#### Overview

This is control over the IT process of acquiring and maintaining technology infrastructure that enables corporate objectives and drives agility and scalability.

Considerations include

* Compliance with technology guiding principles and overall IT Strategy
* Fit to Infrastructure Architecture
* Supplier responsibilities and support
* Total cost of ownership
* Overall Enterprise security

#### 3.1 Purchase of New Technology Infrastructure

##### 3.1.1 Policy Statement

*Management shall ensure that all infrastructure acquisition done within the Enterprise is done in conformance to documented technology guiding principles in the IT Strategy.*

##### 3.1.2 Infrastructure Acquisition Guiding Principles/Standards

Technology guiding principles

|  |  |
| --- | --- |
| **Guiding Principle** | **Decision** |
| IT Investment Perspective | •XXXX will adopt an IT Value Model that is driven by real business needs and value realizable by the organization (as against cost incurred)  •Business application investment at XXXX will be business led with proper business justification, and with support from the IT function  •IT Infrastructure investment at XXXX will be made at the enterprise level |
| Technology Position | •Technology will be viewed as a business enabler, thus XXXX will seek to quickly deploy all tested and proven technology.  •Always seeking to have a first adopter and industry leadership advantage – where reasonable  •XXXX will deploy and manage Infrastructure that is robust, scalable, and will enable significant value creation |
| IT Resource Distribution | •XXXX will centralize the operation of its enterprise applications.  •XXXX will support high value-added operations in-house and will seek to out-source non-core operations.  •Application development will be primarily outsourced to reputable development organizations whilst IMS will build minimal capabilities to enhance core applications |
| IT Processing Distribution | •XXXX Administrative/Operations processes will be centralized  •XXXX transactional data will reside centrally |

##### 3.1.3 PROCEDURE 7: Infrastructure Acquisition

 All acquisition is done in line with the procurement policy as defined by General Services

#### 3.2 Preventive Maintenance for Hardware

##### 3.2.1 Policy Statement

*IT management shall schedule routine and periodic hardware maintenance on to reduce the frequency and impact of performance failures.*

Preventive maintenance in this context is subdivided in to 2 broad segments:

* User systems: Preventive maintenance will be carried out by regional representatives on all systems brought for repair at the point of repair. On a quarterly basis, regional representatives shall routinely carry out preventive maintenance on all user systems in locations under their purview
* Core Infrastructure: This refers to core infrastructure (servers, storage, communications equipment and power equipment) located at the center, branches and all disaster recovery locations. IT management shall ensure all equipment are covered by a support service contract which included a clause for preventive maintenance to be carried out on equipment

##### 3.2.2 Preventive Maintenance Standards

* Technology group will be responsible for supervising all maintenance tasks on IT infrastructure. This includes tasks carried out by vendors and tasks carried out by support staff.
* A review of the maintenance agreements and service level agreements with be done by the Infrastructure management unit and the Service Delivery Manager
* Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications where specified and by the supplier or a nominated third party.
* Only authorized maintenance personnel shall carry out repairs and service equipment.

##### 3.2.3 PROCEDURE 8: Preventive Maintenance

* Prior to scheduled maintenance, a notification would be sent to all support staff notifying them of planned downtime and if necessary all staff of the XXXX and/or customers.
* During maintenance, a representative of IT will physically supervise vendor during maintenance and signs off work sheet verifying work done.

#### 3.3 Capacity Management

Capacity management in the context of this policy refers to component capacity (as defined by ITIL V3). Capacity management refers to ensuring that IT has the capacity in terms of technology to cost effectively meet current and future requirements.

##### 3.3.1 Policy Statement

*Management shall leverage virtualization technologies and cloud computing to ensure cost management of technology infrastructure and dynamic posture to provisioning technology assets in response to business requirements. Capacity plan shall be available and maintained to enable predictive forecast for future requirements for critical components and assets.*

##### 3.3.2 Capacity Management Imperatives

The infrastructure team shall:

* Continuously monitor the performance and throughput or load on all hosts, virtual machines and risk servers
* Review performance and take steps to ensure that critical services have access to adequate infrastructure capacity
* Understanding the demands on IT services and future plans for workload growth (or shrinkage) and develop a capacity management plan for critical services

#### 3.4 Stock and Inventory Management

##### 3.4.1 Policy Statement

*An inventory of all information technology related assets shall be maintained using System, Center Configuration Manager (SCCM) managed by the Enterprise Infrastructure Service.*

**3.4.2 Stock and Inventory Management Guidelines** Examples of assets associated with information systems are:

* Information assets:
  + Databases and data files,
  + System documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information
* Software assets: o Application software, system software, development tools and utilities
* Infrastructure assets:
* Computer equipment (servers, desktops, laptops, modems), communications equipment (routers, switches), storage media, other technical equipment and UPS

**3.4.3 PROCEDURE 9: Software Inventory**

#### PROCEDURE 9: SOFTWARE INVENTORY

* After an off the shelf application is acquired, a copy should be made and stored off-site.
* All Enterprise applications should have copies stored off site along with applications developed in-house
* After changes are made to any applications, the most recent version should replace the copy stored off-site
* Software shall only be retrieved from the media library for contingency reasons
* All applications in-house developed or outsourced (such that the source codes have been acquired by the XXXX) must be stored on Microsoft Team Foundation Server (TFS)

##### 3.4.4 PROCEDURE 10: Hardware Inventory

* Planning

The Head, Infrastructure Management gives an indication of the number and types of infrastructure which would be required for the Financial Year. This can be based on any combination of the following:

* Corporate Objectives and IT Strategy
* Number of requests made
* Infrastructure spending trends
* Market Trends
* Length of time required for delivery; amid other necessary factors
* Order is placed in accordance with the standard purchasing procedures only at the point of an approved request from an end user.
* Inventory Control
* Upon addition of a new infrastructure component, the item will be automatically updated on SCCM

 IT equipment disbursement

* Based on request from regional support staff and user department, the item will be disbursed to the various regions
* Branches and business unit shall make request through Regional support staff or the IT Service desk and complete an (Request for Authorization) RFA
* Regional staff will send RFA to the IT Service Desk for approval
* If the RFA is approved, a request is made to the vendor and the equipment is delivered o After delivery and verification, it is dispatched to the requesting branch/region

# 4. IT Policy and Procedure Management

#### Overview

This addresses the control over the process of developing and maintaining procedures that govern and enable the use of applications by documenting a structured approach to the development of user and operations procedure manuals, service level requirements and training.

It and takes into consideration

* Business process re-design
* Treating procedures as any other technology deliverables
* Timely development of procedures
* User procedures and controls
* Operational procedures and controls
* Training materials
* Managing change

#### Responsibility Clause

The responsibility for managing this policy document is as outlined in the responsibility grid below

|  |  |
| --- | --- |
| Group | Responsibility |
| All XXXX Employee | All XXXX employees (including temporary staff), third party persons are required to read and understand this policy prior to any engagement with the XXXX requiring assess to or use of technology tools and/or services |
| Internal Control | IS Control is expected to ensure adherence to this policy |
| Chief Information Officer | IT is responsible for implementing this policy and ensuring Technology regular updates for continued relevance |
| IS Audit | IS Audit being responsible for auditing the implementation of this policy |

#### 4.1 Operational & Service level agreements

##### 4.1.1 Policy Statement

*IT management shall ensure as much as possible the timely definition of operational requirements and service levels before the software is deployed for use enterprise-wide*

##### 4.1.2 Operational & Service Level Guidelines

The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

#### 4.2 User Procedures Manual

##### 4.2.1 Policy Statement

*IT Management shall ensure that adequate user procedures manuals are developed as part of every information system development, implementation or modification.*

**4.2.2 User Procedure Manual Standard**

These materials should be focused on the system’s use in daily practice.

#### 4.3 Technical Manual

##### 4.3.1 Policy Statement

*IT Management shall ensure that that an adequate technical document manual be prepared and kept up-todate as part of every information system development, implementation or modification.*

##### 4.3.2 Technical Document Standard

These materials should be focused on providing information and guidance for managing, supporting and troubleshooting the application

#### 4.4 Training Materials

##### 4.4.1 Policy Statement

*IT Management shall ensure that a detailed user manual is developed part of every application developed*

**4.4.2 Training Manual Standard**

These materials should be focused on the system’s use in daily practice.

# 5. Change Management

#### Overview

This section of the policy addresses a formal approach to managing operational changes to existing IT assets, services or infrastructure and satisfies the business requirement to minimize the likelihood of disruption, unauthorized alterations and errors.

The change management process is enabled by a management system which provides for the analysis, implementation and follow-up assessment of all changes requested and made to the existing IT infrastructure and takes into consideration:

* Identification of change
* Categorization, prioritization and emergency procedures
* Impact assessment
* Change authorization
* Release management
* Software distribution
* Use of automated tools
* Configuration management

Change Management is a set of procedures and rules established by IT management to monitor and control changes to IT assets (hardware, software, applications, and network environment). This is to ensure that all changes are carried out in a structured manner without causing negative impact to any directly or indirectly business critical IT services.

For purpose of this policy, a change is defined as “anything that transforms, alters, or modifies the operating environment of a system, application or hardware and has the potential to affect its stability and reliability or disrupt the business”. This change, as defined by this policy, can be planned or unplanned.

Changes are required for many reasons, including:

* User requests
* Vendor recommended/required changes
* Regulatory requirements
* Hardware and/or software upgrades
* Acquisition/implementation of new hardware or software
* Hardware or software failures
* Environmental changes (electrical, power, cooling, data center remodels, etc)
* Unforeseen events
* Periodic Maintenance

Change requests as they relate to us have been categorized into:

* Pre-approved/Standard changes: A change with low risk that has been performed before and is part of the operational practice of the business—for example, an update to a user profile, and periodical patches, holiday marking on finacle . Pre-approved changes will be documented as an SOP detailing each step to be taken. To carry out a change the requester seeks approval from CAB members via an email and sends periodic reports to CAB on all changes carried out
* Emergency changes: Changes which need to be implemented outside of the formal change management process and approved after the fact. The changes need to be at the very least implicitly approved by the Head, Information Technology or the

Divisional Head, Business Support prior to implementation

* Major changes: A change where the impact on the Enterprise could be massive with high risk changes that have enterprise financial, regulatory, security, reputational implication. Also, changes that will affect customers through service downtime e.g. Periodic maintenance of the Front-End Processor
* Minor changes: A change affecting small numbers of individuals or Configuration Items these are changes with medium risk with no financial, regulatory, security implication—for example,

#### 5.1 Formal Change Control

##### 5.1.1 Policy Statement

*IT Management requires that changes within the IT group be subject to formal change management process that ensures or provides for a managed approach for changes which are requested, approved, logged and tested.*

##### 5.1.2 Scope

This policy covers all changes (additions, deletions and modifications) to all IT assets in the live environment. These include:

* IT infrastructure

Hardware (servers and storage)

Network and Communications infrastructure

Power infrastructure

* Applications

Proprietary and third-party software

Operating systems

* Application data and Databases
* Data Center Facilities

Primary Data Center and all Disaster recovery facilities.

It however does not apply to changes on test systems but can be applied to changes on development platforms during projects to avoid scope creep or activities which may negatively impact application development.

