

Contents

1	Document	1
1.1	Control	1
1.2	Version control	2
1.3	Review period	2
2	Document purpose	2
3	Change management policy summary	2
4	Key change management policy steps	2
5	Roles and Responsibilities	3
5.1	Roles	3
5.2	Process Responsibilities	3
6	Change types	4
7	Change risks, impact and priority	5
7.1	Change risks	5
7.2	Customer impact analysis	5
7.3	Change priorities	6
8	Change approval	6
8.1	Technical approval	6
8.2	Customer approval and notifications	6
8.3	CAB / ECAB approval	7
8.4	Retrospective	7
9	Implementation and testing	7
9.1	Change implementation	7
9.2	Testing and validation	7
9.3	Change completion	7
9.4	Post implementation review (PIR)	7
9.5	Change closure	7
10	Expected change inputs and outputs	8
10.1	Inputs	8
10.2	Outputs	8

1. Document

1.1. Control

This document is controlled and maintained according to the documentation standards and procedures of Timico. All requests for changes to the document should be sent to the document owner(s). Any new issues will be sent to the recipients as defined within the distribution list maintained by the document owner(s). Requests for additional copies of this document should be sent to the document owner(s) to ensure that alterations or amendments to the distribution list are properly controlled.

1.2. Version control

Version	Description	Editor	Date
1.0	Creation of change management procedures	Technical Support Team Leader	03/05/13
1.1	Change to sections 4.3.2 and 4.3.2.1	Compliance	17/10/13
1.2	Change to section 7.1 update of Title	Compliance	29/10/14
1.3	Change of Document numbers to reflect new version, removal of section 4.3.2.1 and change of document reviewer	Compliance	04/09/2015
2.0	Re-write of policy	Quality Manager	10/04/2017

1.3. Review period

This document shall be reviewed at least annually to ensure that the document remains relevant. Any changes will be recorded in the version history above.

2. Document purpose

This document outlines the change management policy expected to be adhered to by all employees Timico.

3. Change management policy summary

The primary objective of Change Management is to enable changes to be made, with minimal or no disruption to the services we provide to our customers.

Change Management will work in conjunction with other Timico policies related to ITIL and IT Service Management (ITSM).

The goals of the Timico Change Management Policy include establishing a standard process for requesting, planning, approving, communicating, implementing and reporting changes to our Services.

The owner of this policy is of the Timico Chief Operating Officer.

4. Key change management policy steps



5. Roles and responsibilities

5.1. Roles

Roles	Description
Change Requestor	Anyone who wants to raise a request for change (RFC)
Change Owner	Person who ensures the assessment, prioritisation, scheduling communication and delivery of the change
Change Implementer	Person who creates, builds, tests and deploys the change
Change Management Process Manager	Person who is administers the change process, ensuring all necessary process steps are completed and improvements are raised, when necessary
Change Approver	The person / group who approves the change(s)
CAB (Change Advisory Board) / ECAB (Emergency Change Advisory Board)	The group/body who exist to support the authorisation of change and to assist Change Management in the assessment, prioritisation and scheduling of change, resolving priority conflicts.

5.2. Process Responsibilities

Roles / Sub Process	Change Requestor	Change Owner	Change Implementer	Change Management Process Manager	Change Approver	CAB/ ECAB
Change Management Process Administration and Support				AR		
RFC Logging	R	A	I	I		
RFC Scheduling and Forward Planning	I	A	R	C		I
Approval of RFC	I	I	I	A	R	R
RFC Communications	I	R		AR	I	I
Implementation of RFC	I	I	AR	I		I
Change Completion	I	A	R	I		I
Post Implementation Review	C	C	C	AR	I	I
Change Closure				AR		

5.2. Process Responsibilities (continued)

R - Responsible

Those who do the work to achieve the task. Others can be delegated to assist in the work required.

A - Accountable

The one ultimately answerable for the correct and thorough completion of the task. An accountable must sign off work that responsible provides.

C - Consulted

Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.

I - Informed

Those who are kept up-to-date on progress, often only on completion of the task; and with whom there is normally just one-way communication.

6. Change types

Change Type	Definition	Technical Approval prior to CAB	CAB Submission Deadline
Standard	<p>A routine change that is low risk, relatively common, and follows an approved procedure. Management approval from the customer aspect is still required as a customer may need to be notified of the planned change.</p> <p>For a change to requested and approved as a standard change this needs to have been completed successfully three times as a normal change and the procedure documented. The procedure also needs to be approved by the change manager.</p>	N/A	No
Normal	A change to an existing service, system, application or infrastructure component with potential impact and requires CAB approval before being implemented.	Yes	3 hours before CAB
Emergency	A change that must be implemented as soon as possible, for example, to resolve a major Incident, implement a security patch or to prevent an imminent failure.	Yes	Emergency CAB required
Retrospective	A change in response to a major incident where the remedy requires immediate action to resolve and emergency change control process is not possible.	Major Incident Manager approval	Major Incident Manager approval

