IT CHANGE MANAGEMENT PROCESS

WesBank Group IT

Document Background

DOCUMENT OWNER	Head : Quality Assurance & Service Management
TITLE	IT Change Management Process
REFERENCES	• IT CHANGE & RELEASE MANAGEMENT POLICY • INCIDENT AND PROBLEM MANAGEMENT POLICY • FSR IT SECURITY POLICY • ITIL

Revision History:

Modified Date	Author	Version	Description of Changes
Mar 2014	Pieter Oosthuizen	V1	New Document Version
Oct 2016	Constance Matsi	V2	Updated Version
Oct 2016	Nicolene Ray	V2	Updated Version
Oct 2016	Mfundo Nkosi	V2	Updated Version

Document Approval

Name	Title	Signature	Date
Thabang Legae	WesBank Group CIO		
Bessy Mahopo	WesBank Office of Group CIO		
Andries Potgieter	WesBank IT – Head: Infrastructure & Operations		
Gordon Marriday	WesBank IT – Head: QA & Service Management		
Kim Van Staden	WesBank IT – Head: Application Development & Maintenance		
Shannon Naidoo	WesBank Group IT – Head: Business Strategy & Architecture		
Olwethu Sinxoto	WesBank Group IT – Head: IT & Cyber Security		
Denzil Kisten	WesBank CIO Head Office Support Services		
Nenzeni Duma	WesBank CIO Corporate		
Kobus Hechter	WesBank CIO RoA		
Mandi Scott	WesBank CIO Motor		

Contents

1. Preface

The purpose of this document is to outline the procedures that govern the Change Management process in Wesbank Information Technology (IT). This document describes how to use the procedures and provides a definition of the management controls required and some rationale for instituting those controls.

2. Objective

Change Management is the process of planning, coordinating, implementing and monitoring changes affecting any production platform within Information Technology's control, within Wesbank Information Technology Divisions

The objectives of the Change Management process are to:

- Ensure that changes are made with minimum disruption to the services IT has committed to its users.
- Support the efficient and prompt handling of all changes.
- Provide accurate and timely information about all changes.
- Ensure all changes are consistent with business and technical plans and strategies.
- Ensure that a consistent approach is used.
- Provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services.
- Reduce the ratio of changes that need to be backed out of the system due to inadequate preparation.
- Ensure that the required level of technical and management accountability is maintained for every change.
- Monitor the number, reason, type, and associated risk of the changes.

It is important that changes in the IT environment be executed in a controlled manner in order to assess the need of the change, mitigate the risks of interruptions to service during prime access hours and maintain a repository of knowledge on various implemented changes within the WesBank IT environment.

3. Purpose

The purpose of this document is to provide the procedure guidelines on how WesBank will record, evaluate, authorise, planned, tested, implemented, documented and reviewed in a controlled manner.

Manage changes in a standardized manner to ensure that changes to Wesbank's systems do not unintentionally diminish security or interrupt system stability.

4. Procedure

The IT Change Management procedure for the WesBank Information Technology Divisions defines how the change process is implemented in all of the IT platform environments.

The objectives of the operating procedures, in addition to those detailed above are to:

- Provide documentation that allows Wesbank IT management to understand, at any point in time, the **configuration of the IT environment**.
- Minimize the **bureaucratic impact** on the development community while maintaining control of the environment.

Activities of the Change Management Process at WesBank include:

- Receiving change requests from the Request for Service process
- **Determining** whether or not the change is in the **best interests** of WesBank
- **Assigning** the change to **resources** within IT for **solution identification**, sizing and risk analysis
- **Accepting or rejecting** the requested change
- Assigning the change to solution **deployment resources**
- **Reviewing** the solution prior to implementation
- **Scheduling** the change
- **Communicating** change status as required to all interested parties
- **Closing** the change

5. Scope Inclusion

The scope of this process is to ensure the management of any installation or alteration to hardware, network, system or application software, procedure or environmental facilities which adds to, deletes from or modifies the service delivery environment.

6. Scope Exclusion

Activities required to developing, testing and deploying the change.

