NWC OT Security Change Management Process

Document Number:	A01001045-PRO-CM
Issue Date:	August 16, 2021
Revision Number:	01
Issued For:	Approval

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT Cybersecurity Analyst		August 07, 2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		August 09, 2021
Approved by:			
Farhan Rasheed	Operations Manager		August 09, 2021

Issued by:			
Syed Ali Raza	Planning Engineer		August 16, 2021

History Page

Issue No.	Issue Date	Prepared By (Name)	Reviewed By (Name)	Owned By (Name)	Endorsed By (Name)	Approved By (Name)
00	July 29, 2021	Sidrat Mehreen	Sameen Ullah Khan			Farhan Rasheed Khan
Change Description						
Change Description						
Change Description						

Reference Documents

Document Number	Document Title
ECC-1:2018	National Cybersecurity Authority Essential Cybersecurity Controls (NCA ECC)

Document Roles and Responsibilities

	Prepare/ Update/ Amend	Review	Approve	Publish
Owner	YES	YES		
Cybersecurity Steering Committee		YES		YES
Corporate Strategy & Performance Management VP			YES	

Table of Contents

Glossary

Word or Phrase	Explanation
Asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
Change	The addition, modification, or removal of anything that could have an effect on operations.
Change Management	The Process is responsible for controlling the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to OT process.
Compliance	Ensuring that a Standard or set of Guidelines is followed. A means of conforming to a rule, such as a specification, policy, standard or law.
Incident	Vulnerability and threat together result in an incident. An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Word or Phrase	Explanation
Integrity	The property of safeguarding the accuracy and completeness of assets.
Owner	The organization unit department/activity/ business unit which has its own policies and procedure and is responsible for its development and implementation. The owner will be the head of the department/area/activity/business unit that is responsible for developing and implementing the policy or procedure.
Review and approval	The process steps are taken to ensure that policies and procedures are complied. The approval is the evidence that the review has been completed to satisfaction of the appropriate person e.g. CEO / Executive Committee / BOD.
Risk	The possibility of suffering harm or loss. In quantitative Risk Management, this is calculated as how likely it is that a specific Threat will exploit a particular vulnerability. A combination of the probability of an event and its consequence.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Test Environment	A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc.

1. Introduction

The purpose of this document is to establish a procedure for change management. This procedure will ensure the process of following a standard change management procedure for all process complying with the change in NWC.

2. Roles and Responsibilities

Roles	Responsibilities
Requester	Requester shall have the following responsibilities, but not limited to, • Secures appropriate business approval for the Change prior to starting the Change Management Process • Communicates status of the change back to the business or project team as necessary • Determining the timeframe for the change • Working with the appropriate people to schedule the planned change • Identifying the individuals involved in testing the change
Change Manager	Change Manager shall have the following responsibilities, but not limited to, • Determining if the change is an emergency, standard, or a normal change • Identifying the need for changes to production processes or systems • Following the appropriate Change Management Process (Emergency, Standard, Normal) • Maintaining communications with stakeholders as the change progresses from inception to validation • Verifying and documenting the outcome of the changes and rating their success • Risk Evaluation of the change request
Change Advisory Board (CAB)	CAB shall have the following responsibilities, not limited to • Supporting the change manager in decisions for major changes.

Roles	Responsibilities
	• Evaluating Requests for Change (RFCs), the available resources, impact of change, and organizational readiness. • Validating those appropriate tests and evaluation are performed before high-risk changes are approved. • Documenting relevant processes and activities. • Supporting the design of change implementation scheduling. • Reviewing a change implementation process. • Supporting the design and approving new change process models. • Using the diverse knowledge base, skills, and expertise of each CAB member to provide a unique perspective before a decision is finalized.
Change process Owner	• Developing an appropriate test plan • Developing an appropriate verification plan • Identifying any inadvertent consequences that might result in stability or security issues • Verifying successful test results: resolving and re-testing any issues • Documenting test results • Communicating test results to the data owner • Developing, testing and documenting a back-out plan • Verifying back-ups beforehand when production environments are used
Change Implementation Team	• Obtaining authorization from the appropriate Change Manager to migrate the change • Ensuring adequate staff is available to migrate the change • Communicating the migrated change to the appropriate Change Manager • Migrating successfully tested changes to the production environment