##### 5.1.3 Roles and Responsibilities for Formal Change Control

5.1.3.1 Change Owner: Is responsible for

* Submitting a change request via instituted platforms
* Participating in acceptance testing and sign off

5.1.3.2 IT Management: Is responsible for

* Policy dissemination and oversight

5.1.3.3 Change Manager: Is responsible for

* Pre-approval of all change requests
* Categorizing of change requests based on the parameters provided in this policy
* Verifying that change requests are valid and represent the collective view of the requesting unit/team as a whole
* Assessing the business and technical impact of the change
* Constituting and notifying the Change Advisory Board
* Facilitating the entire change management process

5.1.3.4 Change Advisory Board (CAB): The constitution of the change advisory board is a determined by the category of the change. For major changes, which impact on the enterprise and can affect income generation, revenue or customer service on an enterprise wide scale (typically major changes), this body has the responsibility of:

* Assessing, from a business and a technical viewpoint, all Requests for Change (RFCs) categorized as Major changes
* Prioritize RFCs and propose resource allocation, implementation approach as well as security and control considerations for implementing requested change
* Approve or decline change requests based on impact and value assessment

The change advisory board will be constituted of the following:

* + Chief Information Officer
  + Chief Information Security Officer
  + Head, Compliance & Internal Control
  + Chief Inspector
  + Head, ORM
  + Head, BPR
  + Head Applications management
  + Head Infrastructure management
  + IT Steering Committee Secretary
  + Service Delivery Manager
  + Representative(s) of the Implementing units
  + Representative(s) of the requesting units

For other minor changes, the change advisory board will be constituted dynamically taking into consideration the following:

* + A representative of the requesting unit
  + The Head Applications management
  + The Head Infrastructure management
  + Head IS Control
  + Head IS Audit
  + Head, BPR
  + Head, ORM
  + Information security Officer
  + Service delivery Manager
  + Representative of implementing unit
  + Other key team leads depending on the scope of impact for the change

5.1.3.5 Implementation Team: This team has the responsibility of:

* Designing and implementing change based on requirements
* Developing test cases
* Defining a roll back plan
* Testing implemented change
* Deploying change to production environment

5.1.3.4 Software Testing and QA: Has the responsibility for:

* Verifying that system changes are authorized, tested, and implemented in a controlled manner prior to being introduced into the production environment. Also deployment of application to production environment.

#### 5.2 Policy Details

IT Management requires that all changes within the IT group be subject to this formal change management process that ensures or provides for a managed approach for changes which are requested, approved and tested.

An “emergency change”, which may require implementation as quickly as possible to prevent significant downtime to business-critical systems will be handled using after-the fact, follow-up procedure which ensures that all normal change management controls are retroactively applied.

Certain changes which occur regularly will be classified as a “pre-approved or standard changes”. This means that all subsequent iterations of change requests in this category during the specified period are likewise approved.

There are no exemptions to the Change Management Policy.

Changes require two steps of approval:

Prior to commencing the development or testing of a change (a Change Request) and

Prior to releasing the fully tested change into the live environment (a Release Request).

##### 5.2.1 Change Management Process

All change request must be endorsed by end user prior to being submitted to the Change Manager

Preapproved Change Requests must be endorsed via mail by the Change manager and monthly report of all change made should be sent in the requester for review by the CAB

For process changes the Business Process Reengineering team will develop the document on behalf of the requester

The information provided for the change request should be detailed and should include expected business benefits which will be achieved by implementing the change.

The Change Manager will review the change to assess viability and if needed constitute the change advisory board made up of relevant/affected stakeholders from the business, IT and operational units which will be impacted by the change.

The CAB will review the request, determine and review potential failures, and make the decision to allow, deny or delay the request.[[1]](#footnote-2)

Change Requests must receive CAB approval before proceeding.

The change owner will be required during CAB meeting to present a justification for the requested change .

There should be risk assessment and mitigation measures documented by the Operational Risk Management team in every Change Request.

The CAB has the authority to deny a Change Request (or send it back to the change owner for further detail, study or documents) for reasons including, but not limited to, inadequate planning, the timing of the change, business process impact or resourcing.

All requests for changes and related information should be properly documented in the change request template form and circulated round for sign off by requesting unit on purplerworks.

##### 5.2.2 Release Management Process

A release request must be raised for all changes, including emergency changes once the change(s) has been fully tested.

The Change Manager (where applicable) has the authority to refer the release request back to the CAB if it is not consistent with the approved change request(s).

Release requests must receive approval from the Configuration Manager prior to the change being released into the live environment.

The release manager will communicate the details of the release to affected business users and IT staff and arrange for the Release to be implemented once the release request has been approved.

The release manager will update the CMBD and related technical documents to reflect the implemented changes

#### 5.3 Change Categories

##### 5.3.1 Standard Change

A standard change is a change which has been previously performed or is routinely performed. These changes are blanket approved and no longer require specific approval prior to implementation.

Criteria for identifying changes that fall into this category include:

Thresholds: Effort to implement or execute is very low along the following axes; risk, cost, effort, resources required and complexity

Frequency: Operational processes which are executed very regularly e.g. printer purge or

ID reset/sack

Approval: Operational processes which have been approved in principle e.g. adding a newly procured PC or new recruit to the network.

##### 5.3.2 Major Change

A major change is a change which impacts on the entire Business. Changes in this category, impact directly on Line of Business applications/service touch points and has the capacity to affect income streams.

Criteria for identifying changes that fall into this category include:

Fiscal Impact: Directly affects income generation channels

Customer Service Delivery: Affects any or all customer service delivery channels

Scope of Impact: Impacts on communications systems or other business critical systems on an enterprise wide basis.

##### 5.3.3 Minor Change

A minor change is a change which affects a limited number of users or services with low business criticality.

Criteria for identifying changes that fall into this category include:

Cost Impact: Does not affect any income generation channel

Scope of Impact: Impacts a limited number of users

##### 5.3.4 Emergency Change

An emergency change is a change which needs to be effected immediately due to business or regulatory requirements and cannot follow the documented change management process. Changes in this category are approved after the fact.

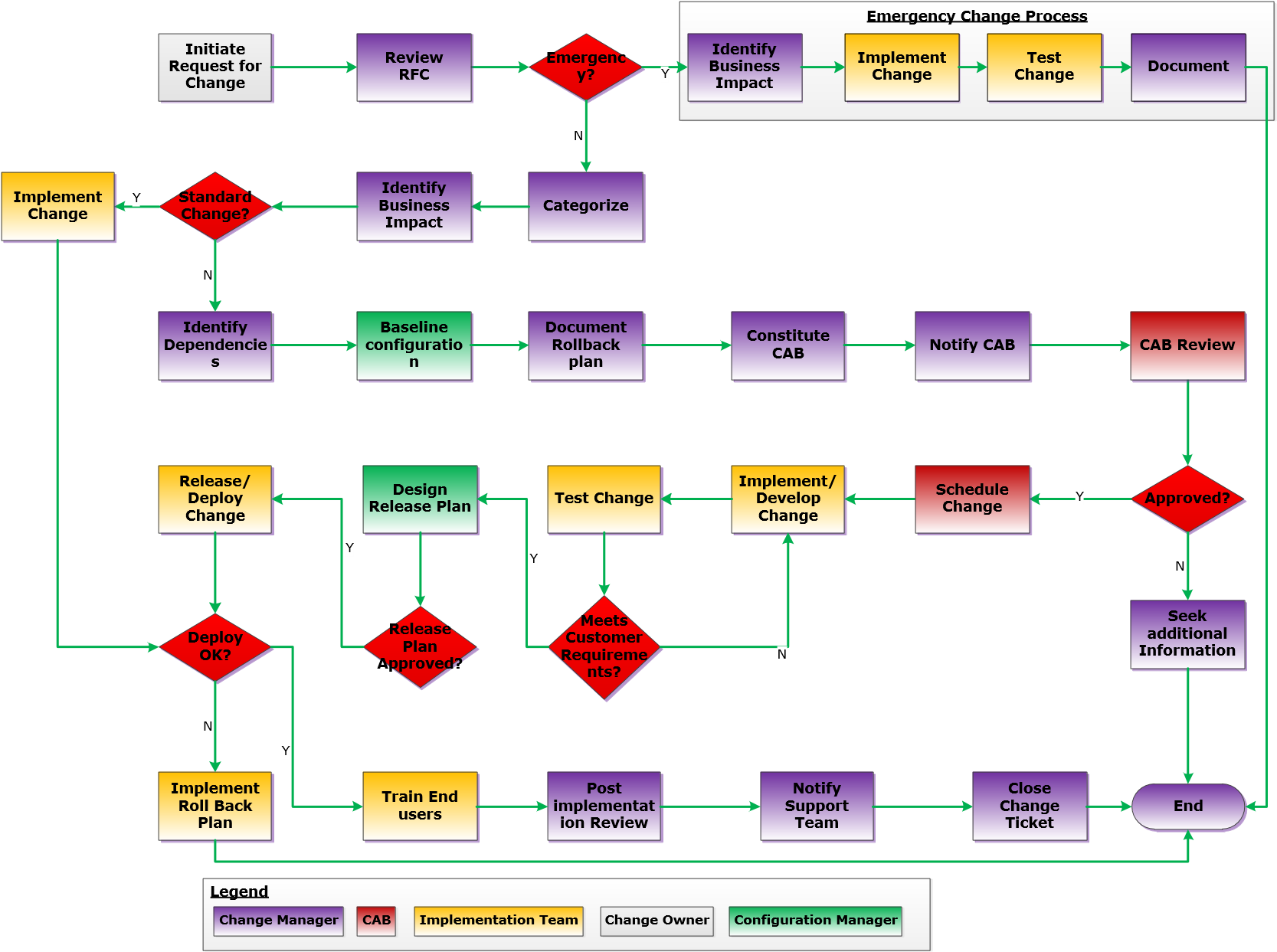
Criteria for identifying changes that fall into this category include:

Impact: Have fiscal or regulatory impact

Urgency: Impacts on a significant number of users

#### 5.4 Change Management Process Flow

**Change and Release Management Process**



#### 5.5 Change Process Notes

All major and minor changes require CAB review and approval

It is the responsibility of the Change Manager to schedule CAB meetings

Release plans need to be approved by the CAB and Configuration Manager prior to approval

Kindly refer to Appendix A.6 for the Business Impact grid for our services

The priority of the change is determined by the Change Manager using the Change Priority Table (Appendix A.7)

Resource allocation for development and testing is done by the CAB

The change implementation team is comprised of the team responsible for developing and testing the change

Depending on the scope of the change the Configuration Manager may or may not be a part of the Implementation Team

For major changes for example shut down of critical servers, backup must be performed before the changes are applied

# 6. Configuration Management

#### Overview

The section of this policy provides description for each component of configuration management as implemented with the Technology department of the XXXX. This manages how changes would be controlled, where responsibility for configuration management would lie, how the product and various versions will be identified. Objectives of configuration management include;

* To ensure that CIs are identified, base lined and maintained throughout their lifecycles, and that changes on them are controlled
* To identify, control and care for assets that are under the control of Information Technology throughout their lifecycles
* To identify, control, record, report, audit and verify services and other configuration items (CIs), including versions, baselines, constituent components, their attributes and relationships
* To work with Change Management to ensure that only authorized components are used and only authorized changes are made

#### 6.1 Definitions

**Configuration Item (CI):** Configuration Items (CIs) can be of various types: the Configuration Management system covers services and IT infrastructure, but may also cover other item types like policies, project documentation, employees, and suppliers. Configuration Items are characterized by their attributes (recorded in the CI's Configuration Record) and their relationships to other CIs. A configuration item (CI) is an asset or a combination of IT assets that may depend on and/or have relationships with other IT processes.

**CMS / CMDB:** System Centre Configuration Manager (SCCM) is the Configuration Management Database (CMDB) used for collecting, storing, managing, updating, analyzing and presenting data about all configuration items and their relationships. Its underlying structure is defined by the Configuration Model, a logical model of the IT department service assets.

#### 6.2 Configuration Management Process

**Configuration Identification**

This defines and maintains the underlying structure of the CMS / CMDB, so that it is able to hold all information on Configuration Items (CIs). This includes specifying the attributes, describing CI types and their sub-components, as well as determining their interrelationships.

