

Internal and Confidential

Netradyne IT Change Management Process

V2.1

Table of Contents

[Netradyne Change Management Process 0](#_Toc167115721)

[Document Control 2](#_Toc167115722)

[1 Purpose 3](#_Toc167115723)

[2 Scope 3](#_Toc167115724)

[3 Roles and Responsibilities 3](#_Toc167115725)

[4 Procedure 4](#_Toc167115726)

[4.1 Policies 4](#_Toc167115727)

[4.2 Key Contacts & Escalation Matrix 4](#_Toc167115728)

[4.3 Controls 4](#_Toc167115729)

[4.3.1 Segregation of Duties 4](#_Toc167115730)

[4.3.2 Segregation of Environments 4](#_Toc167115731)

[4.3.3 Change Authorization 5](#_Toc167115732)

[4.3.4 Testing Evidence 5](#_Toc167115733)

[4.3.5 Change Documentation Quality 5](#_Toc167115734)

[4.3.6 Change Advisory Board Review 5](#_Toc167115735)

[4.3.7 Emergency Change Advisory Board (ECAB) Review 5](#_Toc167115736)

[4.4 RACI 5](#_Toc167115737)

[4.5 Activities 6](#_Toc167115738)

[4.5.1 Weekly Activities 6](#_Toc167115739)

[4.5.2 Monthly Activities 6](#_Toc167115740)

[4.6 Change Management Process Overview & Roles 6](#_Toc167115741)

[4.6.1 Change Process Overview 6](#_Toc167115742)

[4.6.2 Change Management Roles 7](#_Toc167115743)

[4.7 Change Management – Types & Process 10](#_Toc167115744)

[4.7.1 Brief 10](#_Toc167115745)

[4.7.2 Types of Changes 10](#_Toc167115746)

[4.8 Change Management – Workflow & Work Level Instruction 11](#_Toc167115747)

[4.8.1 Normal/Expedited Change 11](#_Toc167115748)

[4.8.2 Emergency Change 17](#_Toc167115750)

[4.8.3 Standard Change 19](#_Toc167115752)

[4.9 Change Relationship with Other Process 22](#_Toc167115753)

[4.10 Key Definitions 22](#_Toc167115755)

[4.11 Unauthorized Changes 23](#_Toc167115756)

[4.12 Post Implementation Review (PIR) 23](#_Toc167115757)

[4.13 4 Eye Check 24](#_Toc167115759)

[5 Conduct 24](#_Toc167115762)

[6 Exception 24](#_Toc167115763)

[7 Terms/Acronyms 24](#_Toc167115764)

[8 References 25](#_Toc167115765)

[Policies 25](#_Toc167115766)

[Process/Procedures 25](#_Toc167115767)

[9 Appendix A: Document RACI Matrix 26](#_Toc167115768)

**Document Control**

|  |  |
| --- | --- |
| **Document ID** | NDCM2024001 |
| **Document Name** | Netradyne Change Management Process |
| **Document Status** | Released |
| **Document Released Date** | 20-May-2024 |
| **Document Author** | Priyesh Parashar |
| **Document Content Contributors** | Priyesh Parashar, Chethan G. |
| **Document Signatory** | saravanan.sankaran@netradyne.com |
| **Document Owner** | priyesh.parashar@netradyne.com |
| **Document Version** | V2.1 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| V1.0 | 17/01/2022 | Released | Vijaykumar Dalal |
| V1.1 | 22/06/2023 | Annual Revision | Chethan G. |
| V2.0 | 20/05/2024 | Major Changes in the contents | Priyesh Parashar |
| V2.1 | 22/04/2025 | Updated Designation | Priyesh Parashar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 17/01/2022 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 26/06/2023 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 20/05/2024 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 25/04/2025 | Saravanan Sankaran | VP – Infosec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Stakeholders | Netradyne |
|  |  |
|  |  |

# Purpose

Change Management Process document is to provide end-to-end context for the Change Management Process. This document serves as an official process to be used by Netradyne, it introduces a Process-Framework and contains the workflow, roles, procedures, and policies needed to implement a high-quality process and ensure that the processes are effective in supporting the business.

