Procedure

Procedure Name	***IT Change Management***		
Procedure #	IT 1.5	Parent Policy	IT 1.0 Service Management Policy
Policy Owner	Vice President Administration & CFO	Effective Date	March 19, 2025
Procedure Owner	AVP Information Technology & CIO	Next Review Date	March 19, 2029
Approved by	AVP Information Technology & CIO	Approval Date	March 19, 2025

1.0 Purpose/ Background

Well-developed and purposeful management processes support the delivery of reliable and effective IT services. NAIT relies on IT change management processes that consider the need for prompt action, service availability, compliance with policies, and alignment with strategic priorities.

2.0 Definitions

Term	Definition
Blackout calendar	A calendar that records specific periods when no changes or only essential changes are permitted to IT systems.
Change	The addition, modification, or removal of anything that could affect IT services.
Change Advisory Board (CAB)	A board of IT and business representatives who approve and schedule changes to the live environment.
Change calendar	A calendar that tracks and manages all planned IT system and service changes.
Change Manager	The person responsible for the quality and integrity of the change process, chairs CAB meetings, and has the final say on CAB decisions.
Change Coordinator	The persons responsible for reviewing RFCs for completeness.
Change Originator	The person initiating the change request. This is typically a member of the IT department who implements changes to the live environment.
Configuration Item (CI)	A record of an object stored within the CMDB (e.g. server, application, service).
Configuration Management Database (CMDB)	A centralized repository for information about all the CIs and their relationships within an IT environment that supports an IT-provided service.
Emergency Change Advisory Board (E-CAB)	A board of IT and business representatives validates and approves emergency change requests.
Request for Change (RFC)	A document that proposes a change to alter a system. The RFC includes all necessary information for evaluating and approving or rejecting the change, such as the reason for the change, the impact, the benefits, and the potential risks.

IT Service	A service provided by ITS using technology to manage and support NAIT's information needs.
Post Implementation Review (PIR)	A retrospective process to evaluate the success of a change. This may include root-cause analysis, mitigation actions, and lessons learned.

3.0 Procedures

3.1 All RFCs are classified as one of the following types:

- Emergency: Changes requiring immediate attention or action due to the disruption of a critical IT service and are associated with a recorded incident.
- Pre-Approved: Changes that typically carry low risk and occur frequently are pre-approved by the CAB and included in a predefined list or catalogue.
- Normal: any non-emergency change that requires risk assessment, planning, approval, and scheduling before implementation.

3.2 The Change Originator is responsible for:

- Selecting the most appropriate RFC template for the requested change (i.e. pre-approved, normal, or emergency).
- Selecting the impacted CIs and associating them with the RFC.
- Completing a risk assessment questionnaire for all normal changes.
- Submitting the RFC for assessment.

3.3 For Normal RFCs, the Change Coordinator evaluates the RFC for completeness, collaborates with the Change Originator to mitigate risks, validates associated components and plans, ensures proper sequencing, and conducts post-implementation reviews.

3.4 The Change Coordinator will identify and recommend regular changes with a low risk rating for consideration by the CAB for addition to the pre-approved change catalogue.

3.5 The Change Coordinator will maintain the Change and Blackout Calendars.

3.6 The CAB must approve and schedule the change for Normal RFCs with a major risk rating. CAB members must not approve changes for which they were involved in risk assessment, testing, or implementation.

3.7 For Emergency RFCs, the E-CAB is notified. Approval requires at least two E-CAB members before proceeding. If two members are unavailable due to the urgency of the change, a retrospective review must occur within 24 hours. The E-CAB consists of (in priority order):

- Change Manager
- IT Director of the Change Originator
- AVP, CIO
- Manager of the Change Originator

3.8 Emergency RFCs will be reviewed and discussed at the next scheduled CAB meeting.

3.9 The Change Coordinator ensures the dates, change plan, risk, test plan, implementation plan, communication plan and backout plan are appropriately documented and verifies that the RFC is associated with the correct CIs.

3.10 Tasks associated with an RFC will vary depending on the template used (e.g. pre-approved, normal, emergency). However, the following tasks will always be completed.

- Communication
- Implementation
- Validation

3.11 The Change Coordinator ensures that the correct approvers are selected in accordance with the Change Approval Matrix.

3.12 For Normal changes, the CAB will ensure that the change is thoroughly documented, properly tested, has an appropriate backout plan, and that the change schedule is suitable.

3.13 A Post Implementation Review (PIR) will be conducted for all Normal changes.

3.14 The Change Coordinator assigns PIR recipients, validates that PIRs are completed and reviews the feedback provided by the PIR.

3.15 The Change Coordinator will recommend action items raised to the Change Manager for CAB review.

3.16 The Change Coordinator ensures all required audit artifacts are attached to the change request or are accessible within the referenced project. These artifacts must include, at a minimum:

- Risk assessments.
- Documented approvals.
- Implementation plans.
- Backout plans.
- Post-implementation testing results.

3.17 The Change Coordinator verifies the completeness of these change records but does not approve the change itself. Any missing audit artifacts must be addressed before the change can be closed.

3.18 The Change Coordinator will determine if an IT Security Analyst is required to validate the security impact of the change. An IT security analyst must review any change affecting authentication, access control, security configurations, Payment Card Industry (PCI) systems, or sensitive data.

4.0 Exceptions to the Procedure

Exceptions to this procedure must be documented and formally approved by the Procedure Owner.

Procedure exceptions must include:

- The nature of the exception
- A reasonable explanation for why the procedure exception is required
- Confirmation that the exception aligns with the general principles
- Any risks created by the procedure exception and how they will be managed.

5.0 Related Documentation

5.1 IT Change Management Standard Operating Procedure

Document History

Date	*Action/ Change*
April 30, 2013	Original ITM.1.5 Changed Control Guideline
August 22, 2019	Updated Guideline to a NAIT Procedure DOC0010070 Rev 0.5
January 7, 2021	Updated to include IT Security NAIT Procedure DOC0010070 Rev 0.6
February 26, 2025	Refresh to include modern change management practices