* The information recorded for each Configuration Item (CI) ensures effective control and include at least:
* description of the CI;
* relationship(s) between the CI and other CIs;
* relationship(s) between the CI and service components;
* status;
* version;
* location;
* associated requests for change;
* Associated problems and known errors.

**Configuration Control**

This ensures that no Configuration Items are added or modified without the required authorization, and that such modifications are adequately recorded in the CMS. CIs are recorded and controlled on the CMDB. CMS tracks all versions of the CIs.

**Configuration verification and audit**

This performs regular checks, ensuring that the information contained in the CMS is an exact representation of the Configuration Items (CIs) actually installed in the live production environment within the XXXX’s infrastructure.

##### 6.2.1 Responsibilities

|  |  |  |
| --- | --- | --- |
| S/N | Role | Responsibility |
| 1 | Configuration Management | Enterprise Infrastructure Service |
| 2 | Configuration Identification | Enterprise Infrastructure Service |
| 3 | Configuration Control | IS Control |
| 4 | Configuration Verification and Audit | IS Audit |

##### 6.2.2 Configuration

# 7. Service Management Framework

#### Introduction

Service Management is a required component to achieving the strategy of the IT group. Service management describes strategy with which IT Services will be delivered to the business in a way that consistently provides value to internal customers.

A service management plan helps us achieve the following:

* Reduction of the service delivery costs
* Understand and define the business impact of all IT Services
* Definition of Service components and configuration items to enable capacity building and forecasting and ensure service level agreements are met
* Improved internal and external customer satisfaction levels

#### 7.1 Service Management Strategy

* Document and deliver on all service availability agreements for all IT services
* Develop capacity and flexibility on an enterprise scale to ensure reduced time to market for all initiatives within the business
* Measure and monitor all services to ascertain business value and identify opportunities for improvement
* Define and measure performance indices for the IT group
* Drive knowledge sharing to ensure we maintain a workforce which is in tune with the corporate climate and acutely aware of their role in the success of the organization as a whole

#### 7.2 Service Portfolio Management

Service portfolio management is the management of all services currently being delivered and controlling the process by which new services and designed.

Service portfolio management classes IT services into three buckets; Services in the Pipeline, Services currently being offered and retired services.

Pipeline services are services which have been envisioned and are awaiting design and implementation.

Services currently being offered are services which are documented in the IT Service Catalog as services which can be subscribed.

Retired services are services which have lost their relevance and are no longer required. These services are then retired and taken off the Service Catalog.

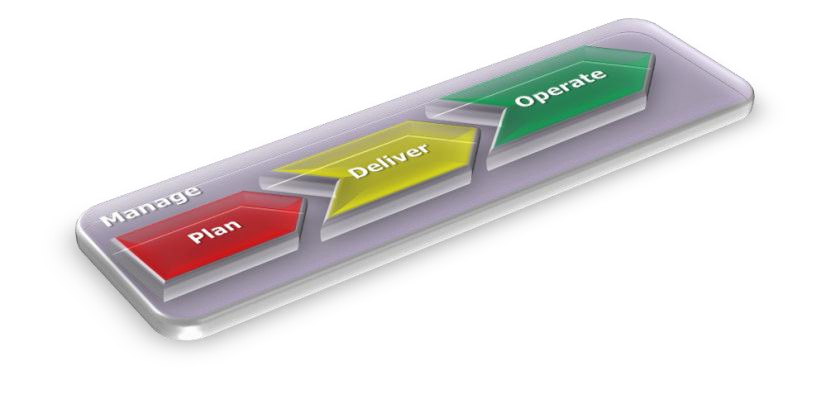
#### 7.3 Service development lifecycle

The IT service lifecycle describes the life of an IT service, from planning and optimizing the IT service to align with the business strategy, through the design and delivery of the IT service, to its ongoing operation and support.

For all services, these phases serve as a check list to ensure all considerations have been evaluated. The rigor with which they will be applied is determined by the scope and impact of each service.

The service development lifecycle adopted is based on the Microsoft Operations Framework which has four basic phases:

**7.3.1 Plan Phase:**

* Business/IT Alignment: Review business value of the proposed service to ensure alignment with the IT Strategy and the overall corporate strategy.
* Performance metrics: Performance metrics from the customer’s perspective to understand what would constitute value from the view of the customer.
* Procedures and Policies: Review the impact of this service on existing business processes and identify gaps which may require new policy definitions
* Fiscal Management: Evaluate effort required to develop service. Review budgeting constraints alongside fiscal benefits.

**7.3.2 Deliver Phase:**

* Visioning: Document the end state which would be achieved by deploying the service. Detail a migration plan and guidelines for moving from current state to proposed end state
* Plan Execution: Evaluate available options and technologies. Evaluate available resources if local development will be done. Document functional specifications and project plan
* Build: Develop or acquire required applications, identify release dependencies.
* Release Management: Review service to ensure “fit-for-purpose” and “fit-for use” from the perspective of the customer. Prepare production environment and perform controlled pilot
* Deploy: Deploy service to production environment

**7.3.3 Operate Phase:**

* Identify operational work requirements i.e. dependencies that ensure the service can be used by the customers for which it has been designed
* Service Delivery Management: Hand over service to service delivery manager. Manage customer experience, ensure SLAs are met, incident and problem management
* Service monitoring and measurement: Monitor overall health of the service and all its dependencies. Manage incidents and ensure continuous improvement

**7.3.4 Manage Phase:**

* The manage layer continuous for the entire lifecycle and happens in parallel for all lifecycle phases
* Risk management: continuously manage all potential risk factors which may impact the service, or which may be enabled by service deployment
* Change control: Ensure all changes are done using formal change control process

### **7.3.5 Updates to Existing ITSM Documentation and Data Sources**

In addition to the creation of documentation for each new or changed service, there is a set of existing data sources that will be updated as part of the Transition process.

These are:

7.3.5.1 ITSM Database

The ITSM database will be updated with details of the new or changed service so that all processes are aware of it including:

• Incident and Service Request Management: New users and customers New request types New incident models New categories and sub-categories

• Problem Management: Details of all known errors with the service that were not resolved prior to live running

• Configuration Management: New configuration items (CI) will be added to the CMDB The version numbers of existing Cls will be updated where appropriate

• Capacity Management: Any additional servers and other resources will be added to the list of those monitored for capacity. The capacity plan will also be updated

• IT availability and Availability: Continuity and availability requirements for the new service will be documented. The IT Service Continuity Plan will be updated to allow for the recovery of the business critical aspects of the new or changed service and the service will be monitored for availability

#### 7.3.5.2 Service Level Agreement

The SLA will be updated or a new one created to document the agreed levels of service for the new or changed service. This will be done under version control via the change management process.

#### 7.3.5.3 Service Catalogue

The new or changed service will be added to the IT service catalogue together with the required details of who uses it, how it can be accessed etc.

#### 7.3.5.4 Budgets

Budget changes resulting from the new or changed service will be incorporated into the IT budget where appropriate and a cost model calculated for the service.

#### 7.3.5.5 Supplier and Contracts Database

Any new or revised contracts will be placed into the contracts database and the details of new suppliers entered into the Supplier database.

#### 7.4 Service Management Policies

Effective service management is dependent on ensuring that defined processes are followed, and operations happen in a controlled manner.

Some policies which are pertinent to a successful service delivery strategy include:

* Change management policy
* Project documentation standards
* Service availability
* Capacity Management
* Backup and Retention Policy
* IT Device Naming Convention
* IT Portfolio Management Framework
  1. **AVAILABILITY MANAGEMENT PROCESS**

# 7.5.1 Overview

This process addresses the availability and service continuity requirements of the XXXX. Current and future requirements for availability of IT services in the XXXX are identified and taken care of in a cost-effective manner. The service continuity requirements in the event of a disruptive incident that significantly affects major IT systems within the XXXX, making them unavailable to business users are also considered by this process.

## Objectives

* To ensure IT Services are designed to deliver the required level of availability in a cost-justified manner
* To ensure through IT availability reporting, that the agreed levels of availability, reliability and maintainability are measured and monitored
* To optimize availability of IT Infrastructure to deliver cost effective improvements that deliver tangible benefits to business and User

• To reduce the frequency and duration of Incidents that impact the availability of IT Services

* To create and maintain a future focused Availability Plan aimed at improving the overall availability of IT Services and infrastructure components to ensure existing and future business availability requirements are met
* Recover the IT systems at an alternative location within an agreed response time
* Ensure that business operations can continue in limited form until IT systems are restored
* Provide a detailed description of how XXXX will respond to a disruptive incident affecting the IT systems covered by this plan
* Set out who will respond to an incident and how the service continuity plan will be activated
* Describe the facilities that are in place to help with the implementation of the plan
* Define how decisions will be taken with regard to our response to an incident
* Explain how communication within the organization and with external parties will be handled
* Provide contact details for key people and external agencies and suppliers
* Define what will happen once the incident is resolved

## Scope

This process will cover all IT Services and supporting infrastructure. IT services outsourced by the XXXX are also within the scope of this process.

# Reactive Availability Management Activities

Availability Management shall maintain a set of reactive activities to respond to availability failures and issues as follows:

* Monitor, measure, analyse, report and review service, hardware, application, and network availability to ensure that agreed levels of availability have been provided.
* Work with Incident and Problem Management to investigate all service, hardware, application and network unavailability and provide remedial action where issues are discovered.
* Analyse availability results achieved to look for possible trends and issues around availability that need to be addressed on an ongoing basis.

# Proactive Availability Management Activities

Availability Management shall maintain a set of proactive activities to manage availability levels to agreed targets and continually improve upon availability levels being delivered:

* Perform risk assessment of new services and changes before they are implemented to determine their impacts to availability levels.
* Implement and oversee cost justifiable countermeasures to prevent or reduce availability risks that might exist in the infrastructure.
* Test implemented availability countermeasures to ensure they will function as planned
* Assist with the plan and design of availability functions and features into new applications, services or other solutions.
* Analyse availability results achieved to look for possible trends and issues around availability that need to be addressed on an ongoing basis.

# Availability Plan

An Availability Management plan shall be produced, managed and maintained to enable the XXXX to continue to provide and improve services in line with availability targets defined in Service Level Agreements (SLAs).

# Availability Testing

Availability mechanisms shall be tested on an ongoing basis. This includes maintaining a schedule of tests for all resilient and failover assets and mechanisms. This is a schedule for the regular testing of all availability mechanisms such as load balancing, mirroring or auto-failover.

All availability mechanisms shall be tested in a regular and scheduled manner to ensure that they will work when they are needed. This schedule shall be maintained and circulated so that all areas are aware of its content and so that all other support activities can be synchronized with its content, such as:

* The Change Schedule
* Release plans and the Release Schedule
* All transition plans and projects
* Planned and preventative maintenance schedules
* The schedule for testing IT service continuity and recovery plans

# Risk Management

A risk assessment should be performed for service continuity and availability. Impacts and risks of changes to service requirements should be determined for existing and new services. Criteria for accepting risks should be based on existing XXXX Risk Management Framework.

# Availability Reporting

Report on service availability shall be produced on an ongoing scheduled basis. This also includes the collection of measurements, analysis and production of regular and ad hoc reports on availability of services.

# Activation Criteria and Procedures

There are two main scenarios in which the service continuity process may be activated:

* In response to a major disruptive incident that has resulted in the organization’s Incident Response Procedure being activated
* As a recovery for a smaller, more localized event which, although not serious enough to result in activation of the Incident Response Procedure, requires action to address its impact

## 7.12.1 Incident Response

As part of the Incident Response Procedure, notice will be received from the Incident Response Team (IRT) by telephone to the main plan owner (or deputy) if this plan is required to be activated. This will depend upon the incident that has occurred and the scope of its effects. It is likely that this plan will be one of several that will be activated and co-ordination across the various plans will be needed.

## 7.12.2 Localized Activation

It will be up to the main plan owner (or deputy) to inform top management of the need to activate the incident response procedure.