Change Management is essential to provide a disciplined process for introducing required changes in IT environment with minimal disruption to ongoing operations.

Change Management is:

* Process to coordinate the change needed by business.
* Authorizes changes and coordinates change timelines to avoid conflict.
* Ultimately to support the change owner and the implementation of a successful change.

Change Management is Important since it:

* Manages risk and priority.
* Prioritizes to implement most important changes first.
* Rapid change capability for business.
* Maintains a complete view of change in the organization.

# Scope

All systems or services connected to or relying on the production network and services provided to Netradyne end users, are covered by the Change Management process. The scope of Change Management comprises aspects listed below.

The organizational scope of the Change Management Process includes changes related to supported IT Services.

The scope of this Process applies to:

* Any “system” within the live environment or attached to the live/production infrastructure.
* Any “system” that is promoted from the development environment into the live environment.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

## 4.1 Policies

The Change Management policies are required to instruct/guide all the stakeholders to make the process effective.

* The approving Change Manager is accountable for the successful execution of the process, to mitigate impact and risk for stakeholders/customers.
* Change Management will manage all changes made to the production environment. This includes changes implemented by internal organizations.
* Effective Risk and Impact Assessment is enforced and is considered the foundation of Change Management.
* All stakeholders are informed of changes that affect the Service(s) they receive prior to change implementation.
* There is a mechanism to implement expedited changes to the managed environment with minimum destabilization of that environment.
* The number of changes deemed expedited are reduced to a pre-specified and progressive metric through proper planning.
* A CAB exists and the Change Manager is the ultimate decision-making authority within the CAB.
* A Change implementation plan is required prior to change deployment.
* All Service Providers will fulfil their roles in compliance with the Change Management process.
* An RFC will not be approved for implementation unless relevant back-out plans are in place.
* The Change Supervisor is ultimately accountable for the success of their respective change.

## 4.2 Key Contacts & Escalation Matrix

In the event if there are any concerns, it should be escalated to the defined list:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **E-mail ID** | **Contact Number** | **Role** |
| Saravanan Sankaran | saravanan.sankaran@netradyne.com | +91 9444161422 | VP - Info Security & IT |
| Priyesh Parashar | priyesh.parashar@netradyne.com | +91 9845227014 | Change Manager |

## 4.3 Controls

### 4.3.1 Segregation of Duties

* Approvers within the change request will not participate in any other role within a ticket. Example: Requestor, Implementer, Developer or Promotion Manager cannot approve their own change, etc. In such scenarios individual approvers will be added for CAB phase approval.
* Developers or Approvers are not authorized to deploy code into the Acceptance and/or Production environments.
* Promotion Managers are not authorized to develop or approve code changes in any environment.

### 4.3.2 Segregation of Environments

Changes made to the Development, Acceptance, Failover or Production environments must be environment specific in order to allow for proper testing and tracking purposes.

### 4.3.3 Change Authorization

In scope changes must be authorized prior to implementation. Changes must be electronically approved within the tool unless working under an emergency change or evidence of approval was provided prior to implementation. e.g., E-mail, text etc.

### 4.3.4 Testing Evidence

* Change must be tested prior to implementation unless the activity cannot be pretested. Testing evidence must be referenced and if testing is not possible, an explanation should be provided.
* Change must be validated post implementation to ensure successful implementation. Evidence of success should be attached or referenced within the change request.

### 4.3.5 Change Documentation Quality

* Change Requestor / Implementer/Change Supervisor is accountable for change documentation which provides a level of detail and ensures that non-technical parties can clearly understand the scope of the change record.