7. Change Management Standards

a) All substantive changes to the IT Environment must **adhere to the Wesbank IT change Management process**. A substantive change has the potential to affect the ability of users and systems to interact with each other.
b) All changes to the production systems within IT will have a **corresponding set of documentation that describes the change**, the **business reason** for the change and the disposition of the change. This includes emergency changes.
c) The **risk** and/or **impact** ratings of the requested change will determine which of the four phases of the **change workflow** (Analysis, Design, Testing and Implementation) will be required to promote the change into production. For "minor" changes only Analysis and Implementation will be required.
d) Only **authorized approvers** will be able to accept a change request into the Change Management process.
e) Anyone with **valid Release Notes** will be able to enter a change into the Change Request process. Only **authorized approvers** will be able to accept a change request into the Change Management process.

7.1 Types of Changes

The Change Management Procedure applies to all types of changes related to the WesBank IT Environment or Platform. The following is a description of each of the **types of changes** that can take place and the rules that apply to each.

A. **Application Software Changes** –

- Changes to any application **code** that is running on or linked to by any **hardware or software/service** in the WesBank IT environment. These changes are typically made to in the IT application environment to:
  i. **Enhance the function (New/Enhancement)** or **performance** of or
  ii. To **fix a known error** (**Maintenance/Bug Fix or Emergency/IT Critical)**.
- These changes cannot be implemented without approval of the **owner of the application** and cannot be requested by any Developer/Systems Analyst/Technical Resource other than the one assigned to the program.
- Assignment of Risk Category Level of the change is to be a joint effort of both the owner and the Change Implementer.
- Changes that may have an impact on the IT support resources**. If the changes affect the system, users or the support staff there is a requirement to enter it into the Change process.**
- If the change is made for the exclusive benefit of the requester and if failure could not affect anyone else, that change would be exempt from the Change Process. However, when **testing time** is required on **a production system**, a change request form is required.
- **Visual Image Changes** – Changes to the "artistic" presentation of web pages are not required to make entries into the Change Management system. Changes to **"Active" areas of the web page are required** to use the WesBank Change Management procedure

B. **Infrastructure Changes** –

- All **WesBank IT** and IT support **Hardware installations, Infrastructure/ Software Upgrades, decommissioning and relocations** are controlled by the Change Management Procedure. This activity can be requested by anyone but must have the **approval of the Operations Manager.**
- **Network Changes** - All installations, **decommissioning and all relocations** of equipment used for IT teleprocessing communications are entered into the change process. This includes all routers, switches and telephone lines as well as Personal Computers if they are connected to the network.
- **Environmental Changes** – Environmental changes normally involve **the facilities associated with the IT Installation**. These facility (**including Shared Facilities with FNB)** changes include items such as generator testing, raised flooring, security, electricity, air conditioning, plumbing and the telephony system for voice and data. For example, when there is planned weekend power outages initiated, this information is submitted to the Change Management Process prior to the scheduled outage and communicated to management, staff and the user community.

7.1.1 Change Risk and Impact

The following guidelines for definition of Change risk levels are provided for consideration during the planning cycle. It must be clearly understood that these requirements are the minimum for each of the defined levels. The Requester may wish to plan additional lead times, documentation or reviews to insure that targets can be met and planned implementation schedules can be achieved.

All changes are tracked, correlated and used for management reporting, statistics, trending, etc., to identify when and where additional resources should be provided. For any change that fails, the Change Requester must enter an explanation in the comments section of the Change Record for that change and notify the Change Coordinator. The Change Coordinator will then close the change with the appropriate close status. If the change is to be attempted at a later time, the Change Requester should re-enter the change with the new date. Changes that cause a Platform outage will be reviewed at a CAB Level.

7.1.1.1 Daily Changes

Daily Changes are pre-approved / standard changes that are considered **Low Impact and Low Risk** changes which will be filtered through the ECAB for approval. It is the responsibility of the Requester to notify any areas of a potential impact. The ECAB will evaluate the request to agree impact and risk. Some application such as

- Application Software Changes = Maintenance/Bug Fix
- Infrastructure Changes = Maintenance

7.1.1.2 Emergency Changes

Emergency changes are those changes that are vital in order to ensure that IT's committed service levels are maintained, **High Impact and High Risk.** An Emergency change should not be used in order to bypass the appropriate lead-time for a change that has been entered into the system.