## 7.13 Activation Procedure

The Continuity of Business Plan (COB) for IT will be invoked

# Service Continuity Requirements Management

The following steps should be taken to plan for the service contunity requirements of IT services

* Assess the business user's needs for service continuity
* Use information from business plans, service requirements, SLAs to determine
  + access rights to the services;
  + response times;
  + end to end availability of services.

# Activation Criteria and Procedures

There are two main scenarios in which the service continuity process may be activated:

* In response to a major disruptive incident that has resulted in the organization’s Incident Response Procedure being activated
* As a recovery for a smaller, more localized event which, although not serious enough to result in activation of the Incident Response Procedure, requires action to address its impact

## 7.14.1.1 Incident Response

As part of the Incident Response Procedure, notice will be received from the Incident Response Team (IRT) by telephone to the main plan owner (or deputy) if this plan is required to be activated. This will depend upon the incident that has occurred and the scope of its effects. It is likely that this plan will be one of several that will be activated and co-ordination across the various plans will be needed.

## 7.14.1.2 Localized Activation

It will be up to the main plan owner (or deputy) to inform top management of the need to activate the incident response procedure.

## 7.15 Activation Procedure

The Continuity of Business Plan (COB) for IT will be invoked

# Roles and Responsibility for Service Continuity Process

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| CIO | * Accountable for ensuring the COB plans for IT are appropriate to the needs of the business users, based on the funds available, business activities, service requirements and any agreed targets of relevance to service continuity. |
| The Service Manager | * Ensuring the service continuity process activities are executed. This includes risk assessment and risk avoidance. Risk management is done via service continuity planning, testing of plans and when necessary invocation of the plans. * Ensuring that changes to the SMS are reflected in changes to the COB plan and vice versa, under the control of change management |
| IT Recovery Team | * Recovering servers, operating systems and any other components upon which the applications are based * Restoration of Applications and data from backups and the restoration of links, including the configuration of switches and routers. * Setup and configuration of the business applications once they have been restored to the server hardware. This might involve liaison with third party application support services. |

# Roles and Responsibility for Availability Process

|  |  |  |
| --- | --- | --- |
| **S/N** | **Role** | **Responsibilities** |
|  | Head,Enterprise Infrastructure Service | * Optimize the availability of the IT infrastructure to deliver cost effective improvements that deliver tangible benefits to business units and customers * Provide holistic management of availability that includes people and processes as well as technology. * Take actions to achieve reductions in frequency and duration of incidents that impact IT Service availability. * Ensure shortfalls in IT Service availability are recognized and appropriate corrective actions are identified and taken. * Create and maintain a future focused availability plan aimed at improving the overall availability of IT services and infrastructure components to ensure that existing and future availability requirements can be met. * Provide regular reports on availability to the Service Manager. * Determine the availability requirements from the business for new or enhanced IT services. * Establish measures and reporting that reflect business, user and IT support organization requirements. * Assess and authorize changes from an availability perspective. * Conduct availability risk assessment for existing services. * Define the key targets of availability required for the IT infrastructure and its components that underpin a new or enhanced IT service as the basis for an SLA agreement. * Maintain an awareness of technology advancements and best practices that support availability. * Gather availability data as needed for reporting and communications |

#### Associated Documents

* IT Service Catalog
* IT service dependency maps

# 

# 8. Incident Management Framework

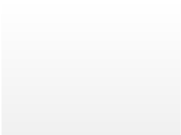
#### Overview

An incident is an unexpected service disruption which may or may not be anticipated. As is expected with any technology service, disruptions occur making it critical as part of the effective service delivery process to document a process for handling all incidents, communicating to affected users and keeping customers in the update loop until resolution.

#### Incident Management

All IT related incidents and service requests within XXXX are handled centrally by the IT Service Desk using the following process:

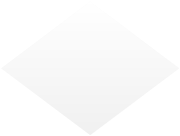
#### Incident Management Process



Assign to Service

Desk Support for

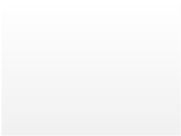
First Level Support



Resolved within

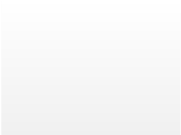
SLA

?



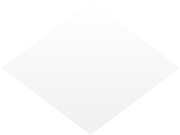
Obtain feedback

from User



Escalate to Second

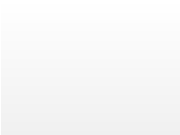
Level Support



Resolved within

SLA

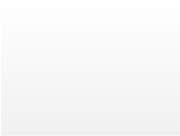
?



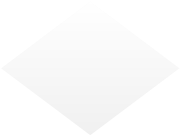
Classify as problem

and escalate to

Third Level

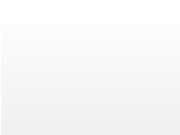


Categorize



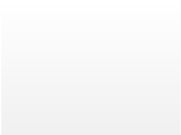
Known Problem

?



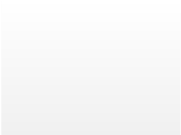
Refer user

knowledge Base



Update Knowledge

base



Give feedback to

User

Y

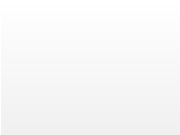
N

Y

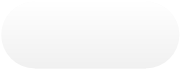
N

Y

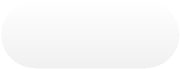
N



Obtain Resolution



Incident Logged



Close Cal

**Incident Management Process**

#### Major incidents are classified as High Priority while Minor incidents can be classified as Medium or Low priority.

#### Incident Classification

|  |  |
| --- | --- |
| **Category** | **Description** |
| **High (H)** | * The damage caused by the Incident increases rapidly. * Work that cannot be completed by staff is highly time sensitive. * A minor Incident can be prevented from becoming a major Incident by acting immediately. * Several users with VIP status are affected. |
| **Medium (M)** | * The damage caused by the Incident increases considerably over time. * A single user with VIP status is affected. |
| **Low (L)** | * The damage caused by the Incident only marginally increases over time. * Work that cannot be completed by staff is not time sensitive. |

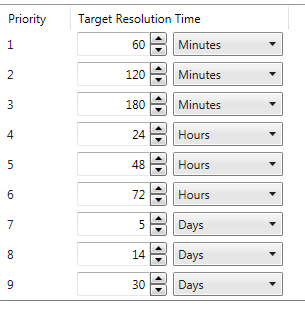
|  |  |
| --- | --- |
| **Category** | **Description** |
| **High (H)** | * A large number of staff are affected and/or not able to do their job. * A large number of customers are affected and/or acutely disadvantaged in some way. * The financial impact of the Incident is (for example) likely to exceed $10,000. * The damage to the reputation of the business is likely to be high. * Someone has been injured. |
| **Medium (M)** | * A moderate number of staff are affected and/or not able to do their job properly. * A moderate number of customers are affected and/or inconvenienced in some way. * The financial impact of the Incident is (for example) likely to exceed $1,000 but will not be more than $10,000. * The damage to the reputation of the business is likely to be moderate. |
| **Low (L)** | * A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort. * A minimal number of customers are affected and/or inconvenienced but not in a significant way. * The financial impact of the Incident is (for example) likely is less * The damage to the reputation of the business is likely to be minimal. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Priority Levels** | **Description** | **Scope** |
| **High (H)** | Priority 1  Priority 2  Priority 3 | This refers to incidents affecting Line of Business applications and impact directly on the business in terms of revenue and customer service delivery | Enterprise Wide |
| **Medium (M)** | Priority 4  Priority 5  Priority 6 | This refers to incidents that affect a smaller group of people like a unit, department or branch and for which a work around can be provided | Limited number of users |
| **Low (L)** | Priority 7  Priority 8  Priority 9 | This refers to an incident which has no immediate impact on customer service delivery. | Very limited number of users |

The categorization of incidents is done using the impact – urgency matrix as shown below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** |  | **High(H)** | **Medium(L)** | **Low(L)** |
| **High(H)** | HH – Priority 1 | HM – Priority 4 | HL – Priority 7 |
| **Medium(M)** | MH – Priority 2 | MM – Priority 5 | ML – Priority 8 |
| **Low(L)** | LH – Priority 3 | LM – Priority 6 | LL – Priority 9 |
| **Urgency** | | | |

**SCSM Priority Levels**



**Utilization of IT Reps** **Services**

The procedure for IT Rep deployment to branches for incidents’ resolution is itemized below:

* **All incidents must be properly logged on the Global Service Desk portal.**
* **IT Reps must get the approval of the Service Deliver Manager before treating any logged incident**
* **The affected user must not leave his/her desk during the period of visit**
* **IT Reps should not repair systems in the absence of the affected user**
* **The affected user should check his/her system properly and ensure no external device is connected/attached to it after repairs**
* **The Automated Branch Visitation Form (BVF) adopted by the XXXX must be duly completed by the IT Reps. IT Reps must ensure the affected user and BSM fields are filled for proper notification/confirmation.**

# 9. Service Request Management Framework

**Overview**

Service request management process enables effective and efficient management of all service requests, in alignment with business and customer priorities. Service requests may include standard changes, e.g. low risk, well defined pre-approved changes, requests for information or requests for access to standard IT services.

Service Request management is obviously one of the most critical and visible processes to the user and as such represents an excellent opportunity to promote a positive view of the Technology Department amongst the user population. The process of service request management is delivered via the IT Service Desk function.

#### 9.1 Service Request Management

All IT related incidents and service requests within XXXX are handled centrally by the IT Service Desk. Service requests are categorized, prioritized and escalated in the same manner as the incident management process.

##### 9.1.1 Service Request Management Process



# 10. Problem Management Framework

#### Overview

The objective of the Problem Management process is to manage the lifecycle of all problems. The primary aim of problem management is to prevent incidents from happening and to minimize the impact of incidents that cannot be prevented. Proactive Problem Management Analyses Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant problems. Effective problem management also means that fewer incidents will be logged at the service desk thus freeing up resources within XXXX IT Service Desk function and increasing user productivity within the organization.

A problem is defined by the ISO/IEC 20000 standard as:

“Root cause of one or more incidents”

#### 10.1 Problem Management

All recurring incidents within XXXX are handled centrally by the IT Service Desk. When recurring incidents are identified, the Service Desk Owner sends this to the unit responsible for resolving the incident. The incident is then analyzed/investigated, the root cause is diagnosed, an available workaround is identified and then a solution is proposed.

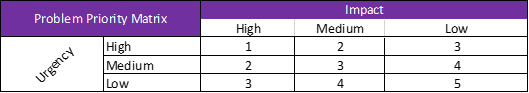
##### 10.1.1 Problem Management Process Flow

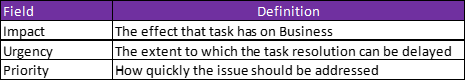


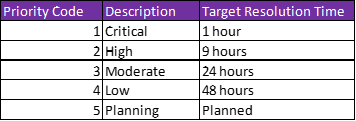
#### Problem Classification

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Critical** | * There is significant business service impact because multiple customers are affected * The damage caused by the Incident increases rapidly |
| **High** | * The damage caused by the Incident increases considerably over time. * Rate of re-occurrence |
| **Moderate** | * There is little impact on services |
| **Low** | * Workaround is available * Limited number of staffs are affected |
| **Planning** | * Planned Downtime |

The categorization of Ps is done using the impact – urgency matrix as shown below:







##### 10.1.2 Process Narrative

The following sections set out what happens at each stage of the process as depicted in the diagram above.

**Problem Identification**

All logged incidents, email and tickets raised on the Service Desk application are analyzed on weekly basis to proactively identify problems through the correlation of incident reports, error logs and other problem identification resources.

The Service Desk Owner documents the whole process of resolving the problems in the problem record detailing information such as:

* the recurring incident,
* the root cause,
* an available workaround and
* the resolution status (whether open or closed)

This report is then compiled and sent out on Bi-monthly basis to IT GRC unit by the Service Desk Owner.