### 4.3.6 Change Advisory Board Review

* Moderate, High, or Very High-risk Production / Failover Environment changes must be reviewed at the weekly Change Advisory Board (CAB) Meeting
* Exclusions include Emergency, Standard, Development, Non-Prod/ Acceptance Environment
* Moderate, High, and Very High-risk change must be formally reviewed at the CAB prior to implementation.
* Exceptions such as off-line review/approval may occur given that justification has been accepted and approved by the Global Change Management team.
* Appropriate stakeholders must be present for proper review and approval. (Change Implementor/supervisor, Change Team)

### 4.3.7 Emergency Change Advisory Board (ECAB) Review

* High-risk Emergency Changes would be reviewed for documentation.
* Retro ECAB will happen on Tool within five business days post emergency change implementation to verify the documentation and the process being followed in a correct manner.
* ECAB jury would consist of Change manager, Supervisor/Implementor & CI/Service Owner

## 4.4 RACI

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Roles/Activities** | **Change Requester** | **Change Manager** | **Change supervisor** | **Change implementer** | **Process Owner** | **CAB** |
| Request Change | R, A | I | I | I |  |  |
| Review and assess change |  | A, R | C, I | C, I |  |  |
| Assess technical and business impact and risk |  | R | AR | C |  |  |
| Approve change for built |  | R, I | A, R | R, C |  | I |
| Confirm implementation schedule and impact/Risk review |  | R | A, R | C, I |  | I |
| Approve for change implementation | I | C, R | R | C |  | A, R |
| Implement and validate change |  | C, I | C, I, R | A, R |  |  |
| Change Evaluation process |  | R, A, I | R | C, I, R |  |  |
| Close change | I | A, R | R | C, I |  |  |
| Process Improvement |  | A, R | C, I | C, I | A, R | I |

This section maps the Roles and Responsibilities to the various steps in the workflow.

* **R**esponsible: Those who do the work to achieve a task. There is typically one role with a participation type of Responsible.
* **A**ccountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom Responsible is accountable. Typically, the process owner is Accountable for a process, and there must be only one Accountable specified for each task or deliverable.
* **C**onsulted: Those who are not directly involved in the process but provide inputs and whose opinions are sought.
* **I**nformed: Those who receive outputs from the process or are kept up to date on the progress, often only on completion of the task or deliverable.

## 4.5 Activities

### 4.5.1 Weekly Activities

* Review Change
* Initial Approval
* Update Change
* Host CAB Meeting
* Change Governance

### 4.5.2 Monthly Activities

* Conduct PIR
* Conduct ECAB

## 4.6 Change Management Process Overview & Roles

### 4.6.1 Change Process Overview

Diagram

Description automatically generated

### 4.6.2 Change Management Roles

Each role is assigned to perform specific tasks within the process. Within a specific process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following table describes the typical roles defined for Change Management:

| **Role** | **Responsibility** |
| --- | --- |
| Change Requestor | The Change Requestor initiates the request for change and provides as much information within the ticket prior to assigning the change to the implementing support team.   * Identifies change requirements. * Creates change request. * Provides mandatory change requirements (Change plan, schedule, backout plan) * May share role as the implementer or tester |
| Change Manager | The Change Manager is responsible for the execution of the Change Management process. This includes operating the defined and agreed process, ensuring it interfaces with all other relevant processes.   * Setting targets * Reviewing the effectiveness and efficiency of the process, * Performing process audits * Managing the process improvement cycle. * Facilitates the Change Management process. * Facilitates Change Advisory Board (CAB) * Review the efficiency and effectiveness of the Change Management processes and make recommendations for improvement. * Responsible for education of the Change Management process * Approves/Rejects changes based on the information provided. * Conducts PIR call and reviews responses updated by Implementor/supervisor. * Create a problem record for changes needing PIR. * Conduct UCR for unauthorized Changes and reviews the responses updated by Implementor/supervisor. * Monitors, review and analyze changes to ensure: * Minimum Acceptance Criteria is met. * Changes are closed appropriately. * Reporting / Metrics * Reports process breaches * Analyze failed/ backed out Changes. * Drive Post Implementation Review for unsuccessful changes. * Review all outstanding RFCs awaiting consideration or awaiting action. * Review schedule of change for conflicts * Analyze Change Records to determine any trends and to proactively identify process issues. |
| Change Supervisor | The change supervisor is responsible for leading, coordinating and supporting the planning, build and test, and implementation phases associated to a change.  Responsible for:   * Leading and coordinating with technical capability teams. * Assigning individual/SME to plan, Build & Test and Implementation * Obtaining regular updates for planning, testing and implementation * Providing required information to Change Manager * Approve Change in Schedule & CAB phase. * Review the 4-eye check. * Review the Change plan, test plan, implementation plan, schedule. |
| Change Implementor/  Coordinator | The implementor role includes the below responsibilities:   * Owns the lifecycle of the change (this includes obtaining approvals, closing tasks and closing the overall change ticket in a timely manner) * Provides change minimum acceptance criteria. * Coordinates change related activities such as resource coordination, pre/post implementation and/or testing activities. * Presents relevant changes to Change Advisory Board (CAB) * Ensures that any incident, either caused by or pending change is related to the subject change. * Update the PIR questionnaire for Failed Changes. * Assist in RCA analysis for failed changes. * Update UCR questionnaire for unauthorized changes.   A Change Implementor role may also be referred to as release packaging or deployment practitioner. Responsibilities include the above implementor role responsibilities as well the building, testing and physical deployment tasks associated with approved changes that may be assigned to multiple individuals.   * May implement technical changes in Development, Acceptance, Production or Failover environments.   A Developer Coordinator role responsibility includes the coordinator role responsibilities as well as the below responsibilities:   * Develops application code changes in the development environment. * Relates any relevant request number to the Production change. |
| Process Owner | A senior process consultant with the ability and authority to ensure the process is rolled out and used by all departments within the IT organization.  Responsible for:   * Owns and maintains Change Management Policy and standards. * Ensures that Change Management is aligned with IM processes. * Owns Change Management product and related workflows. * Defining the overall mission of the process. * Establishing and communicating the process mission, goals, and objectives to all stakeholders. * Resolving any cross-functional (departmental) issues. * Ensuring consistent execution of the process across the organization. * Reporting on the effectiveness of the process to senior management. * Initiating any process improvement initiatives |
| Task Assignee or Promotion Manager | * Ensures that proposed task work/date/times can be supported. * Implements changes in authorized environments. * May participate in testing activities. * Closes applicable task upon completion of work * Promotion manager may be an automated function within specific deployment tools. |
| Change Approver | * Reviews proposed changes for accuracy and validity. * Challenges any inaccuracies/risk/ impact within the proposed change. * Approves / Rejects changes in a timely manner. * The change approvers can include the Change Manager/Lead, Change Supervisor group peer, Service Owner/Manager, CAB. * Service owners/CI Owner to Provide Approvals for raising expedite & emergency changes (post validating the justification) * Service owners/CI Owner to Provide approval for Change window extension (where schedule is missed or change window needs to be extended) |
| Change Advisory Board (CAB) | The purpose of the CAB (Change Advisory Board) is to ensure that only changes that have met a minimum and agreed state of readiness are deployed into Production. There is adequate representation from the Service Owners/Manager, Requestor, Infrastructure/technical solution, and security leads, and if required 3rd party providers or suppliers or vendors) supports the assessment, prioritization, authorization, and scheduling of changes.  Review meeting facilitated by Change Manager to provide the following:   * A formal forum where changes are presented and vetted for impact, risk and conflict. * Reviews Production moderate and above risk level changes * Chaired by Change Management |
| CI Owner | Responsible for maintaining CI’s (Applications/Infrastructure) within the enterprise Configuration Management Database (ServiceDesk+). |
| Service Owner | * Represents the service across the organization. * Manages the risk of operating the service. * Designates technical lead and backup. * Coordinates communication among support staff and systems staff. |
| Application owner | Responsible for application processing. Typically, the application owner maintains application information, checks eligibility, makes the final determination, and authorizes benefits for a client. |

## 4.7 Change Management – Types & Process

### 4.7.1 Brief

Following are the details of the types of changes, the workflow followed & the process that will be executed in Netradyne.

Careful planning and adherence to the Change Management process can reduce any potential risk and impact associated with an individual Change.