A Change that must be introduced as soon as possible, to resolve a Major Incident.

These types of changes proceed to the implementation phase when the requester's manager and the **IT EXCO and Business CIO** acknowledge that an **Emergency** exists and authorize the modification planned. These changes will be post-reviewed to assure successful implementation, along with identification of any external impacts or new requirements. Post-review will also evaluate the reason for the Emergency change request and try to determine a way of eliminating this requirement in the future. The post-review will also evaluate if, in fact, the change addressed a real or a perceived emergency condition. In all cases, the review must determine if additional action is required, what that action should be and who will be responsible for the action.

How do you know that the change falls under Emergency?

- Is the change needed to restore immediate service to the end user?
- Is the change necessary to fix an existing problem immediately?
- Is this a change that must be installed immediately but the need for it was not recognized early enough to be approved through the regular process?
- Must this change be done immediately to fix problems for jobs that ABENDed/Failed during the previous night or are required to run in order to bring up on-line systems?
- When a stop, start, or restart of a service is required, which are the dependent services are also affected during core business hours?
    - Starting a service does not automatically restart its dependent services. (Risk & Impact)
    - Changing the default service settings may prevent key services from running correctly. These services are required for the operating system to function properly. (Risk & Impact)
    - If a reboot is required to correct a fault but no changes are being made then the reboot should be tracked against the recorded Incident. (Preventative measures included)

Communication is to be sent to respective Stakeholders for Change Awareness. An Emergency Change Record to be raised later, linking the associated incident to the change.

It important is to ensure users affected are informed in advance of the planned outage and the activity is recorded against the CI, to prevent interrupting other CIs or unsuspecting users working in the middle of an important business transaction.

7.1.1.3 Business / IT Critical

Business and IT Critical changes are those changes are those changes that are a result of a business/IT need and must be installed prior to the required lead-time **High/Medium Impact and High/Medium Risk.**

- (Urgent requests from Business that are implemented outside the release cycle)

Changes that are required quickly due to a pressing need such as legal requirement or a business need but are not related to restoring service

Preventative Maintenance or Urgent request from IT that could not wait for the planned maintenance slot

These types of changes proceed to the, build, test and implementation phase outside of the planned release planned dates when the requester's manager and the **IT EXCO and Business CIO** acknowledge that an a **Business / IT Criticality** exists and authorize the modification

planned. These changes will be post-reviewed to assure successful implementation, along with identification of any external impacts or new requirements. Post-review will also evaluate the reason for the Level E change request and try to determine a way of eliminating this requirement in the future. The post-review will also evaluate if, in fact, the change addressed a real or a perceived emergency condition. In all cases, the review must determine if additional action is required, what that action should be and who will be responsible for the action.

7.1.1.4 Weekly Changes (Normal)

A Normal Change would have a **High/Medium Impact and High/Medium Risk** on IT services if a problem occurs during install. The install time is lengthy and the backout is very difficult or impossible.

Normal Change Requests are to be entered into the Change Management Data Base (Tool) at **least thirty days to 2 weeks in business** days prior to the planned implementation date.

The Requester or representative for **Normal Change** is required to attend the **CAB** immediately prior to implementation so that any questions or concerns may be addressed.

Whenever a **Normal Change** must be expedited to address a critical timing situation, a special meeting must be held. To expedite a **Normal Change**, all parties that may be affected by this change **must** be present or represented at the **CAB.** It is the responsibility of the change requester to assure attendance by the required groups or individuals. If the required groups or individuals cannot be assembled, the change cannot be expedited and an escalation will be required.

How do you know that the change falls under Normal Change?

- From the end user's eyes, is it possible for the change to have a major impact on services if problems occur?
- Is the change visible to all end users?
- Is this a high-risk change?
- Is this the first time this change has been done?
- Is the change difficult or impossible to backout?
- Is it extremely difficult to install the change?
- Does the change involve a lengthy install time?
- Would failure of the job/program being changed stop the flow of all jobs for critical files or an application system?

7.2 Status of Changes

The following status codes are used to reflect the status of a change request:

- **Open** – The change has been received and accepted but has not been assigned
- **In-Progress** – The change has been received, acknowledged and assigned. Work is in progress to fulfill the change request.
- **Approved** – The business and technical assessments have been completed and the change has been approved and committed to the change scheduler.