The identified problems are then collated and sent to the individual units responsible for a permanent fix.

**Problem Categorization**

The Service Desk Owner determines categorization across IT Service to address problems in a timely manner based on business risk and service definition to ensure that problem identification and root cause analysis are handled in a timely manner.

**Problem Diagnosis and Resolution**

The Service Desk Owner identifies problems that may be known errors by sending the list of recurring incidents to the unit responsible. The unit then analyses the problem, finds the root cause and then resolution is carried out.

If it is established that an immediate fix for the problem does not exist, the status of the problem record would read **“Active”.**

If the unit responsible is unable to resolve the problem, the Service Desk Owner may opt to escalate it further to third party external vendors.

The Service Desk Owner ensures proper escalation of problems, e.g. escalation to a higher management level according to agreed-on criteria, contacting external vendors, or referring to the change advisory board to increase the priority of an urgent request for change (RFC) to implement a temporary workaround.

**Workarounds**

Any workaround found which reduces or eliminates the symptoms of the problem temporarily are recorded in the problem record and made available to all staff of IT. A workaround is implemented pending the identification of the root cause; after which the problem is documented in the problem record.

**Reporting**

The Service Desk Owner reports the status of identified problems to all staff of IT so customer and IT management can be kept informed. The aim of the report is to communicate the progress in resolving problems and to monitor the continuing impact of problems not solved.

**Problem Closure**

The problem is closed either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.

##### 10.1.3 Major Problem Review

In the case of major problem which have had a significant impact on service delivery to users, a problem review will be carried out to identify lessons learned.

# 11. IT Device Naming Convention

#### Overview

This procedure is to delineate specific conventions regarding the assignment of host or device names for equipment attached to (or part of) the XXXX Group network infrastructure.

#### Scope

This set of conventions applies to all XXXX Group Local Area Networks (LAN) and all devices attached to those networks.

Infrastructure Management Unit is responsible for IT asset (specifically, hardware and software) installation throughout the group and as such, is responsible for ensuring installed assets are named according to the conventions spelled out in this document. Even though this role may be assigned to authorized vendors, the responsibility for the compliance resides with the Head of Infrastructure Management.

**Equipment/Software**

Servers, Laptop Computers, Desktop Computers, Network equipment

#### 11.1 Policy Statement

*All devices attached to the Company network infrastructure shall be assigned names that facilitate easy management of network resources.*

#### Server Naming Conventions

**Network file servers, web servers, print servers, mail servers, etc., shall be assigned names composed of a combination of the departmental abbreviation, function or role, and unique number. The pattern for this name shall be:**

#### <Company Acronym>-<location abbreviation>-S-<related name>-<unique no>

Location abbreviation shall contain a minimum of two alphabets and the unique number shall contain three digits and start with 001.

The following names are examples of valid server names:

XXXX-HQ-S001

XXXX-HQ-SBERRY-002

**Network Host Naming Conventions**

**Workstation Naming Conventions**

Desktop computing resources shall be assigned names using this format:

#### <company acronym>-<dept./branch abbreviation>-<W>-<unique no>

**The unique number shall contain three digits and start with 001. Examples are:**

XXXX-IT-W003

XXXX-KAN-W001

XXXX-APP-W095

Laptop computers shall have letter “L” to replace “W” .

#### <company acronym>-<dept./branch abbreviation>-<L>-<staff number>

**For example:**

XXXX-IT-L2993

XXXX-JOS-L3000

XXXX-CAL-L4450

#### Printer Naming Conventions

Printers are assigned names in order to make it easier for users to find and connect when required. Printer names will be constructed in such a manner that it is easy to determine them: They should be number using this format:

#### <company acronym>-<dept./branch abbreviation>-<P>-<unique number>

The unique number shall contain three digits and start with 001.

Examples are:

XXXX-KAN-P001

XXXX-APP-P002

#### Infrastructure Device Naming Conventions

Infrastructure devices include all hardware that makes up the actual network. The following table details the naming conventions for the applicable hardware:

|  |  |  |
| --- | --- | --- |
| **Device Type** | | **Naming Standard** |
| Router |  | **<company acronym>-<location abbreviation>-R-<unique number>**  XXXX-HQ-R005  XXXX-JOS-R001 |
| Bridge |  | **<company acronym>-<location abbreviation>-B-<unique number>**  XXXX-HQ-B004  XXXX-JOS-B001 |
| Modem XXXXs,  Modems, | | **<company acronym>-<location abbreviation>-M-<unique number>**  XXXX-HQ-B004 |
|  | | XXXX-JOS-B001 |

# 12. IT Backup Policy

#### 12.1 Introduction

In information technology, a backup or the process of backing up refers to making copies of data so that these copies may be used to restore the original data or information after a data loss event.

Backups are useful primarily for two purposes. The first is to restore a state following a disaster (called disaster recovery). The second is to restore small numbers of files after they have been accidentally deleted or corrupted and prevent data loss.

#### 12.2 Backup Strategy and Technical Considerations

##### 12.2.1 Strategy

The need to backup business critical data is largely borne out of the need to be able to provide business continuity and ensure that line of business applications and systems can be restored to full operation from a disaster or crisis without causing significant loss to the business.

In the light of that, Return Point Objective and Return Time Objectives which are critical factors which determine significant aspects of the backup strategy, approach and technology are determined strictly by business and regulatory requirements.

Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users.

Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time.

The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation.

The recovery grid below describes the Priority of each data category based on the RTO and RPO as defined by business requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **RECOVERY TIME**  **OBJECTIVE** | **RECOVERY POINT OBJECTIVE**    **Within 1 Hour Within 24 Hours** | | **>24 Hours** |
| **Within 1 Hour** | Priority 1 | Priority 1 | Priority 1 |
| **Within 24 Hours** | Priority 1 | Priority 2 | Priority 2 |
|  |  |  |  |

##### 12.2.3 Technical Considerations

Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. In the modern era of computing there are many different types of data storage devices that are useful for making backups. The storage device options usable are however limited by specific technology capabilities and requirements in our local environment.

The goal however, is to ensure that whichever storage device used provides geographic redundancy, data security, and portability.

For the purpose of the IT environment within XXXX, we will be using a combination of a **Full and incremental application and data Backup** model. This type of backup is designed to allow an entire system to be recovered to the point at which the last backup was taken.

A full system backup makes a complete image of a systems application and databases while an incremental backup makes a copy only of changes in data; if needed, these backups can be copied back to the same or a different system to ensure minimal data loss.

#### 12.3 Policy Scope

This policy applies to all Information Technology services and applications supported by the IT group of XXXX and their dependencies. It also applies to all services supplied by external vendors which are hosted within our environment.

* Backup of data from critical business applications shall be performed daily by the system administrator / delegate
* Data shall be backed up to tape or disk and taken to an offsite location at least once a week by the Database administrator

#### 12.4 Policy Statement

*All Priority 1 and Priority 2 applications, data and file systems will be regularly backed up using media provided and the backups retained for the periods agreed in this policy document.*

All applications and services have been categorized based on the recovery grid detailed above into 2 broad categories:

* Priority 1 Applications

These are services which impact directly on business processes and customer relationship management. These typically refers to transactional and communication applications.

* + Core XXXXing System
  + Front End Processor (FEP)
  + Internet XXXXing and Mobile XXXXing
  + EFT Systems (NFP, NEFT, RTGS, SWIFT, PayDirect, WesternUnion)
  + Communication and Collaboration platforms (O365, Intranet, Corporate Website)
* Priority 2 Applications

These are services which impact on internal enterprise enablement, management and control systems with no direct or negligible cost impact on the business.

* + Other applications (custom built and third party)

The retention period for which all application and data backed up is determined primarily by the business impact of the application or service. The following table shows the application, categorization and the corresponding backup and retention requirements.

##### 12.4.1 Priority 1 Applications

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Core XXXXing System** | |  | |  |  |
| **Backup Type** | **Frequency** | **Media** | | **Retention** | **Data Integrity Check** |
| Full Database | Weekly | Tape/Disk | | One Week | Monthly |
| Incremental Database | Daily | Tape/Disk | | One Week | Quarterly |
| Full Database & Application | Monthly | Tape/Disk | | Two Years | Quarterly |
| **Postilion/FEP** | |  | |  |  |
| **Backup Type** | **Frequency** | **Media** |  | **Retention** | **Data Integrity Check** |
| Full Database | Weekly | Disk |  | One Week | Monthly |
| Incremental database | Daily | Disk |  | One Week | Monthly |
| Full Database and  Application | Monthly | Disk  Tape | & | One Month | Monthly |
| **Exchange** | |  |  |  |  |
| **Backup Type** | **Frequency** | **Media** |  | **Retention** | **Data Integrity Check** |
| Full Database and Mailbox | Weekly | Disk |  | 2 weeks | Monthly |
| Incremental  database and  Mailbox | Daily | Disk |  | 2 weeks | Monthly |
| Full database and mailbox | Monthly | Disk  Tape | & | 2 weeks | Monthly |
| **Active Directory** | |  |  |  |  |
| Full system backup | Daily | Disk |  | 2 weeks | Monthly |
| **Third Party Transactional Applications** | |  |  |  |  |
| **Backup Type** | **Frequency** | **Media** |  | **Retention** | **Data Integrity Check** |
| Full Database | Weekly | Disk |  | One Month | Monthly |
| Incremental database | Daily | Disk |  | One Week | Monthly |
| Full database and  Application | Monthly | Disk Tape | and | One Month | Monthly |
| **Virtual Machines** | |  | |  |  |
| **Backup Type** | **Frequency** | **Media** | | **Retention** | **Integrity Check** |
| VHD files on all Hosts | Weekly | Disk | | Forever | Quarterly |
| **SQL Server Databases (Consolidated)** | |  | |  |  |
| **Backup Type** | **Frequency** | **Media** | | **Retention** | **Data Integrity Check** |
| MDF and LDF files | Daily | Disk | | Forever | Quarterly |

##### 12.4.2 Priority 2 Applications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Warehouse** | |  |  |  |
| **Backup Type** | **Frequency** | **Media** | **Retention** | **Data Integrity Check** |
| Full database | Weekly | Disk | One week | Quarterly |
| Incremental database | Daily | Disk | One week | Quarterly |
| Full database and application | Monthly | Disk | One Month | Quarterly |
| **In-House Developed Applications** | |  |  |  |
| **Backup Type** | **Frequency** | **Media** | **Retention** | **Data Integrity Check** |
| Full database | Weekly | Disk | One Week | Quarterly |
| Incremental database | Daily | Disk | One Week | Quarterly |
| Full application and Database | Monthly | Disk & Tape | One Month | Quarterly |
| **Third Party Non-Transactional Applications** | |  |  |  |
| **Backup Type** | **Frequency** | **Media** | **Retention** | **Data Integrity Check** |
| Full database | Weekly | Disk | One Week | Quarterly |
| Incremental database | Daily | Disk | One Week | Quarterly |
| Full application and Database | Monthly | Disk & Tape | One Month | Quarterly |

For Priority 1 Applications (Oracle and SQL server databases), the underlisted backup policy would apply