7. Change risks, impact and priority

7.1. Change Risks

When assessing a change, a risk assessment is undertaken using the following criteria: -

High:

- High complexity with technical coordination required from multiple teams within the business
- High likelihood of system/service outage
- Previous change has been made and was not successful
- Complex implementation or back-out plans
- Will impact SLAs and /or could result in service credits

Medium:

- Significant complexity with technical coordination required from one team within the business
- Moderate risk to system/service availability
- Some complexity to implementation or back-out plans
- Possibility of some effect on SLAs

Low:

- Low complexity repeatable change
- Low risk to system/service availability
- Simple implementation or back-out plans
- No impact to SLAs

7.2. Customer impact analysis

When assessing a change, an impact assessment is undertaken using the following criteria: -

High:

- The proposed change poses significant impact to the customer(s) system in the form of greater than 50% or a complete outage of the services provided.

Medium:

- The proposed change poses an impact to the customer(s) system in the form of reduced resiliency, redundancy or capacity or an outage of 50% or less of our services provided.

Low:

- The proposed change has no impact to the customer(s) system.

7.3. Change priorities

When assessing a change, a priority assessment is undertaken using the following criteria: -

- **1 - Critical** – a change that, if not implemented immediately, will leave the organisation open to significant risk of degraded service and reputational damage
- **2 - High** – a change that is important for the organisation and must be implemented soon to avoid a potentially risk, although there is no immediate danger
- **3 - Medium** – a change which is subject to an agreed, non-urgent timescale
- **4 - Low** – a change which will be advantageous but is not pressing and has no strict timescale

8. Change approval.

For each change type the following approval matrix needs to be adhered to: -

Change Type	Technical Approval	Customer	CAB / ECAB
Standard	No	Yes	No
Normal	Yes	Yes	Yes
Emergency	Yes	Yes	Yes
Retrospective	N/A*	N/A*	N/A*

* Approvals for retrospective changes will be managed during the major incident

8.1. Technical approval

Technical approval must be given by a higher skilled engineer (of the technology / technologies related to the change) than the engineer implementing the change.

If the engineer planning and implementing the change has no reviewer of a higher skillset, then the change must be set as a high risk and assessed by the CAB / ECAB.

8.2. Customer approval and notifications

The change approver must ensure that relevant level of customer approval or notification:

- Planned notifications (2 weeks' advanced notice is required)
- Emergency change notifications
- Individual customer approval (for changes related to one customer only) from an authorised customer representative

8.3. CAB / ECAB approval

All Normal and Emergency changes are to be reviewed by the CAB / ECAB, where they will be approved or rejected. This is in addition to technical and customer approval.

8.4. Retrospective

A change in response to a major incident where the remedy requires immediate action and will be approved by the Major Incident Manager.

9. Implementation and testing

9.1. Change implementation

All changes should be carried out as described in the RFC and within the designated planned times. If a variation is identified during the change then this must be presented to either the Change Manager or the Duty Manager to approve the variation. This variation must then be documented in the change notes.

If the variation is not approved, this will result in the change being backed out. This change will then need to be re-planned and re-raised.

9.2. Testing and validation

Following the implementation of the change, tests in line with the testing plan set out in the change must be carried out to ensure that the desired result has been verified.

If a change has not met the acceptance criteria then the back-out plan must be invoked, as detailed in the RFC.

9.3. Change completion

Once the change has been tested and validated, the change status is changed to completed ready for the post implementation review by the Change Manager.

9.4. Post implementation review (PIR)

A change review should be carried to confirm that the change has met its objectives, that the change initiator and stakeholders are happy with the objectives, and that there have been no unexpected side effects (e.g. no P1 incidents after implementation)

Spot checking of changes rather than large scale PIR's is acceptable for successful changes, however a PIR is mandated for changes that have been rolled, led to unexpected service impact, changes with a high risk, changes with a high impact or changes where there was a variation during implementation.

9.5. Change closure

Once the Change Manager has satisfied themselves all stages of the change life cycle has been completed, the change can be closed.

10. Expected change inputs and outputs

10.1. Inputs

- Request of the change recorded
- Change window
- Impact duration
- Resourcing
- Acceptance criteria
- Testing plan
- Back out plan
- Impact assessment
- Risk assessment
- Services on system monitoring
- Method statement for a high risk or high impact changes
- Configuration items identified

10.2. Outputs

- Technical approval recorded prior to CAB
- Customer approval recorded
- CAB approval
- Customer confirmation of successful implementation
- CMDB updated
- Documentation updated
- Reporting
 - Successful changes
 - Unsuccessful changes
 - Reporting by change type
 - Trend analysis
 - Changes promoted from Normal to Standard
- Internal forward schedule of change
- Customer forward schedule of change
- Customer notifications