3. Change Management Process

Changes that are requested by the Requester will undergo following steps:

3.1 Plan and Request the Change

1. The Requester and Change Manager when planning the change will determine the type of change, identification of individuals and scheduling, as mentioned in section 2.
2. Submit a Change Request Form, see attached in Appendix A.

3.2 Risk Assessment

1. Every requested change is to be followed by a formal risk assessment procedure to evaluate the impact analysis of change on the system or environment.

3.3 Test the Change

1. A test plan will be shared with the CAB. The verification plan may include pre-testing in a test environment, or alternatively breaking the change into sufficiently small increments that can be tested in off-hours using production environments for systems that do not have a test environment. The results will be documented and verified as part of the change management process.

3.4 Document the Change

1. All change requests must be formally documented, classified, and prioritized to ensure they are planned for accordingly.
2. All those involved in the Change Management Process are responsible for reviewing the documented changes for correctness, completeness, and adherence to standards and procedures.
3. All change requests must be maintained for awareness that a change is being or has been implemented.
4. Change control documentations such as diagrams, schematics, processes must be updated to reflect the current state after the change (i.e., all documentation must be updated before the change request can be closed). An index must be maintained of revision levels to identify current official revision.

3.5 Approve the Change

1. Change will be reviewed and then approved by each member of the Change Advisory Board (CAB). The Change Advisory Board (CAB) should assess the risks and benefits of either

making the change or not making the change. The CAB reserves the right to alter the change plan, make recommendations and/or send it back for revisions if the change proposal is unacceptable or requires additional work.

3.6 Implement the Change

1. The Change Advisory Board authorizes the change to be implemented. Only changes that have been approved may be implemented in a production environment.

3.7 Validate the Change

1. After implementation of a change, validation of the change must occur in order to verify if the change was successful. If validation fails, the change must be reverted using its back out plan.

3.8 Close the Change

1. All changes must be closed by the Requestor within a six-month period and must indicate one of the following closing codes:
   - Change Successful
   - Change Successful but had a few issues
   - Change Successful but exceeded the planned end time
   - Change Backed out
   - Change Cancelled – it was never started
2. Standard and Normal changes that were successful with few issues or backed out will need a post-change review by the change manager prior to closing.
3. All emergency changes will require a post-change review by the Change Manager prior to closing.

4. Change Classification

There are four types of changes.

Change Type	Description- business impact, change duration and frequencies
Emergency Change	A change that requires immediate implementation to correct an important issue, such as a disruption or outage of service. Examples of emergency changes include repairing a service issue that severely impacts the business, or a situation that requires immediate action to either restore a service or prevent an outage. An emergency change requires: • Sufficient review and discussion with all impacted and involved parties, including business users, the Line Manager of the team performing the change. • Approval by the ECAB prior to implementation. At minimum, approval should be from at least one member of the ECAB and the system owner. • Testing may be reduced, or not performed altogether if necessary, and may be performed after implementation of a change request within one business day after the issue has been resolved. • Post-implementation review performed by manager of the team that performed the change and provided to the ECAB.
Major Change	A change that is high risk and complex potential impact, with a significant potential impact to production services, and limited backup/recovery in the event of an issue. A major change requires: • Formal review and discussion with all impacted and involved parties, including business users, the Line Manager of the team performing the change. • Formal testing (when possible)

Change Type	Description- business impact, change duration and frequencies
	• Formal review and approval by the CAB prior to implementation. • Notification of the change to affected users. • Formal post-implementation review.
Minor Change	A change that is low risk and well understood, with a limited potential impact to production services, is sufficiently tested prior to implementation and is easy to back-out in the event of an issue. A minor change requires approval to start from the manager of the team performing the change, and approval from the system owner prior to going live or upon completion.
Standard Change	A change that is low risk and relatively common, where the implementation follows a simple documented procedure or work instruction. For example, password reset or provision of standard equipment to users. A standard change follows a formal procedure or work instruction that has been authorized in advance.