### 4.7.2 Types of Changes

1. **Standard:** A well-defined, fully documented Change with low risk and impact. These Changes follow a predefined set of work instructions. These types of Changes are pre-approved by the CAB.

**Note -** If the standard change fails then it must follow normal change procedure for further four attempts, if all four attempts get successful then again it can be considered as a standard change.

1. **Normal:** Any temporary or permanent Changes to a service / infrastructure within a managed environment. Approval is delegated to specific groups / individuals for respective changes. CABs approve changes which are likely to have significant impact on the services, but low-risk changes are approved directly by Change Manager. All approved changes are scheduled on the Forward Schedule of Change (FSC). There should be lead time of 5 business days to log a normal change. Changes are still recorded and assessed to confirm that risk and impact is low/High/Medium.
2. **Emergency:** A Change required to be applied to a managed environment because of (or to prevent) the sudden loss or reduction of service. Emergency Changes are always derived from business-critical Incidents. Change to restore Service due to a very high impact incident, or to prevent an imminent outage that must be handled in a reactive mode. Retro ECAB will happen within 3 business days post emergency change implementation to verify the documentation and the process being followed in a correct manner.

**Note:** In Emergency change case, RFC will get initiated and then directly implementation will be carried out basis on verbal approvals over the call, later on documentation will take place and basis on documentation present assessment and Review will take place to get that initiated RFC approved.

**Emergency change Justification:**

* Emergency changes must be utilized for a high severity incident (P1/P2) or a potential MI.
* An incident with less than a Priority 1 or 2 must not utilize an emergency change.
* Retrospective emergencies may be used when time does not allow for ticket submission but must be entered and electronically approved within 48 business hours after the change implementation.
* Approvals must be captured prior to implementation and noted/attached within the change record as evidence of authorization.
* Misuse of the process may result as an unauthorized change.

1. **Expedited Change:** An Expedited change does not meet the lead time requirement for a normal change but is not an Emergency Change. It follows same process and approval flow as a ‘Normal’ Change, but lead times are much shorter and they require a reason for being expedited. These changes need Technical, Business and CAB Jury approval on tool. Normal rules for approval by CAB Jury apply. Expedited changes must meet the following justification:

* Required to address a current or impending Security concern.
* Required to resolve a current Production impacting incident which may not qualify as an emergency.
* Required to address an immediate business driven requirement which may have a financial or regulatory impact to the organization if not implemented.
* Required to address an oversight in change planning activities.

\*Expedited change may require additional approvals prior to implementation.

**Expedited change Justification:**

* Expedited changes must provide explicit justification.
* Examples of relevant expedited justification:
* Business Driven – A business requirement that may impact the business financial or regulatory if not implemented as soon as possible.
* Vendor Driven – A request from a 3rd Party Provider to address an urgent need that will cause impact if not addressed quickly.
* Security or Safety Driven – To address an urgent vulnerability or safety related scenario.
* Oversight – Planning issue by the Change Requestor or Project Team but required to meet a critical deliverable.
* Misuse of the process may result as an unauthorized change.

