Change Management

Process Policy

This policy is owned by the General Manager of Integrated Service Delivery.

Ownership has been delegated to Service Management Process Delivery.

Date:	29 January 2013
Version:	1.0
Status:	Final

Table of Contents

Change Management Process Policy

1. Purpose

A technology change is defined as “the addition, modification or removal of anything that could have an effect on IT Services.”

The purpose of this policy is to ensure that:

- Standard methods and procedures are used for the efficient and prompt handling of all changes, allowing both technology and the business to plan accordingly
- All changes to service assets and configuration items are recorded in the Configuration Management System
- The decision making process balances the need for change with the risk and impact of change to ensure business benefit is delivered and business risk is minimised.

2. Governance

This process policy is subject to all associated technology policies and procedures which include, but are not limited to the Group Information Security Policy and the Group Data Quality Policy.

Failure to comply with this policy places the organisation at undue risk. As an ADI (Authorised Deposit-taking institution), NAB is obligated to comply with the regulations set out by relevant regulators (e.g. APRA). Compliance with IT policies and procedures forms part of these regulatory obligations. There are no exemptions to this policy.

All process participants must understand their role and accountabilities. People Leaders are accountable to ensure that new staff are provided with appropriate induction and support to ensure this.

Breaches will be dealt with in accordance with company policies, including the Code of Conduct. For Managed Service Providers and Delivery Partners, it could result in a breach of contract.

3. Scope

This process policy applies to all technology components (all of the hardware, software, networks, facilities) in the NAB technology controlled environments as well as technology components hosted or managed by external Service Providers on behalf of NAB.

It is the accountability of the NAB Business Unit owning the relationship with external Service providers to ensure that this policy is adhered to.

4. Mandatory Process Training

All process participants are required to successfully complete relevant process training and assessments. The training curriculum and assessment criteria are owned and managed by the Process Owner. For more detailed information please see: http://go/smpd

5. Policy Statements

The following policy statements represent NAB's position with respect to the prudent management of technology services to ensure NAB meets the obligations to customers, community, shareholders and regulators.

The policy statements are aligned to COBIT V5 IT Controls and related standards including ISO/IEC20000-1 IT International Standard for Service Management, and ITIL V3 IT Service Management practices set.

This alignment provides a reference point for governing technology policies and processes to facilitate auditability.

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
CHG01	All technology change activity must be carried out in accordance with the Change Management Procedure by opening and managing appropriate Change Records through their lifecycle using the NAB Service Management tool. Failure to do so will be viewed as Unauthorised Change and escalated accordingly.	BAI06.01	Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	Unauthorised changes being applied to NAB's controlled environments No impact assessment carried out to assess business need vs. business risk No milestone management of an implementation to detect and address issues in a timely manner No formal categorisation/prioritisation on changes Urgent changes not authorised appropriately	Increasing number of preventable incidents resulting from unmanaged change causing conflicts with planned/managed changes Without impact assessment, unable to determine the legal, regulatory or contractual implications of a failed change. Without an effective backout plan to activate during the implementation when expected milestones/success criterion is not met, there will be an increase in preventable service impacts resulting from failed implementations.
CHG02	Change planning must include appropriate assessment of risk and impact to service. The CMDB and Service Management tools must be used to conduct an impact analysis of the proposed change activity on CIs and ensure this is accurately reflected in the Change Record.				
CHG03	Change implementation planning must include checkpoints and verification testing to test				

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
	for success. These will form go/no go decision points and criterion for backing out the implementation. The proven backout plan must be accurately reflected in the Change Record. See also CHG11				Without effective categorisation, changes may not accurately reflect the business risk Urgency may override standard governance and scrutiny resulting in business impacts
CHG04	Appropriate testing must be completed prior to change implementation. Evidence of this and any residual risk must be contained in the Change Record. Testing must be conducted in compliance with appropriate Segregation of Duties. Testing results must meet stakeholder approval – which must be evidenced in the Change Record.				
CHG05	Any change which needs to be expedited urgently for business reasons and can not meet standard lead times must be approved by appropriate senior				

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
	management and comply with the Change Management Procedure.				
CHG06	Any change made to resolve or prevent a critical incident must comply with the Emergency Change Procedure. Emergency Changes may be logged retrospectively if there is insufficient time to do so prior to the change taking place to resolve or prevent a service impacting incident. This situation will be under the strict governance of the Incident Management process.	BAI06.02	Carefully manage emergency changes to minimise further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorised after the change.	Inaccurate information being used in Emergency change situations No definition of what constitutes an emergency change No documented procedure for emergency changes No monitoring or testing of emergency change No tracking of any change	Incident Management decisions are based on incorrect information, potentially making the situation worse. Unable to determine priority of change which may lead to delays in remediation or execution of change. Without testing unable to monitor change and ensure the change is successful.
CHG07	The status of a Change Record must be updated as the Change moves through the stages of its lifecycle. This includes	BAI06.03	Maintain a tracking and reporting system to document rejected changes, communicate the status of approved	Status of changes not tracked accurately No performance	Impact to service availability due to unmanaged, uncontrolled change

