

Contents

Contents.....	1
1. Document	3
1.1 Control	3
1.2 Version control.....	3
1.3 Review period	3
2. Document purpose	4
3. Change management policy summary.....	4
4. Key change management policy steps	4
5. Roles and responsibilities.....	4
5.1 Roles.....	4
5.2 Roles.....	Error! Bookmark not defined.
R – Responsible.....	Error! Bookmark not defined.
A – Accountable.....	Error! Bookmark not defined.
C – Consulted	Error! Bookmark not defined.
I – Informed	Error! Bookmark not defined.
6. Change types	5
7. Change risks and impact.....	6
7.1 Change Risks.....	6
7.2 Customer impact analysis	6
8. Changed approval	7
8.1 Technical approval	7
8.2 Customer approval.....	7
8.3 CAB / ECAB approval	7
8.4 Emergency.....	7
9. Implementation and testing.....	8
9.1 Change implementation.....	8
9.2 Testing and validation	8
9.3 Change completion	8
9.4 Post implementation review (PIR)	8
9.5 Change closure.....	8
10. Customer Notification	8

- 10.1 Notification Notice Period.....8
- 11. Expected change inputs and outputs..... 9**
- 11.1 Inputs9
- 11.2 Outputs9

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	03/05/2013
1.1	Change to sections 4.3.2 and 4.3.2.1	Compliance	17/10/2013
1.2	Change to section 7.1 update of Title	Compliance	29/10/2014
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
2.1	Removal of section 7.3 (change priorities) and amendments to sections 6 and 8 related to CAB requirements for Normal change requests	Change Manager	14/01/2020
3.0	Major rewrite to accommodate revised CM process	Change Manager	20/03/2020

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 (CM) 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, communicating, approving, 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

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 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.

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 a pre-defined procedure. Customer approval is still required.</p> <p>For a Normal change to be upgraded to a standard change, it must have been completed successfully three times as a normal change and the procedure documented. The creation of the standard template requires approval by the change manager.</p>	No	No
Normal	<p>A change to an existing service, system, application or infrastructure component with potential impact which may require CAB approval before being implemented.</p>	Yes	3 hours before CAB for high risk changes only
Emergency	<p>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.</p>	Yes	Emergency CAB required

7. Change risks and impact

7.1 Change Risks

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

High:

- Previous change has been made and was not successful
- Complex implementation or back-out plans
- Novel technology, not previously implemented

Medium:

- Previous similar changes have occasionally been problematic
- Some complexity to implementation or back-out plans
- Standard technology utilized in a non-standard application

Low:

- Previous similar changes have always been successful
- Simple implementation or back-out plans
- Standard technology used in a BAU context

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) or internal systems in the form of loss of service or serious performance degradation for an extended period.
- Multiple customers or internal departments suffer loss or degraded service during the change window

Medium:

- The proposed change poses an impact to the customer(s) or internal systems in the form of reduced resiliency, redundancy or capacity.
- A single customers or internal department suffers loss or degraded service during the change window

Low:

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

8. Changed 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	Risk related
Emergency	Yes	Yes	Yes

8.1 Technical approval

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

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

8.2 Customer approval

Individual customer approval (for changes related to one customer only) must only be accepted from an authorised customer representative.

8.3 CAB / ECAB approval

All 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 Emergency

A change in response to a major incident where the remedy requires immediate action and will be approved by the Major Incident Manager with evidence of retrospective approval from the customer being requested as soon as reasonably practicable.

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 a member of the Change Management team 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.

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 back, led to unexpected service impact or changes where there was a variation during implementation.

9.5 Change closure

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

10. Customer Notification

10.1 Notification Notice Period

For planned changes which may cause outage or serious performance degradation for multiple customers, notifications must be issued at least 14 days in advance. In emergency situations, the 14 day notice period may be waived.

11. Expected change inputs and outputs

11.1 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

11.2 Outputs

- Technical approval recorded prior to CAB
- Customer approval recorded
- CAB approval
- Customer confirmation of successful implementation (if available)
- 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