## 4.8 Change Management – Workflow & Work Level Instruction

### 4.8.1 Normal/Expedited Change

### 

| **Activity** | **Description** |
| --- | --- |
| **Request Change** | **Create / Update RFC (Request for Change/CR Form)**  Change Requestor identifies required information, such as contact information, requested schedule, business rationale (e.g., Functional enhancement to an application or service, increased performance/capacity/availability, resolution/fix to a known error). Change requestor will create/update RFC in ServiceDesk+.  Set of more Change Reason Codes as follows:   * Business Requirement * Resolution/Known error Fix * Upgrade * Patching * Functional Enhancement * Code * Demand/Build Deployment * Network Services * Install/Configure * Remove/Delete * Security * Application Software * Compliance * Access * Capacity * Other   **Identify Impacted Stakeholders**  Identify impacted stakeholders by identifying impacted CI's & services and indicate if they are in other jurisdictions (change authorization required). Identify if resources will be required from other jurisdiction(s) to assist in the change.  **Classify Change**  Change requestor will provide the initial classification elements. This includes completing an initial impact/risk assessment to determine the change type.  **Reference / Attached Supporting Documentation**  Include all documentation appropriate to the nature of the change Project Charter, Business Case, detailed Change Description etc.)  **Note:** If build-test is in-scope an approved & verified Implementation plan, back-out plan, communication plan etc. to be included at this time.  **Submit RFC for Acceptance**  Once the request is complete, submit for acceptance. |
| **Review & Assess Change** | **Validate Change Submission**  Verify that all information required to process the RFC has been provided.  **Verify RFC**  Verify that the RFC complies with Change Management Standards and any jurisdiction-specific policies and business requirements.  **Validate RFC Acceptance**  Verify that this is a legitimate RFC and within the scope. Identify and assign RFC to Change Supervisor for further Review and Assessment. |
| **Assess Technical & Business Impact/Risk** | **Identify Impacted Technical and Business Stakeholders and circulate assessment**  Change Supervisor requests appropriate participation to assess the change using the standard risk/impact assessment (RIA) in ServiceDesk+. If RFC impacts other entity (like Service or application), the Change Supervisor coordinate for required assessment.  **Complete Technical and/or Business Impact and Risk Assessment**  Change Supervisor conducts both Business Risk-Impact assessments and Technical Risk-Impact assessments.  **Consolidate Assessment Results**  Change Supervisor will consolidate input from all jurisdictions, which may inform updates to the overall impact and risk assessment. If Assessments are provided from multiple jurisdictions, Change Supervisor will use worst case scenario to update the RIA (Risk impact analysis) to arrive at a single value for Risk, Impact, and derived Change Type value. |
| **Build & Test Required?** | **Build & Test**   * If Build-test activities are not required, or if this is a re-assessment following Build-test completion, then request an approval for Implementation. * If Build-test is required, then ask requestor to attach test artifacts or test approvals. |
| **Approve Change for Build** | **Include RFC in CAB Agenda and Schedule**  Take the steps necessary to include the RFC in the agenda for upcoming CAB meeting. This may be necessary across multiple CABs.  **Change Advisory Board Review of RFC**  CAB members review the RFC to provide additional input. The Change Requestor may be requested to speak on these items and provide additional details in the change as identified by the CAB prior to full change approval.  **Change Authorized?**  CAB members will review RFC, Risk-impact Assessment and associated documentation and provide authorization.  **Review RFC**  The RFC is reviewed for approval.  **Change Approved?**  Prior to approval, Change Manager will ensure that all conditions (from conditional Authorizations) are satisfied. Change Manager approves start of Build-Test, involving CAB at its discretion. This can only occur if all jurisdictions have authorized the change.  **Update Change Record and Communicate Change Approval**  Update the record with all necessary information and ensure the change is approved accordingly.  **Plan Build & Test activities:**  Once approved for Build & Test, Change Supervisor would:   * Assign Resources * Design and Build Change * Create Implementation, Test and Back-out Plans. * Test Change * Update RFC with Build- Test and Implementation documentation. * Update RFC with Revised Implementation Date (if required) |
| **Confirm Implementation Schedule & Impact / Risk Review** | **Reassessment Required?**   * Compare requested date against known scheduling constraints and review scope of the original change request to determine if the change needs to be re-assessed. * Change Manager consults CAB based upon jurisdiction-specific detailed required. * Circulate Assessments(s) for Technical and/or Business Impact. * Change Manager requests impacted jurisdiction Service Owner/CI Owner to provide authorization. * Complete Technical and/or Business Impact and Risk Assessment * Change Supervisor & Change Assessors use the RIA (Risk impact analysis) model to conduct both Business Risk-Impact assessments and Technical Risk-Impact assessments:   This may be a Re-Assessment prior to Implementation approval if significant scope change encountered during Build-Test  **Consolidate Assessment Results**   * Change Supervisor will consolidate input from all jurisdictions. If Assessments are provided from multiple jurisdictions, Change Owner will: * Use worst case scenario to update the RIA (Risk impact analysis) to arrive at a single value for Risk, Impact, and derived Change Type value. * Consolidate Operational feedback which may influence build/test and/or implementation plans.   **Review and Update Change Classification (if required) and Set Final Implementation Schedule**   * Use priority and RIA (Risk impact analysis) to select candidate RFC's to be rescheduled and negotiate revised date(s) with the Change Owner(s) to minimize or eliminate impact. * If RFC being considered for change is in another jurisdiction, request Change Manager from that jurisdiction to facilitate access to the Change Owner. |