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
	notification to relevant stakeholders.		and in-progress changes, and complete changes.	metrics of changes status to enable management review	Business benefit not realised and business risk increased
CHG08	If a Change Record is rejected – the reasons for rejection (at any stage in the lifecycle) must be recorded in the Change Record and the Change Owner notified.		Make certain that approved changes are implemented as planned.	Lack of governance around management of change Business verification of change success may not be carried out effectively	
CHG09	All Change Records must meet the data quality criteria as specified in the Change Management Procedure.				
CHG10	All Change Records must be fully approved before implementation activities commence (with the exception of Emergency Change activity authorised by Incident Management for immediate implementation, in response to a critical incident). Any Change implemented without full approval will be				

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
	deemed as Unauthorised Change and escalated accordingly.				
CHG11	Appropriate post-implementation testing including business verification must be conducted as part of the change activity. Plans and details of these activities must be included in the Change Record.				
CHG12	All required CMDB updates must be completed before the Change Record is closed.	BAI06.04	Close and document the changes. Whenever changes are implemented, update accordingly the solution and user documentation and the procedures affected by the change.	Change record status is not updated or change records are not closed Support processes and documentation not updated User processes and documentation not updated CI (component or	Accurate change implementation status is unknown impacting ability to manage the environment Completed change records which remain open clutter the change schedule making it difficult to assess true risk of new changes being reviewed
CHG13	The Change Record must be managed throughout its entire lifecycle. Closure details and change success or failure status must be recorded in the Change Record.				
CHG14	Appropriate updates to user and support				

Policy Ref	Policy Statement	COBIT Ref	COBIT Statement	Risk Factor *(control failures or causes that lead to the risk materialising)*	Risk *(actual risks that can eventuate if the policy statements are not complied with)*
	processes and documentation must be included as part of the delivery of the change.			Service) information in the CMDB is not maintained	Change reporting will be inaccurate Lack of effective transition of the change leading to impaired ability to support the changed components Decreased ability to proactively manage IT infrastructure

6. References

Reference	Link
AUR Change Management Intranet Site	http://intranetweb.au.thenational.com/site103/c4100.htm
Wholesale Change Management Intranet Site	http://intranet.global.thenational.com/Units/Services/Technology/ATLAS/ServiceMan/Pages/ChangeManagement.aspx
BNZ Change Management Intranet Site	http://bnzintranet.nz.thenational.com/bnz/intranet/channelpolicyteaser/home/0,2690,2308_145549748,00.html
SMitN Change Management Intranet Site	http://teams.national.com.au/workspaces/SMiTN-ProcessMaps/SMiTN%20source/Web%20Content/index.htm
Incident Management Process Policy	http://teams.national.com.au/workspaces/TechOpsServiceManagement/SMP/Process%20Library/2.0%20Incident%20Management%20Process%20Policy.pdf
Group Information Security Policy	http://intranetweb.au.thenational.com/group_policy_central/Group%20Information%20Security%20Policy.pdf
Group Data Quality Policy	http://intranetweb.au.thenational.com/group_policy_central/5308.htm
Enterprise Glossary	http://teams.national.com.au/workspaces/FSO/EIDM/TeamDocuments/Glossary.aspx

7. Definitions

For a complete list of definitions, please refer to the Glossary of Terms within the Enterprise Glossary.

8. Document Reviewers

Version	Review Date	Role / Area	Name
1.0	12/12/2012	ISD Technology Risk Partner	Peter Ly
1.0	10/12/2012	Service Integration & Management Program – Process & Requirements Stream Manager	Adam Price

9. Document Endorsement

Version	Endorsement Date	Role / Area	Name
1.0	17/12/2012	GBS Technology Change Management Process Manager	Chris Pehrson
1.0	26/11/2012	Wholesale Banking Technology Head of Technology Risk & Assurance	Nigel Bell
1.0	20/12/2012	Wealth Technology Head of Technology Operations	Michael Garrett (Robert Mazzotti as delegate for Mike Garrett)
1.0	7/12/2012	BNZ Technology Manager Services Management	Mike Morris

10. Document Approval

Version	Approval Date	Role / Area	Name
1.0	20/12/2012	Manager Service Management Process Delivery (as delegate of GM Integrated Service Delivery)	David Mitchell

11. Changes to this Document

Any changes to this document are subject to control and management via the Service Management Office Release process.

12. Document Change Log

Version	Version Date	Change Description	Author
0.1	1 July 2012	Draft of the Enterprise Change Policy	L. Monro
0.2	30 Aug 2012	Major re-write and updates to content (remove tool specific references, use consistent terminology, align with ITIL v3, ensure content is at policy-level, add statements to cover emergency and urgent change) and format for enhanced template (align policy statements to COBIT v5 IT controls)	M. Lampert
0.3	10 Sep 2012	Minor updates after feedback from WBT. Added definitions table.	M. Lampert
0.4	25 Sep 2012	Minor changes to incorporate feedback from Gary Percival. Removed references to roles.	M. Lampert
0.5	11 Oct 2012	Clarify wording for emergency Changes	M. Lampert

Version	Version Date	Change Description	Author
0.6	15 Oct 2012	Clarify wording for emergency and expedited Changes (removed the Definitions table)	L. Monro
1.0	26 Nov 2012	Version 0.6 draft accepted. Updated version to 1.0 to make this the first live version of the Policy. No other changes were made between v0.6 and v1.0	L. Monro