4.1 Emergency Change Process:

Activity		Description
1.1	Create Request for Emergency Change	Incident response team will initiate request for function restoration, but restoration procedure is inadvertently result in emergency change.
1.2	Submit RFC	The RFC is submitted by incident response team for approval from ECAB.
1.4	ECAB Approval	The risk and impact analysis of the change is reviewed by ECAB. The change is authorized for deployment and sent to requestor. If the RFC need to be updated, it is

Activity		Description
		returned to the requester with an explanation for update.
1.6	Communicate Change Details	The change requester communicates the change details to the appropriate stakeholders.
1.7	Coordinate Change Implementation	Incident response team has overall responsibility of coordination and implementation
1.8	Review Change Outcomes	After change implementation, the incident response team will validate change.
1.9	Close RFC	The incident response team document the final changes and closes emergency change request.

4.2 Major Change Process:

Activity		Description
1.1	Create Request for Major Change	The change requester must have Line manager prior approval to plan, build and test a change. Once completed, the change requestor follows the change management work instructions to create the RFC.
1.2	Submit RFC to Change Manager	The RFC is submitted by line manager for approval from Change Manager.
1.4	CAB Approval	The risk and impact analysis of the change is reviewed by the CAB. The CAB validates that there are no conflicts in the published change schedule. The change is authorized for deployment and sent to requestor. If the RFC need to be updated, it is returned to the requester with an explanation for update.

Activity		Description
1.6	Communicate Change Details	The change requester communicates the change details to the appropriate stakeholders.
1.7	Coordinate Change Implementation	The change implementer defines the steps for the change implementation, coordinates the work, and executes the change.
1.8	Review Change Outcomes	Upon execution of the change, the change implementer and change requester validate that the change produced the intended outcomes. In case of failure, change manager will either request implementer to roll back changes or provide fixes.
1.9	Close RFC	The change requester closes the change.

4.3 Minor Change Process:

Activity		Description
1.1	Create Request for Minor Change	The change requester must have Line manager prior approval to plan, build and test a change. Once completed, the change requestor follows the change management work instructions to create the RFC and requires line manager approval.
1.2	Submit RFC to Change Manager	After line manager approval, RFC is submitted by line manager for approval from Change Manager.
1.6	Communicate Change Details	Once approved, change requester communicates the change details to the appropriate stakeholders.