| **Approve Change for Implementation** | **Include RFC in Change Advisory Board Agenda and Schedule**  If CAB approval is required, take the steps necessary to include the RFC in the agenda for upcoming CAB meeting. This may be necessary across multiple CABs.  **Change Advisory Board Review of RFC**  CAB reviews all RFC to approve the change for implementation.  **Change Authorized?**  CAB Members will review RFC, Risk-impact Assessment and associated documentation and provide authorization.  Prior to approval, Change Manager will ensure that any conditions (from conditional Authorizations) are satisfied. Owner jurisdiction Change Manager approves implementation, involving CAB at his or her discretion. This can only occur if all jurisdictions have authorized the change.  **Update Change Record and Communicate Change Approval**  Update the record with all necessary information and ensure the change is approved accordingly. |
| **Implement and Validate Change** | **Coordinate Implementation**  Confirms that any prerequisite prep work has been performed and implementation resources:   * are available at scheduled times * have documented implementation, verification, and back-out plans * understand their implementation tasks * are aware of implementation task dependencies * are aware of communication protocols * are aware of change window timelines, back-out go/no-go decision point * have necessary parts, files, media * have necessary logical & physical access * if multiple Change Implementers involved ensure a lead is assigned and task created & assigned appropriately   **Perform Implementation Procedures**  Execute Implementation tasks as per approved, documented implementation plan. Document and resolve any minor deviations/corrections in the implementation procedures. Report implementation results to Change Manager.  **Perform Verification Procedures**  Execute Verification tasks as per approved, documented verification plan and report verification results to Change Manager.  **Successful Implementation?**  Check to see if successfully implemented as planned. If yes, go to "Update RFC Completion Status" and if no, go to "Back-out Change?"  **Minor Defects?**  If the cause of verification failure is known and corrective action is minor in scope, the Change Supervisor may direct Change Implementer to fix the defects and re-conduct Verification Testing. The Change Implementer must document any deviations/extra steps performed during this activity. At no time can the corrective action jeopardize the ability to execute the back-out plan within the originally approved Change Window.  **Back-out Change?**  Determine whether the change can/should be backed out or whether it will be left in a partially implemented state. Change requestor/implementers and Service Owners may be consulted to assist in this decision if the direction to contact the Change Requestor is detailed in the change verification/back-out plans.  **Coordinate Back-out**  Communicate back-out decision to implementation team and Change Manager. Ensures that implementation resources:   * understand back-out tasks * are aware of back-out task dependencies * are aware of communication protocols * are aware of change window timelines   **Perform Back-out Procedures**  Perform the back-out and report back-out results and any deviations to Change Supervisor and Change Manager.  **Perform Back-out Validation Procedures**  Execute validation tasks as per approved, documented plan and report results to Change Owner. Document any deviations and send results to the Change Supervisor.  **Successful Back-out?**  Determine whether change appears to have been successfully backed out as planned. If yes, update the RFC completion status.  **Update RFC Completion Status**  Change Implementor/Supervisor will update RFC completion codes (Successful or not) in ServiceDesk+.  **Log Planned Outage Incident and Associate to RFC**  Create a Service Outage Incident that serves as the Master Incident  **Log Service Interruption Incident**  Contact Service Desk and report Incident associated to RFC and include details in the Incident that describe the deficiencies in the production environment resulting from the partially implemented change (i.e. functionality, performance, outage). At the end relate the incident in RFC along with PBI (Problem Ticket Number).  **Resolve Planned Outage Incident**  Resolve the Planned Service Outage Incident that was previously created. |
| **Change Evaluation Process** | **Confirm Change Outcomes**  Change Manager asks Change Requestor and supervisors to validate the change success from their perspective.  **Confirm Business Objectives Met**  Change Requestor uses Validation criteria to confirm that requested business objectives were met.  **Monitor Change**  Determine if any adverse effects resulted from Change that was not encountered during verification testing. If related issue exist, incidents should be reported.  **Identify Adverse Change Impacts**  Determine if the change introduced has adverse service impact on impacted jurisdictions either during the change window (e.g., Impact to unintended CI's) or following implementation.  **Consolidate Validation Feedback**  Consolidate input received (to be used by PIR). Note that feedback may indicate unacceptable impact, which could lead to logged Incident and subsequent RFC to remediate or back-out the change. Set the change closure code with an initial value.  **Update Change Record**  Change record is updated accordingly, including the change closure code if necessary. |
| **Close Change** | Ensure appropriate documentation is attached to RFC (updated instructions, PIR if applicable, related incident and problem ticket if applicable etc.), update Change Record Status as Closed and ensure closure code is updated.  **Closure Codes are as follows:**   * Successful * Successful with Issue * Cancelled * Backed Out - Customer Impact * Backed Out - No Customer Impact * Withdrawn * Implemented with Customer Impact   **In above closure codes some will be considered as failed change:**  Failed change means if the impact of the issue may be high which results in unexpected Major Incident and a business loss to the customer.   * Backed out – Customer Impact * Backed out – No Customer Impact * Implemented with Customer Impact |