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **HOSTNAME** | **DB/INSTANCE  NAME** | **DATABASE** | **BACKUP TYPE** | **BACKUP FREQUENCY (Disk)** | **BACKUP FREQUENCY (Tape)** | **BACKUP  DESTINATION** | **DISK RETENTION PERIOD** | **TAPE RETENTION PERIOD** | **OFFSITE MOVEMENT** |
| **PRIORITY 1 APPLICATONS** | | | | | | | | | |
| **findb** | **FINDB** | **Oracle** | **RMAN** | **Daily -Full (post-eod)** | **Daily -Full (post-eod)** | **Disk/Tape** | **1 month** | **1 Month** | **Weekly** |
| **EXPORT** | **Daily - Major schemas (pre&post)** | **Daily - Major schemas (pre&post)** | **Disk/Tape** | **1 month** | **1 Month** | **Weekly** |
| **RMAN** | **Monthly -EOM (pre&post)** | **Monthly -EOM (pre&post)** | **Disk/Tape** | **2 years** | **2 Years** | **Monthly** |
| **EXPORT** | **Monthly -EOM (pre&post)** | **Monthly -EOM (pre&post)** | **Disk/Tape** | **2 years** | **2 Years** | **Monthly** |
| **finapp** | **FINTXXXX** | **Oracle** | **RMAN** | **daily –full** | **daily -full** | **Disk/Tape** | **1 month** | **1 month** | **Weekly** |
| **EXPORT** | **daily -full (pre&post)** | **daily -full (pre&post)** | **Disk/Tape** | **1 month** | **1 month** | **Weekly** |
| **RMAN** | **Monthly -EOM (pre&post)** | **Monthly -EOM (pre&post)** | **Disk/Tape** | **2 Years** | **2 Years** | **Monthly** |
| **EXPORT** | **Monthly -EOM (pre&post)** | **Monthly -EOM (pre&post)** | **Disk/Tape** | **2 Years** | **2 Years** | **Monthly** |
| **XXXX-chd-db.XXXXXXXX.local** | **DePotterSch** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **SchVirtualPayment** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **TotalNigReport** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-app.XXXXXXXX.local** | **UnilagDb** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-db.XXXXXXXX.local** | **BranchPay** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **FarmerDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **NUBAN** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **TreasuryBill** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **OauDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-db.XXXXXXXX.local** | **napsgateway** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **remIT GRCtp** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **remIT GRCtp\_OLD** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXXDirectDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-epay.XXXXXXXX.local** | **EKSG** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **LASG** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **OSSG** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **PLSG** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-ib-db.XXXXXXXX.local** | **CorporateInternetXXXXingDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **MobileXXXXingDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **RetailInternetXXXXingDB** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **RetailInternetXXXXingDB\_AddOn** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-micr.XXXXXXXX.local** | **BtsWeb** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-nibbsdb.XXXXXXXX.local** | **NIBBS** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-via-d.XXXXXXXX.local** | **ViaCard\_Live** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXX-hq-ib-test.XXXXXXXX.local** | **Voyager (Western Union)** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **XXXXfep** | **Postcard** | **MSSQL** | **Full** | **Daily** | **weekly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **Postilion** | **MSSQL** | **Full** | **Daily** | **weekly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |
| **postoffice** | **Postilion Office** | **MSSQL** | **Full** | **Daily** | **Monthly** | **Disk/Tape** | **1 month** | **1 Year** | **Bi-Monthly** |

**12.5 Disaster Recovery (DR) Plan**

The Disaster Recovery Plan preparation process includes several major steps as follows:

1. Identify Systems and Applications currently in use
2. Analyze Business Impact of technology downtime
3. Determination of critical recovery time frames (Recovery Point Objective and Recovery Time Objectives)
4. Document Recovery Team Organization and Responsibilities
5. Develop and Document Emergency Procedures
6. Document Training & Maintenance Procedures

The Backup and DR policy shall fulfill the requirements of XXXX Business Continuity Policy

# 13. Collaboration Service: User Access Policy

#### 13.1 Background

Workplaces the world over are changing. Teams have become more distributed. Employees need productivity tools that enable them to work from virtually anywhere. Yet, in spite of significant investment in technology within the Enterprise, users still struggle to stay connected with colleagues and the business.

Slow innovation in traditional technologies such as telephony force users to choose other media for collaboration and communication creating a need for IT professionals to deliver new capabilities in an integrated, cost-effective, and secure manner.

Microsoft Lync connects users in new ways, regardless of their physical location. The latest release of the Unified Communications platform delivers a fresh, intuitive user experience that is directly accessible from Microsoft Office applications such as office 365 SharePoint.

brings together the different ways people communicate in a single interface, deployed as a unified platform and administered through a single management infrastructure. The unified nature of the system helps reduce costs and facilitates rapid user adoption.

**Why Digital Collaboration?**

* **Control costs:**  Voice over IP (VoIP) enables communications among geographically dispersed company locations without long distance charges. Integrated audio, video, and Web conferencing helps reduce travel costs as well as the cost of third-party conferencing solutions.

* **Improve productivity:**  Rich presence information helps employees find each other and choose the most effective way to communicate at a given time. Instead of e-mailing documents back and forth for approval, workers can rely on real-time collaboration through enhanced conferencing with desktop, application, and virtual whiteboard sharing—or contact a collaborator from within Microsoft Office or other applications. The unified Microsoft Lync 2010 client provides access to enterprise voice, enterprise messaging, and conferencing from one simplified interface.

* **Support the mobile workforce:**  Mobile workers get access to rich Unified Communications tools from practically anywhere with an Internet connection, no VPN needed. An updated Lync Mobile client makes joining and managing conferences, searching the Global Address List, and viewing presence information easy. Rich presence in Lync Server 2010 has been updated with mobile location information, making on-the-go workers easier to find and contact. A single user experience across PC, phone, mobile phone, and browser gives workers more, less complex ways to stay in touch.

* **Gain operational efficiencies:**  By integrating Unified Communications and rich presence into business workflows, latency and delays can be reduced or eliminated. For geographically dispersed teams, group chat can enable efficient, topic-specific, multiparty discussions that persist over time.

* **Be more responsive to customers, partners, and employees:**  Enhanced delegation through Lync 2010, one-click call routing and management features in skype for business for receptionists, and rich presence information in both help ensure that opportunities are routed to the right person at the right time.

#### 13.2 Purpose

The purpose of this document is to define the controls around the usage of collaboration services within the XXXX with the intent secure confidential data, protect system resources, avoid wasteful and costly legal proceedings for the XXXX and protect our corporate image.

**13.3 Scope**

This policy applies to all the use of collaboration services from outside the XXXX’s network.

**13.4 Policy Details**

#### 13.5 Feature Definitions

* Remote Access: Access to collaboration and communication services from outside the network i.e. connectivity through the Internet.
* Federation: Ability to connect with other corporate IM networks i.e. XXXX being connected to users within another XXXX’s network.
* Public IM: Ability to connect with external Instant Messaging networks e.g. AOL, Yahoo, and Skype.
* Enterprise Voice: Access to make inbound, outbound and IDD (international) using IP phones.
* PC 2 PC: Access to instant messaging within the corporate network and inbound calls within the organization but across office locations
* Anonymous Users: Access to audio and video conferencing facilities by non XXXX staff. This feature useful for customers, suppliers and partners.
* View Presence Information: Access to view online status of staff who are signed on.
* Instant Messaging (peer-to-peer): Access to instant messaging facilities within the network.
* Audio/Video Conferencing (peer-to-peer): Access to audio and voice conference calls within the network
* Audio/Video Conferencing: Access to audio and video calls from outside the network.

#### 13.6 User Access Policy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Collaboration Feature** | **EXCO** | **GMs and**  **Above** | **Mobile**  **Workers[[2]](#footnote-3)** | **All staff** | **External Users3** |
| Remote Access | YES | YES | YES | NO | NO |
| Public IM | YES | YES | YES | YES | YES |
| **Collaboration Feature** | **EXCO** | **GMs and**  **Above** | **Mobile**  **Workers2** | **All staff** | **External**  **Users3** |
| Enterprise Voice (Inbound,  Outbound, IDD) | YES | NO | NO | NO | NO |
| Enterprise Voice (Inbound, Outbound) | YES | YES | NO | NO | NO |
| PC 2 PC | YES | YES | YES | YES | YES |
| Anonymous Users | NO | NO | NO | NO | YES |
| View presence information | YES | YES | YES | YES | NO |
| Instant messaging (IM) peer-topeer | YES | YES | YES | YES | YES |
| Audio/video (A/V) conferencing (peer-to-peer) | YES | YES | YES | YES | YES |

# 14. Service Level Management Framework

#### Overview

Service Level Management (SLM) Process is defining, establishing, monitoring and optimizing service quality and service levels of services agreed with the customer. Objectives and framework of the service levels and service quality are defined in the Service Level Management Process.

Service Level Management aims to negotiate Service Level Agreements with the customers and to design services in accordance with the agreed service level targets. Service Level Management is also responsible for ensuring that all Operational Level Agreements and Underpinning Contracts are appropriate, and to monitor and report on service levels.

#### 14.1 Service Level Management

Information Technology Architecture and Strategy manages the process for IT service level management. IT GRC shall define the process strategic goals and allocate all required process resources. IT GRC shall ensure effectiveness and efficiency of the IT service level management process.

##### 14.1.1 Service Levels

Quality of service can be defined by diverse metrics and descriptions. The ideas behind this is to describe the quality of the agreed service. Numerous possibilities for service level definitions are possible and depend typically of the service content:

* + Hours of operations for IT operations
  + Duration of support team issue solution for support teams
  + Number of bugs per line of code in case of software delivered
  + Other

Typically, these metrics need a reference like time period, number of customer, number of users etc. E.g. the SL for IT operations of an IT system could be defined as follows:

* 24 hours / 7 days operation
* 99% availability of the system
* Non-availability only on 2 hours per month

The basic service is described in the Service Level Agreement document signed by both parties.

##### 14.1.2 Service Level Management Process

###### 14.1.2.1 Maintenance of the SLM Framework

This entails the design and maintenance of the [customer agreement portfolio](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#Customer_Agreement_Portfolio), and the provision of [templates for the various SLM documents](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#SLM_Document_Templates).

**Identification of Service Requirements**

This involves collation of relevant information on customer requirements for new services or major service modifications. The [service requirements](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#Service_Requirements) are to be documented and submitted to an initial evaluation, so that alternatives may be sought at an early stage for requirements which are not technically or economically feasible.

**Agreements Sign-Off and Service Activation**

This ensures that all identified service requirements are agreed on and signed off. This process makes sure that all relevant Operational level Agreement ([OLAs)](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#OLA)  are signed off by their [service owners](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#Service_Owner), and that the Service Level Agreement ([SLA](http://wiki.en.it-processmaps.com/index.php/Service_Level_Management#SLA)) is signed off by the customer.

**Service Level Monitoring and Reporting**

This process involves monitoring of achieved service levels and comparing them with agreed service level targets. This information is circulated to customers and all other relevant parties, as a basis for measures to improve service quality.



# 15. Business Relationship Management Framework

#### Overview

Business Relationship Management aims to create/maintain and understand the needs of new and existing customers and also establish a positive relationship between Information Technology and information technology’s customers on a strategic and tactical level.

This framework outlines how customer relationship with IT is to be created and maintained to ensure the right services are provided to satisfy customer requirement and business needs

The Objectives of business relationship management are to:

* Establish a business relationship with customers
* Understand the customers’ needs and value perception
* Establish and formulate business requirements for new or changed services
* Ensure that Information Technology Department meets customers’ business requirements
* Interfere when there is a conflicting situation on an operational level

#### 15.1 Business Relationship Management Processes

##### 15.1.1 Maintain Customer Relationship

This ensures that the IT Department continues to understand the needs of existing customers and establishes relationships with potential new customers.

**Identify Service Requirement**

This ensures that Information Technology Department is able to understand and document the [desired outcome of a service](http://wiki.en.it-processmaps.com/index.php/Business_Relationship_Management#ITIL_Service_Outcomes), and to decide if the customer's need can be fulfilled using an existing service offering or if a new or changed service must be created.

**Sign up Customers to Standard Services**

Capture customer requirements and agree service level targets with customers who request the provision of existing standard services.