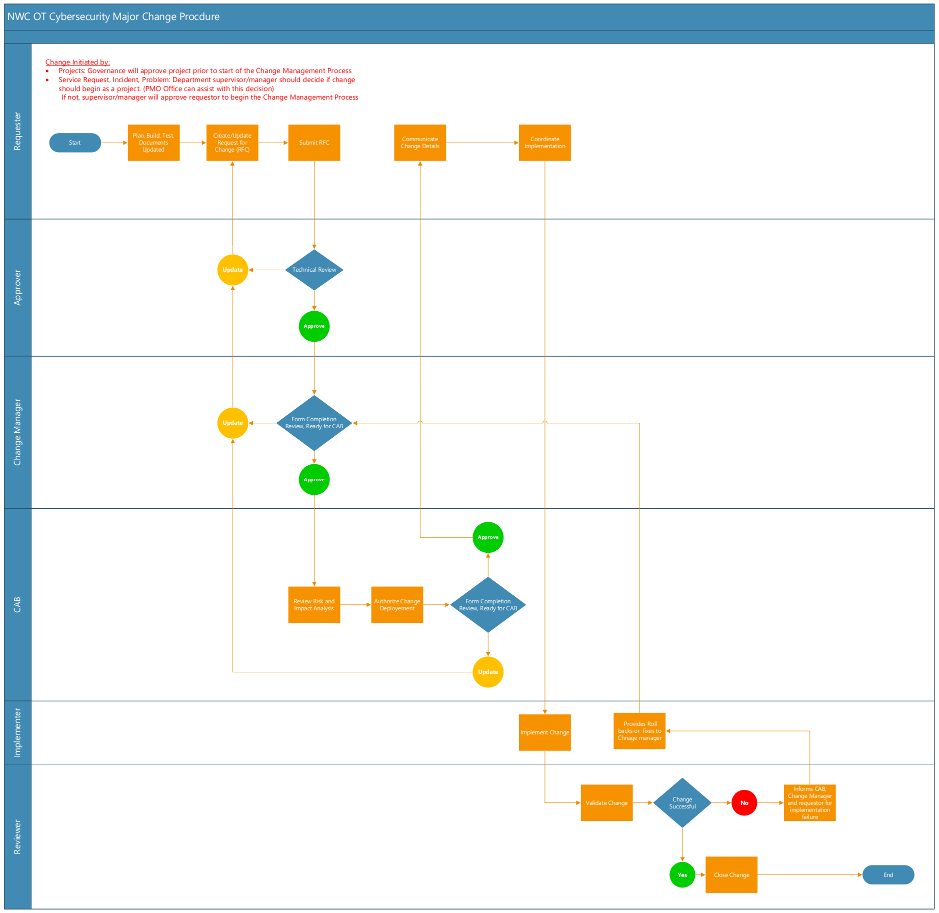
Activity		Description
1.7	Coordinate Change Implementation	The change implementer defines the steps for the change implementation, coordinates the work, and executes the change.
1.8	Review Change Outcomes	Upon execution of the change, the change implementer and change requester validate that the change produced the intended outcomes. In case of failure, change manager will either request implementer to roll back changes or provide fixes.
1.9	Close RFC	The change requester closes the change.

4.4 Standard Change Process:

Activity		Description
1.1	Create Request for Standard Change	The change requester must have Line manager prior approval to plan, build and test a change. Once completed, the change requestor follows the change management work instructions to create the RFC and requires line manager approval.
1.2	Submit RFC to Change Manager	After line manager approval, RFC is submitted by line manager for approval from Change Manager.
1.6	Communicate Change Details	Once approved, change requester communicates the change details to the appropriate stakeholders.
1.7	Coordinate Change Implementation	The change implementer defines the steps for the change implementation, coordinates the work, and executes the change.

Activity		Description
1.8	Review Change Outcomes	Upon execution of the change, the change implementer and change requester validate that the change produced the intended outcomes. In case of failure, change manager will either request implementer to roll back changes or provide fixes.
1.9	Close RFC	The change requester closes the change.