- **Rejected** – The change has been rejected and will be routed back to the Request for Service process and sent back to the customer with an explanation and a recommended course of action.
- **Canceled** – The change request has been canceled. No Longer required after Approval.
- **Withdrawn** - No longer required before Approval
- **Closed** – The change request has been closed.
    - **Successful** - No issues experienced. Successfully deployed. Post Testing successfully tested
    - **Successful with Issues** - Deployed successfully but later issues raised due to the deployment
    - **Unsuccessful** - Deployment did not provide the desired result as per the Request
    - **Backed Out** -Started deployment and experienced issues during deployment. Rolled back code to the previous version after successful / unsuccessful deployment

7.2.1.1 Authorisation for a Change

Change Type Approval Matrix					
Approval, depending on the scope and impact of the proposed change, **approval by a member of** the following are required.	**Emergency**	**Urgent**		**Normal**	**Daily**
		IT Critical	**Business Critical**		
Manager/Team Lead of the user department requesting the change	**R**	**R**	**R**	**R**	**R**
Business and Business CIO / Process Owner or his designee	**I A**	**I A**	**A**	**A**	**A**
Head of Development	**C A**	**C A**	**I**	**A**	**I**
Head of Quality Assurance	**C**	**C**	**I**	**C**	**I**
Head of IT Operations	**C A**	**C A**	**I**	**A**	**I**
Quality Assurance Manager	**C**	**C**	**C**	**C**	**C**
Application Development Manager	**A**	**A**	**C**	**C**	**C**
Operations Manager / Network & Technical Services Manager.	**A**	**A**	**C**	**C**	**C**
Change Management	**C**	**C**	**C**	**C**	**C**

R is Responsible = Owns the problem

A is Accountable = to whom "R" is Accountable - who must sign off (Approve) on work before it is effective

C is Consulted = to be consulted - has the information, resources or capability to complete the work

I is Informed = to be informed - must be notified of results, but not consulted

7.3 Roles and Responsibilities

7.3.1 Change Advisory Board (CAB)

The Change Advisory Board (CAB) is the body of people responsible for tracking and evaluating all changes based on their urgency and strategic value to the business, ensuring business risk is understood and all relevant documentation is available to ensure successful changes are made.

The Change and Release Manager, or delegated authority, will chair any CAB meetings.

The CAB will compose of base members and may potentially include additional member i.e.:

- User manager(s)
- Contractor's or third parties' representatives, e.g. in outsourcing situations
- Other parties as applicable to specific circumstances

It is important to emphasize that the CAB:

- Will be composed according to the changes being considered
- May vary considerably in make-up even across the range of a single meeting

7.3.2 CAB Members

A CAB Meeting is held once a week to approve and discuss changes and facilitate communication.

All changes should be submitted before _____ to be considered in the CAB and eligible for the next release date.

It is compulsory for the following people/ positions to attend CAB meetings

1. Changes to be assessed and approved
    1. Include:
        1. Planned or requested changes for the next week
        2. Pending changes not approved at previous CAB meetings
        3. Unsuccessful changes that are being resubmitted
    2. For each change assessed:
        1. Why: Defined expected outcome and benefit?
        2. Risk analysis?
        3. Requested date and time? If not in an agreed maintenance window, have users approved the downtime?
        4. Implementation plan including internal and supplier resources?
        5. Post-implementation verification plan?
        6. Backout plan?
        7. Are there any pre-requisite changes?
        8. What other changes or projects depend on this?
        9. Decision: approve or postpone the change.
2. Review and confirm the "Forward Schedule of Changes" (FSC)
    1. Approved future changes by date
3. Changes implemented in the past week
    1. Emergency changes: why? how to avoid in future?

2. Changes that occurred without any authorisation: who implemented? Why? How to prevent in future?
3. Changes with any negative impact: why? how to avoid impact in future?
4. Unsuccessful, backed out changes: why? What lessons learned?
5. Successful changes: just note them (Were they communicated to everyone affected?)
6. Is a Post-Implementation Review (PIR) required for any of the above?