**Customer Satisfaction Survey**

This process manages and records customer [complaints](http://wiki.en.it-processmaps.com/index.php/Business_Relationship_Management#ITIL_Complaints_Log) and compliments, to assess the complaints and to instigate corrective action if required. The service complaints procedure and customer feedback form are used to capture feedback from customers on IT service performance.

**Monitor Customer Complaints**

This process continuously monitors the processing status of outstanding customer [complaints](http://wiki.en.it-processmaps.com/index.php/Business_Relationship_Management#ITIL_Complaints_Log) and to take corrective action if required.

##### 15.1.1 Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Maintain Business r Relationship | IT GRC |
| Identify Service Requirement | IT GRC |
| Sign up Customer to Standard Service | IT GRC |
| Customer Satisfaction Survey | CSM |
| Monitor Business Complaints | IT GRC |

##### 19.1.2 Business Relationship Management Process Flow



# 16. Service Complaints Management Framework

#### Overview

#### Service complaints procedure manages and handles internal customer complaints and feedback, in order to deliver a consistent, high-quality, accountable service and customer satisfaction throughout the service lifecycle.

#### 16.1 Process Overview

#### The following key steps are to be followed for all internal customer complaints received by Information Technology Architecture and Strategy:

1. Receive and Classify

This phase ensures that all potential issues are captured by the organisation, and classified for escalation, review and action as required.

* Any complaint, issue or negative internal customer interaction (whether this is formally logged by the customer or not), must be logged and classified for action.

All complaints are to be prioritised as follows:

* Priority 1 – urgent,
* Priority 2, - non-urgent

All Priority 1 complaints must be escalated immediately to the Head of Information Technology Architecture and Strategy.

1. Acknowledge

Ensure that every complaint receives a formal written acknowledgement, containing an expectation of when they will receive a response, and the person dealing with it.

1. Investigate

Follow up all aspects of the complaint, to ensure that the key facts are identified and clarified.

* The priority of the complaint will drive the timescale for completion
* All areas of interaction and communication should be established (who, what, where, when, why etc) and documented where possible.

1. Resolve and Confirm

Ensure that the final resolution is clear and fair. Also confirm the proposed action and resolution with another senior person.

* Ensure that the proposed resolution meets corporate guidelines and does not prejudice IT or XXXX in any unnecessary legal or financial manner.
* Document the proposed action and discuss and agree with the Complaints Manager.
* Discuss and review the solution from both the corporate and customer viewpoint to ensure fairness and clarity.

1. Respond to Customer

Provide the customer with the resolution within the timescales promised.

1. Follow Up

Ensure that complaints are followed up to confirm that customers are satisfied with the response given.

1. QA and Close

Ensure that the IT Department as a whole is aware of complaints and any underlying issues. Plan actions to remove these and prevent future recurrence.

##### 16.1.1 Service Complaints Process Flow



### GLOSSARY AND DEFINITIONS

* Access Control List. A list of entities and their authorized access rights to a resource.
* Authorization. A grant to a requesting entity (computer, system, person or process) for access to a protected system and its resources. Not all entities will have access to all XXXX information. Authorization requirements can be implemented using techniques such as access control lists, file and resource permissions, and digital certificates.
* Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.
* Biometrics. Biological characteristics such as fingerprint, face or retinal blood vessel patterns used by authentication devices to allow an individual access to information, services or other resources.
* Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, customer account records, information about XXXXing transactions, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.
* Data. Coded representation of quantities, objects and actions. The word, “data,” is often used interchangeably with the word, “information,” in common usage and in this policy.
* Digital Certificate. An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.
* Firewall. Either software or a combination of hardware and software that implements security policy governing traffic between two or more networks or network segments. Firewalls are used to protect internal networks, servers and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a notebook computer, and must be configured properly to enable protection.
* Identification and Authentication. The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques, such as user ID, password, personal identification number, digital certificates, ***security tokens*** or biometrics, to enforce I&A, depending upon the level of access control required to protect a particular system.
* Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of data in the XXXX’s databases, the data owner and adapt custodian must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.
* Least-Privilege. A method for assigning privileges in a system. The objective is to assign only those privileges that are necessary to perform the required functions, and ensure that other privileges are not assigned and cannot be improperly accessed. For example, a typical system user should not be assigned rights to read, write and execute all of a department’s files when the user only requires the ability to read a subset of these files to do an assigned job.
* Malicious Code. Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.
* Packet. In networking, a packaging unit for transmitting data that has a defined header and data section. The header includes information for routing the packet to the intended destination.
* Packet Filtering. A process that allows or denies an Internet Protocol (IP) ***packet*** based upon criteria in the packet header. Filtering decisions can be based upon the source address of the packet, the destination address, the protocol and the port. Packet filtering is typically implemented on routers or general-purpose computers acting as routers for a network or network segment. Packet filtering is generally effective to control services like Simple Mail Transfer Protocol (SMTP, used for e-mail transmission), Hypertext Transfer Protocol (HTTP, used for Web page transmission) or Network Time Protocol (NTP, used to synchronize time). For services such as Domain Name Service (DNS, which translates names into IP addresses) and File Transfer Protocol (FTP, used to upload files to and download files from the Internet), the more complex security controls available only in proxies may be required.
* Network User. Any employee of the XXXX, whether in a temporary or permanent capacity, and any other person making use of IT resources on the XXXX’s network, including, but not limited to, a consultant, contractor, advisor or a member of a project team.
* Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security.
* Risk Management. A discipline concerned with the planning, implementing and monitoring of processes for the identification, measurement, control and minimization of security risks to information systems at a level commensurate with the value of the assets to be protected. Risk management attempts to maximize the results of positive events and minimize the results of adverse events.
* Risk Mitigation. A systematic methodology used to reduce risk by employing one of the following risk options: risk assumption, risk avoidance, risk limitation, risk planning, risk transference.
* Router. A network traffic control device that implements network policy and provides a measure of control for traffic entering and leaving a network. Routers help ensure that network traffic reaches its intended destination. During the routing process, routers can implement ***packet filtering*** based on network traffic packet content and discard packets that do not adhere to network policy.
* Security Controls. Management, operational and technical policies, procedures and tools required to achieve and maintain the necessary level of assurance of confidentiality, integrity and availability.
* Security Policy. A written principle or course of action adopted by the XXXX to ensure that its security affairs are conducted effectively.
* Security Procedure. A method of securely conducting business or of accomplishing a task to ensure security in accordance with established XXXX wide security policies.
* Security Token. A portable, physical device that enables pre-approved access to data or systems. An example is a security-enabled key fob.
* System Assets. Information, hardware, software and services required to support the business of the agency, and identified during the risk assessment process as assets that need to be protected.
* Threat. An event with the potential to cause harm to an information technology process or service. A threat can be natural, human or environmental.
* Two-Factor Authentication. Authentication that incorporates two elements. There are three elements of authentication: “what you know” (for example, a password or PIN), “what you have” (for example, a digital certificate or a smart card), and “what you are” (for example, a biometric). Two-factor authentication is commonly used for access to systems that contain data requiring secure access or information when disclosure would cause serious disruption or harm. It is also known as strong authentication, although strong authentication can have more than two elements.
* Users. For the purposes of this policy, users are defined as employees, contractors, temporary personnel and persons in the XXXX who administer or use privately-owned (if authorized) or XXXX-owned computer and telecommunication systems on behalf of the XXXX.
* Vetting Process. A verification process used to validate the identity and trustworthiness of a person who is seeking access to computer systems and networks.
* Vulnerability. A flaw or weakness in system security procedures, design, implementation, or internal controls of business functions supported by technology, processes or facilities which may promote or contribute to a disruption.
* Internet.The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide  TCP/IP. Transmission Control Protocol / Internet Protocol.
* IT GRC.Information Technology Architecture and Strategy Unit]
* Passphrase. Used for public/private key authentication. A passphrase is a longer version of a password. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

# APPENDIX

## A.1 Project Documentation Checklist

|  |  |  |
| --- | --- | --- |
| **Project Name**  **Requesting Unit/Contact Person**  **Start Date – End Date**  **Expected deployment date** |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Document** | **Required/Optional** | **Available (Y/N)** |
| Requirement Specification Document | Required |  |
| Project Initiation Document | Required |  |
| Functional/Technical Specification Document | Required |  |
| Project Budget Plan | Optional |  |
| Project Plan | Required |  |
| Signed UAT Test Scripts | Required |  |
| Training Plan | Optional |  |
| **Developer/Implementer**    **Supervisor**    **Client Engagement Officer/Project**  **Manager**    **Head, IT Governance Risk & Compliance** |  |  |
|  |  |
|  |  |
|  |  |

## A.2 Requirements Specification Template

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Name** | |  | | | | | |
| **Requester (Name/Unit)** | |  | | | **Request Date** | |  |
| **Project Objectives** *(Describe in plain terms what exactly the project is meant to achieve)* | | | | | | | |
|  | | | | | | | |
| **Project Scope** *(Detail the specific project coverage in terms of deliverables)* | | | | | | | |
|  | | | | | | | |
| **Challenge Addressed** (Detail the deficiency/pain being addressed) | | | | | | | |
|  | | | | | | | |
| **Value Proposition** *(Document the value proposition of this project to the business)* | | | | | | | |
|  | | | | | | | |
| **Expected Business Benefit** *(Document expected business benefit in terms of ROI, TAT or Cost savings)* | | | | | | | |
|  | | | | | | | |
| **Functional Requirements** *(List all expected application or system functionality in detail)* | | | | | | | |
|  | | | | | | | |
| **Current Process: AS IS** | | | **Expected Process: TO BE** | | | | |
|  | | |  | | | | |
| **Reporting Requirements** *(List all required reports which will arise as a result of this project, include information around specific fields, report delivery media and frequency)* | | | | | | | |
|  | | | | | | | |
| **Project Security Implications** (List all possible security threats/risks that might arise as a result of this project) | | | | | | | |
|  | | | | | | | |
| **System/Technology Requirements** (List all technology dependencies e.g. software, hardware, tools etc.) | | | | | | | |
|  | | | | | | | |
| **Application Architecture** *(Describe with the help of the client engagement officer details around how the application is envisioned to work)* | | | | | | | |
|  | | | | | | | |
| **Accounting Events** (Detail accounting implications of events that may impact on any account of the XXXX) | | | | | | | |
|  | | | | | | | |
| **Risk Assessment & Mitigation (Determine the quantitative or qualitative value of risk related to the change been requested and the recognized threat.)** | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| **Requester**  **Name:**  **Signature:**  **Date:** |  | | | **Supervisor**  **Name:**  **Signature:**  **Date:** | |  | |
| **Client Engagement Officer**  **Name:**  **Signature:**  **Date:** |  | | | | | | |
| **Developer**  **Name:**  **Signature:**  **Date:** |  | | | **Development Team Lead**  **Name:**  **Signature:**  **Date:** | |  | |
| **Head, IT Governance Risk & Compliance**  **Name:**  **Signature:**  **Date:** |  | | | | | | |
| **CIO**  **Name:**  **Signature:**  **Date:** |  | | | | | | |

**Other Stakeholders**

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **Name** | **Department** | **Signature and Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## A.3 Functional & Technical Specification Template

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** |  | | |
| **Developer** |  | | |
| **Application Front End Functionality***(Describe in plain terms all functionality from the perspective of what is available to the user)* | | | |
|  | | | |
| **Technical Architecture** *(Detail the system design, detail all system components and how they interact)* | | | |
|  | | | |
| **Database Design** *(Describe all database tables, procedures, functions and libraries including server information for servers hosting all databases)* | | | |
|  | | | |
| **Configuration Requirements** *(Document all settings and configuration information required for support. Passwords should be hashed out)* | | | |
|  | | | |
| **System Requirements** *(List all hardware and software interfaces and dependencies)* | | | |
|  | | | |
| **Security Framework** *(List all security parameters and configuration)* | | | |
|  | | | |
| **Client Engagement**  **Officer** |  | | |
| **Developer** |  | **Development Team Lead** |  |
| **Head, IT Governance Risk & Compliance** |  | | |
| **Head, Automation & Innovation** |  | | |