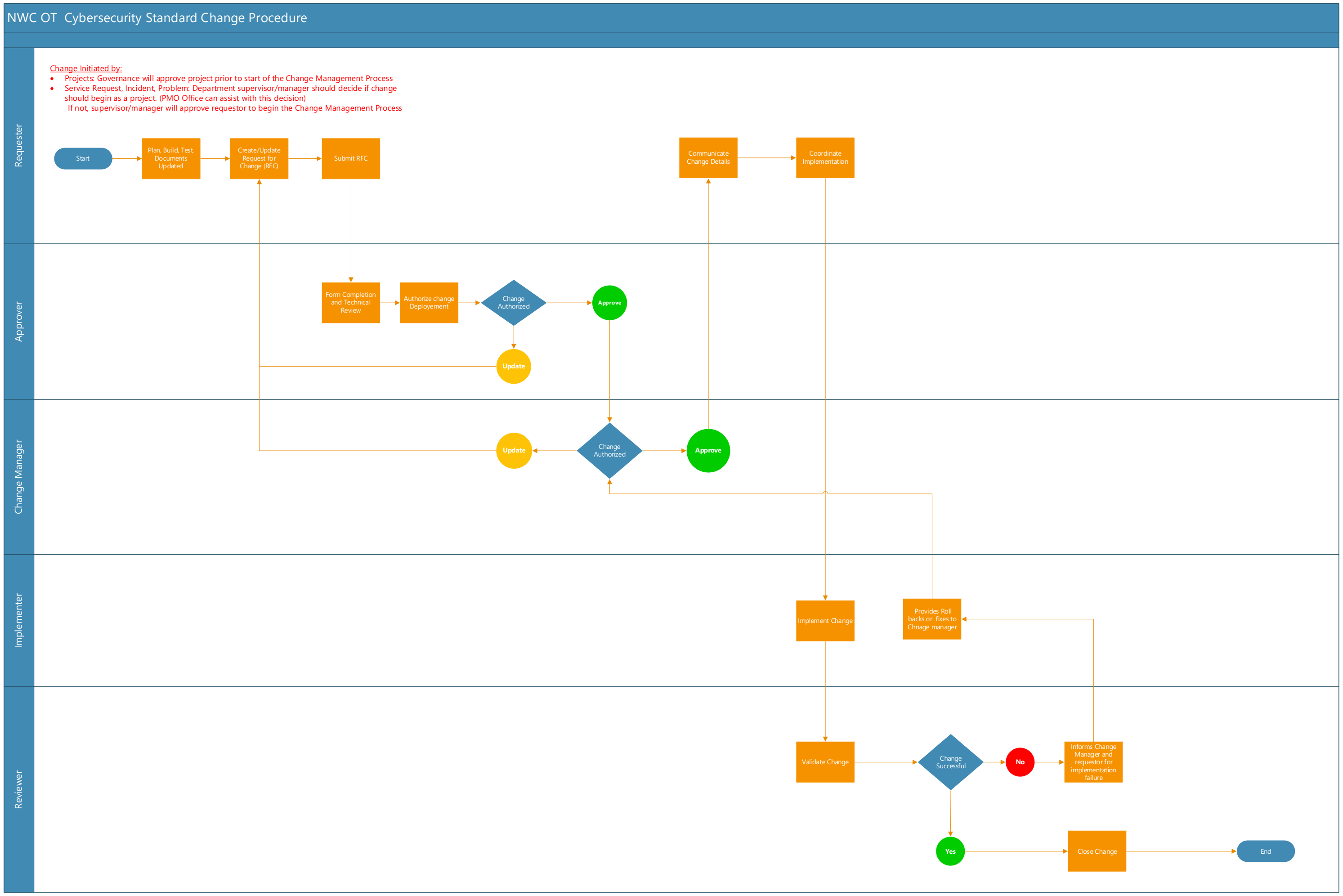
5. Process Flow chart



Change Initiated by:

- Projects: Governance will approve project prior to start of the Change Management Process
- Service Request, Incident, Problem: Department supervisor/manager should decide if change should begin as a project. (PMO Office can assist with this decision)
  If not, supervisor/manager will approve requestor to begin the Change Management Process

NWC OT Cybersecurity Major Change Procdure
Requester
Approver
Change Manager
CAB
Implementer
Reviewer
Start
Plan, Build, Test, Documents Updated
Create/Update Request for Change (RFC)
Submit RFC
Communicate Change Details
Coordinate Implementation
Update
Technical Review
Approve
Update
Form Completion Review, Ready for CAB
Approve
Approve
Review Risk and Impact Analysis
Authorize Change Deployement
Form Completion Review, Ready for CAB
Update
Implement Change
Provides Roll backs or fixes to Chnage manager
Validate Change
Change Successful
No
Informs CAB, Change Manager and requestor for implementation failure
Yes
Close Change
End