4. Review previous PIRs
5. Review actions agreed from any previous lessons learned
6. Discuss Standard Changes

7.3.3 CAB Meeting Agenda

- Confirmation of previous minutes
- Changes to be assessed and approved
- Review and confirm the changes authorized for the next release *"Forward Schedule of Changes" (FSC)*
- Review changes implemented in the past week – Including Failed, and Successful but exceeding slot allocation
- Review previous PIRs (Post-Implementation Review)
- Review actions agreed from any previous lessons learned
- Discuss Standard Changes

7.4 Emergency Change Advisory Board (ECAB)

The Emergency Change Advisory Board (ECAB) refers to the body of people responsible for evaluating emergency and business critical changes, ensuring business risk is understood and the decision to go ahead is made timeously.

Every request for an Emergency change is based upon the initiators assessment of the Business impact and urgency of the change. The priority assigned to the RFC is derived from the agreed impact and urgency and is reached by consensus by the ECAB members. The risk evaluation associated with the emergency change request is of paramount importance and includes all facets of Service Management including, but not limited to, business governance and risk assessment, security, IT service continuity, service availability, the perceived business financial impact which includes business and customer confidence.

7.4.1 Members

7.5 Reports

The agreed reports for Change Management are:

- Number of submitted change requests by classification – standard, normal and emergency per week / month
- Number of change requests successfully implemented at first implementation – Weekly / monthly
- Number of non-authorised changes to services detected weekly / monthly
- Number of change requests raised against each service that was updated / modified per month
- Number of change requests sent back to initiator for insufficient information queries.
- Number of Failed changes per week / month

- Status log of all submitted change requests being evaluated by CAB or ECAB – daily / weekly

7.6 Change Manager

The main duties of the change manager, some of which may be delegated, are listed below

- Receive logs and allocates a priority, in collaboration with the initiator, to all RFC's; rejects any RFCs that are totally impractical. Communicates with initiator on reasons where rejected.
- Tables all RFCs for a CAB meeting, issues an agenda and circulates all RFCs to CAB members in advanced of meetings to allow prior consideration.
- Decides which people will come to which meetings, who get specific RFCs, depending on the nature of the RFC, what is to be changed, and people's areas of expertise.
- Attends all CAB and ECAB meetings.
- After consideration of all the advice given by the CAB or ECAB, authorizes/implements acceptable changes.
- Update the change log with all progress that occurs, including any actions to correct problems and/or to take opportunities to improve service quality.
- Analyses change records to determine any trends or apparent problems that occur; seeks rectification with relevant parties
- Closes RFCs.
- Produces regular and accurate management reports.

7.7 Cut off days and timings

Timings Guidelines	Day	Start Time
Meetings		
CAB	Wednesdays	9:00 AM
Daily requests, Emergency, IT/ Business Critical to be represented in ECAB	Daily	9:30 AM
Release Planning	Mondays Wednesdays	10:00 AM
Approvals		
ECAB Changes to		
ECAB Changes Signoff / Approved	Daily	15:00 PM
Deployment and Plan items for Weekly Friday Release to be logged	Tuesday	12:00pm
CODE into QA for Weekly Friday Release / Enhancements	Wednesdays	10:00 AM
Weekly Friday Release / Enhancements (DEV/QA/OPS)	Friday	12:00 PM
Deployments		
Auto On line / Auto Card	Tuesday Friday	17:00 PM 17:30 PM
Business Intelligence (BI)	Daily	13:00 PM 17:00 PM
NEW WHOLESALE FINANCE (NWSF)	Daily	16:00:PM
VAPS	Friday	20:00 PM
SOA	Friday	20:00 PM
WesBank on line (WOL)	Friday	20:00 PM
Credit on line (CRO)	Friday	20:00 PM
COR, SMAC, Acquisition (SPIF) (Due to Direct Axis working hours. Batch to start after deployment refresh)	Friday	21:00 PM
Fleetactiv / MS Application	Tuesday Friday	17:00 PM 18:00 PM
Infrastructure / Maintenance	Tuesday	17:00 PM
Daily Changes	Daily	17:00 PM
Bimonthly Saturday Release (Due to Direct Axis and other Business working hours)	Saturday	14:00 PM
Month end Freeze	Starts on the 25th of every month	