## A.4 Test Script Template

|  |  |
| --- | --- |
| **Project Name** |  |
| **Developer** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Module Summary** *(Describe functionality of module to be tested)* | | | |  |
| **Module Name:**  **Summary:**      **Functionality:** | | | |  |
| **Functionality** | **Scenario** | **Expected Response** | **Actual Response** | **Comments** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4

## A.5 Change Request Template

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Application/Service**  **/Infrastructure Component** | | |  | | | | | | | **Priority** | | | | |  |
| **Requester information** | | | | | | | | | | | | | | | |
| ***Name*** | | | | | | | ***Unit*** | | | | | | ***Signature/Date*** | | |
|  | | | | | | |  | | | | | |  | | |
| **Description – Detailed description of what change should be implemented and why** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Network Components Affected if any** | | | | | | | | | | | | | | | |
|  | **Source Address**  **/Subnet Mask** | **Source Protocol/Port** | | | **Destination Address**  **/Subnet Mask** | **Destination Protocol/Port** | | **Action: Deny/Permit** | | | **Rule: Add/Remove/Modify** | | | **Description** | |
|  | **NONE** |  | | |  |  | |  | | |  | | |  | |
|  |  |  | | |  |  | |  | | |  | | |  | |
|  |  |  | | |  |  | |  | | |  | | |  | |
| **Business Benefits (in terms of ROI, TAT, Cost Savings or other Fiscal benefits)** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Expected impact of change request *(Please specify any/all that apply –* to be filled by Effecting Uni*t)*** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Supervisor Concurrence** | | | | | | | | | | | | **Desired Implementation Date** | | | |
| **Name** | | | | | | | **Signature/Date:** | | | | |  | | | |
| **HOD Concurrence** | | | | | | | | | | | | **Desired Implementation Date** | | | |
| **Name** | | | | | | | **Signature/Date:** | | | | |  | | | |
| **Roll back plan in the event change is not successful (Operational or Technical where applicable)** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Risk Assessment & Mitigation (Determine the quantitative or qualitative value of risk related to the change been requested and the recognized threat.)** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **IT Governance Risk & Compliance: Review Comments** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Change Advisory Board (CAB) Members** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Change Advisory Board (CAB) Recommendations and Comments** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| **Change Advisory Board Sign Off** | | | | | | | | | | | | | | | |
| **Name/Unit/Signature/Date:** | | | | **Name/Unit/Signature/Date:** | | | | | **Name/Unit/Signature/Date:** | | | | | | |
| **Name/Unit/Signature/Date:** | | | | **Name/Unit/Signature/Date:** | | | | | **Name/Unit/Signature/Date:** | | | | | | |
| **Name/Unit/Signature/Date:** | | | | **Name/Unit/Signature/Date:** | | | | | **Name/Unit/Signature/Date:** | | | | | | |
|  | | | |  | | | | |  | | | | | | |
| **Head, Applications Management Signature/Date:** | | | | **Head,Infrastructure Management –Signature/Date:** | | | | | **Head,Information Technology – Signature/Date:** | | | | | | |

|  |  |  |
| --- | --- | --- |
| **Testing of Change ( put comments and the new change to be made here )** | | |
|  | | |
| **Supervisor Concurrence** | | **Implementation Date** |
| **Name** | **Signature/Date:** |  |

## A.6 IT Service Business Impact Grid

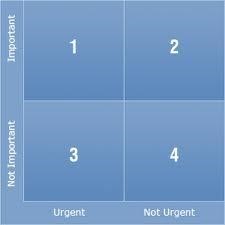
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Application** | **Status** | **Service**  **Component** | **Business Owner** | **IT Owner** | **User Groups** | **Impact** |
| 1 | Intranet | Active | Enterprise  Enablement -  Communication and Collaboration | All Users | ESD | All Staff | 3 |
| 2 | Mandate | Active | Service Delivery  Channels -  Account  Management | Operations | XXXXing  Application  Support | Branch  Coordination  Operations | 2 |
| 3 | Mobile XXXXing | Active | Service Delivery Channels - Mobile  Platforms | Virtual  XXXXing | E-Channels | All Customers | 1 |
| 4 | Xceed | Active | Enterprise  Management and  Control - HRMS | HCM | Non-XXXXing App Support | All Staff | 3 |
| 5 | ShowMate AML | Active | Enterprise  Management and  Control -  Regulatory  Reporting | Branch  Coordination | Non-XXXXing App Support | Operations/Com pliance | 2 |
| 6 | NIBSS Faster PAY | Active | Service Delivery Channels | Corporate Solutions | E-channels | All Customers | 2 |
| 7 | Internet XXXXing | Active | Service Delivery  Channels -  Internet XXXXing | Virtual XXXXing | E-Channels | All Customers | 1 |
| 8 | SMS Alert | Active | Customer  Notification  Services - Alerts | All Users | Business  Automation | All Customers | 1 |
| 9 | AD Updater | Active | Enterprise  Management and  Control | IT | Business  Automation | All Staff | 3 |
| 10 | KSS Portal | Active | Enterprise  Management and  Control | HCM | Business  Automation | KSS Marshals | 3 |
| 11 | ENCOMPAS | Active | Service Delivery  Channels -  Electronic Transfers | Clearing | Non-XXXXing App Support | Clearing Ops | 1 |
| 12 | SWIFT | Active | Service Delivery  Channels -  Electronic  Transfers | Trade  Services | Non-XXXXing App Support | Treasury Ops | 1 |
| 13 | MICR | Active | Enterprise  Enablement -  Cheque Printing | MICR | Non-XXXXing App Support | MICR | 2 |
| 14 | HardCat | Active | Enterprise  Management and Control - Asset  Management | FINCON | Non-XXXXing App Support | FINCON | 3 |
| 15 | MS Exchange 2010 | Active | Enterprise  Enablement -  Communication and Collaboration | All Users | ESD | All Staff | 1 |
| 16 | ATM Plus | Active | Enterprise  Management and  Control | ATM & POS | E-Channels | E-Business IT | 3 |
| 17 | FEP | Active | Service Delivery  Channel -  Alternate  Channels | ATM & POS | E-Channels | All Customers | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Application** | **Status** | **Service**  **Component** | **Business Owner** | **IT Owner** | **User Groups** | **Impact** |
| 18 | Post Card | Active | Service Delivery  Channel -  Alternate  Channels | Cards | E-Channels | All Customers | 1 |
| 19 | PayDirect | Active | Service Delivery  Channels - Payments and  Collections | Corporate Solutions | E-Channels | All Customers | 1 |
| 20 | Remita | Active | Service Delivery  Channels - Payments and  Collections | Corporate Solutions | E-channels | All Customers | 1 |
| 21 | AutoReg | Active | Service Delivery  Channels - Payments and  Collections | Retail XXXXing | Non-XXXXing Apps | All Customers | 1 |
| 22 | AutoPay | Active | Service Delivery  Channels -  Electronic  Transfers | Corporate Solutions | E-channels | All Customers | 1 |
| 23 | Western Union | Active | Service Delivery  Channels -  Electronic  Transfers | Corporate Solutions | Non-XXXXing Apps | All Customers | 1 |
| 24 | RTGS | Active | Service Delivery  Channels -  Electronic  Transfers | Treasury Operations | Non-XXXXing Apps | Operations Treasury Ops | 1 |
| 25 | NEFT | Active | Service Delivery  Channels -  Electronic  Transfers | Operations | Non-XXXXing Apps | All Customers | 1 |
| 26 | XXXX Store | Active | Enterprise  Management and  Control -  Inventory  Management | General Services | Non-XXXXing Apps | All staff | 3 |
| 27 | InfoShare | WIP | Enterprise  Management and  Control -  Reporting and  MIS | MIS | Business  Automation | All Staff | 2 |
| 28 | SCSM | Active | Enterprise  Management and Control - Service  Management | IT | ESD | All Staff | 3 |
| 29 | XXXXDirect | Active | Service Delivery  Channels -  Electronic Transfers | Virtual XXXXing | E-Channels | All Customers | 1 |
| 30 | Card Management System | Active | Enterprise  Management and  Control | Cards | E-Channels | Card Operations | 2 |
| 31 | EPAY |  | Service Delivery  Channels - Payments and  Collections | PSG | E-channels | All Customers | 1 |
| 32 | Post Office | Active | Service Delivery Channels | ATM & POS | E-Channels | E-Business IT | 2 |
| 33 | ExtraSwitch | Active | Service Delivery Channels | E-Channels Operations | E-channels | E-Business  IT | 2 |
| **#** | **Application** | **Status** | **Service**  **Component** | **Business Owner** | **IT Owner** | **User Groups** | **Impact** |
| 34 | PayOutlet | Active | Service Delivery  Channels -  Electronic  Transfers | Corporate Solutions | E-channels | All Customers | 1 |
| 35 | XXXXPay | Active | Service Delivery  Channels -  Electronic  Transfers | E-Business | E-channels | All Customers | 1 |
| 36 | CashCard Navigator | Active | Service Delivery Channels | Cards | E-channels | Cards | 2 |
| 37 | MS Forefront | Active | Enterprise  Enablement -  Support Services | IT | ESD | All staff | 1 |
| 38 | MS Lync | Active | Enterprise  Enablement -  Communication and Collaboration | IT | ESD | All Staff | 3 |
| 39 | Office  Communicator  2007 | Active | Enterprise  Enablement -  Communication and Collaboration | IT | ESD | All Staff | 3 |
| 40 | BlackBerry  Enterprise Server | Active | Enterprise  Enablement -  Communication and Collaboration | IT | ESD | All Staff | 2 |
| 41 | CSM Tool | Inactive | Enterprise  Management and  Control | CIC | Business  Automation | All Customers | 2 |
| 42 | Appraisal Tool | Active | Enterprise  Management and  Control - HRMS | HCM | Business  Automation | All Staff | 2 |
| 43 | Loan Tracker | Active | Enterprise  Management and  Control | Retail XXXXing | Business  Automation | Retail XXXXing  Central  Operations | 3 |
| 44 | NUBAN A/C Search | Active | Enterprise  Management and  Control | CIC | Business  Automation | All Customers | 2 |
| 45 | UTME Collection  Tool | Active | Service Delivery  Channels - Payments and  Collections | Operations | Business  Automation | Operations | 1 |
| 46 | XXXX Call Over | Active | Enterprise  Management and  Control | Operations | Business  Automation | Internal Control Operations | 3 |
| 47 | i-Capture | Inactive | Service Delivery  Channels - Payments and  Collections | Operations | Business  Automation | Operations | 1 |
| 48 | Alert manager | Active | Enterprise  Management and  Control | E-Business | Business  Automation | VB and EFT | 3 |

**Notes**

- Impact is numbered 1 to 3 with 3 as the lowest in terms of business impact.

## A.7 Change Request Priority Table



## A.8 Change Categories Guide

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Request for Change** | **Request Fulfillment** |  | **Incidents** |
| -  -  -  -  - | Requests for new features on applications  Changes to IT assets (Servers, Communications infrastructure, power infrastructure)  Changes to Databases  Changes on the messaging platform  Changes to support services  (Active Directory,  SharePoint)  Change in service catalogue and other importan t Documentation | - Request for a new service (new OS, new user profile, new application, new PC) | - | Service failure |

1. CAB meetings are scheduled to hold weekly and an Emergency CAB (E-CAB) can be constituted to review emergency changes if required. [↑](#footnote-ref-2)
2. Users who need to have for business reasons need to have access to network resources from remote locations 3 Customers, Suppliers or Partners who need to interface with the XXXX using collaboration services [↑](#footnote-ref-3)