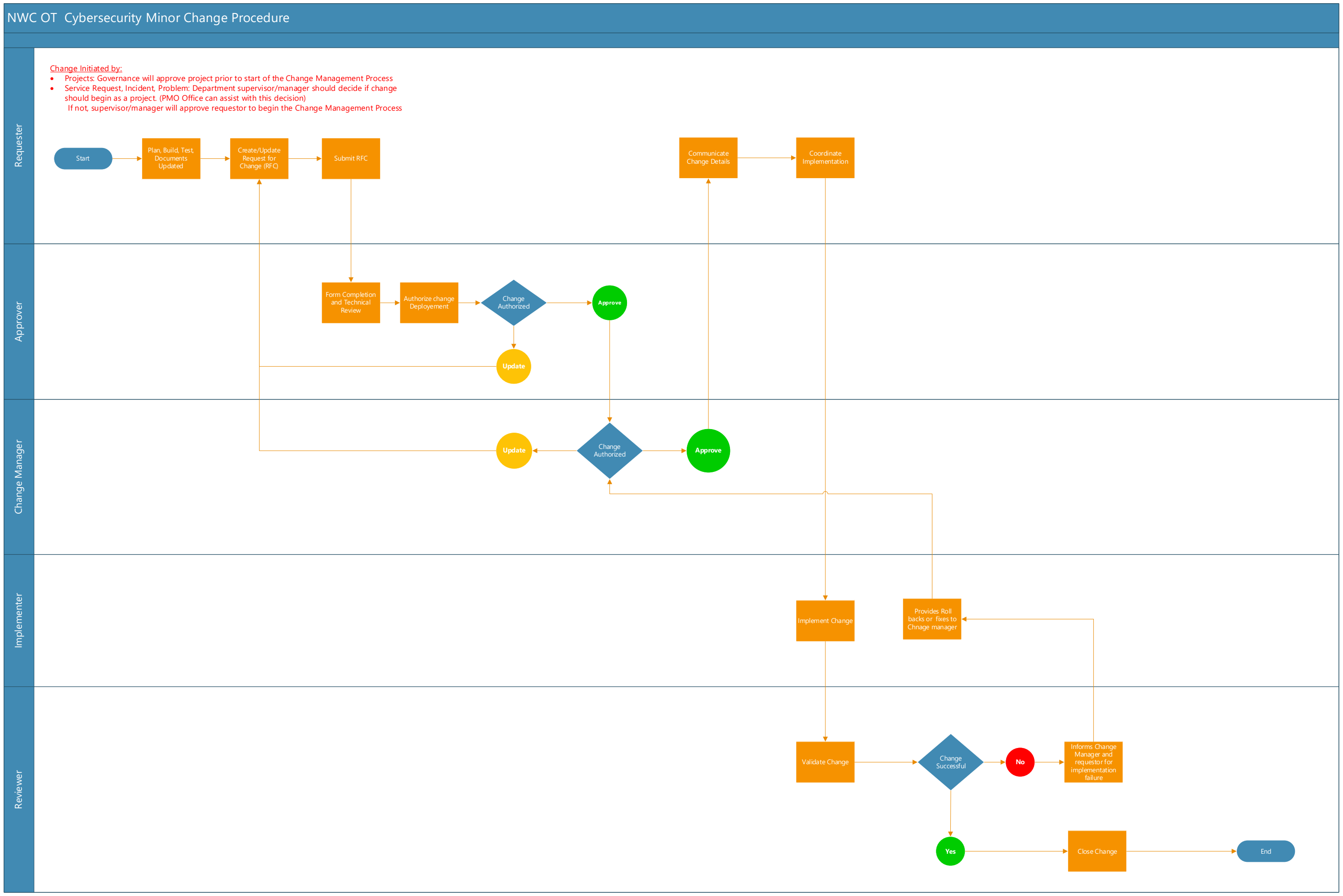

NWC OT Cybersecurity Standard Change Procedure
Requester
Approver
Change Manager
Implementer
Reviewer
Start
Plan, Build, Test, Documents Updated
Create/Update Request for Change (RFC)
Submit RFC
Communicate Change Details
Coordinate Implementation
Form Completion and Technical Review
Authorize change Deployement
Change Authorized
Approve
Update
Update
Change Authorized
Approve
Implement Change
Provides Roll backs or fixes to Chnage manager
Validate Change
Change Successful
No
Informs Change Manager and requestor for implementation failure
Yes
Close Change
End

Change Initiated by:

- Projects: Governance will approve project prior to start of the Change Management Process
- Service Request, Incident, Problem: Department supervisor/manager should decide if change should begin as a project. (PMO Office can assist with this decision)
  If not, supervisor/manager will approve requestor to begin the Change Management Process

PROPRIETARY NOTICE

THIS DOCUMENT CONTAINS INFORMATION PROPRIETARY TO NWC. ANY DISCLOSURE OR USE THEREOF IS EXPRESSLY PROHIBITED EXCEPT UPON THE WRITTEN PERMISSION OF NWC.



NWC OT Cybersecurity Minor Change Procedure

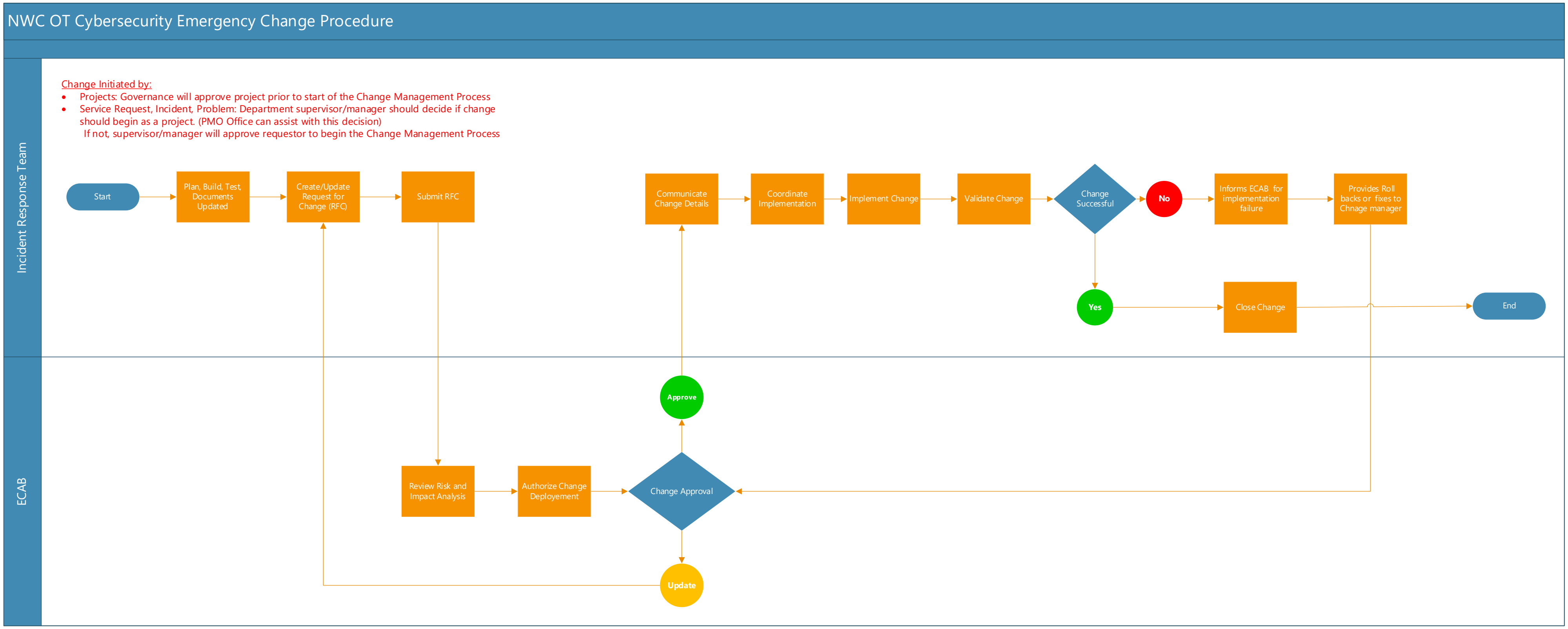
Change Initiated by:

- Projects: Governance will approve project prior to start of the Change Management Process
- Service Request, Incident, Problem: Department supervisor/manager should decide if change should begin as a project. (PMO Office can assist with this decision)
  If not, supervisor/manager will approve requestor to begin the Change Management Process

Requester
Approver
Change Manager
Implementer
Reviewer
Start
Plan, Build, Test, Documents Updated
Create/Update Request for Change (RFC)
Submit RFC
Communicate Change Details
Coordinate Implementation
Form Completion and Technical Review
Authorize change Deployement
Change Authorized
Approve
Update
Update
Change Authorized
Approve
Implement Change
Provides Roll backs or fixes to Chnage manager
Validate Change
Change Successful
No
Informs Change Manager and requestor for implementation failure
Yes
Close Change
End

PROPRIETARY NOTICE

THIS DOCUMENT CONTAINS INFORMATION PROPRIETARY TO NWC. ANY DISCLOSURE OR USE THEREOF IS EXPRESSLY PROHIBITED EXCEPT UPON THE WRITTEN PERMISSION OF NWC.



NWC OT Cybersecurity Emergency Change Procedure

Change Initiated by:

- Projects: Governance will approve project prior to start of the Change Management Process
- Service Request, Incident, Problem: Department supervisor/manager should decide if change should begin as a project. (PMO Office can assist with this decision)
  If not, supervisor/manager will approve requestor to begin the Change Management Process

Incident Response Team
ECAB
Start
Plan, Build, Test, Documents Updated
Create/Update Request for Change (RFC)
Submit RFC
Communicate Change Details
Coordinate Implementation
Implement Change
Validate Change
Change Successful
No
Informs ECAB for implementation failure
Provides Roll backs or fixes to Chnage manager
Yes
Close Change
End
Approve
Review Risk and Impact Analysis
Authorize Change Deployement
Change Approval
Update

6. Change Compliance and Audit

A central Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

1. Date of submission and date of change
2. Owner and custodian contact information
3. Nature of the change
4. Indication of success or failure

7. Forms & Templates

NWC-IS-PRO-CM-FRM-01.00 D1 Change Request Form

Appendix A

Change Request Form

Change Description/Change Request File Name:				
Change Request No.		**Project:**		
Requested By:		**Date:**		
Department:		**Contact:**		
Description of Change:				
Reason for the Change:				
Requester Sign-off:				
Approval of Request:				
Change Impact Evaluation				
Change Type	Application	□	Database	□
	Hardware	□	Procedures	□
	Network	□	Security	□
	Operating System/Utilities	□	Schedule Outage	□

Change Priority	Urgent	□	**Change Impact**	Minor	□
	High	□		Medium	□
	Medium	□		Major	□
	Low	□			
Environment Impacted:					
Resource Requirements:					
Test Plan Description:					
Roll back Description:					
Change Approval or Rejection					
Change Request Status	□	Accepted	□	Rejected	
Comments:					
Change Scheduled for: (date)					
Implementation Assigned to:					
Change Approval Board **Sign off:**					
Change Implementation					
Staging Test Results:					
Implementation Test Results:					
Date of Implementation:					
Implementer Sign off:		**Date:**			