### 4.8.2 Emergency Change

## Diagram Description automatically generated

| **Activity** | **Description** |
| --- | --- |
| **Emergency Change Raised**  **(Post ITLT approval)** | **Click on ‘Create New’** |
| **Review Change details** | **Validate Change Submission**  Verify that all information required to process the RFC has been provided.  **Verify RFC**  Verify that the RFC complies with Change Management Standards and any jurisdiction-specific policies and business requirements. |
| **Is there MI?** | **YES**  **or**  **NO** |
| **ECR Justification & proceed with E-CAB** | **Is there MI - YES**  Change manager verifies the business justification added in the change record and schedules a E-CAB. |
| **Link incidents, update reason and impact** | **Is there MI - YES**  Implementer links incident with the CR, updates the business justification for an emergency change and adds the business impact of the change. |
| **Schedule the E-CAB for review** | Change manager schedules a E-CAB. |
| **Change Approved on Tool?** | YES  Or  NO |
| **Proceed with Change Implementation** | Change is fully approved and can be implemented within planned window. |
| **Is change Successful?** | **Change Manager verifies if Change Successful or not**  **YES**  **or**  **NO** |
| **Update Implementation task & Closure Code** | **Change Successful - YES**  Implementer updates the change status as successful |
| **Update Implement task as close incomplete** | **Change Successful - NO**  Implementer updates the one of the below Closure Code:   * Backed Out- Customer Impact * Backed Out- No Customer Impact * Implemented with Customer Impact |
| **Update PIR question** | Implementer updates the PIR questionnaire and attach the sheet in the change |
| **Review PIR & Raise PRB record** | Change Manager reviews the PIR, schedules a PIR discussion call. An Problem record needs to be created after the CR is closed. |
| **Close Change** | Ensure appropriate documentation is attached to RFC (updated instructions, PIR if applicable, related incident and problem ticket if applicable etc.), update Change Record Status as Closed and ensure closure code is updated.  **Closure Codes are as follows:**   * Successful * Successful with Issue * Cancelled * Backed Out - Customer Impact * Backed Out - No Customer Impact * Withdrawn * Implemented with Customer Impact   **In above closure codes some will be considered as failed change:**  Failed change means if the impact of the issue may be high which results in unexpected Major Incident and a business loss to the customer.   * Backed out – Customer Impact * Backed out – No Customer Impact * Implemented with Customer Impact |

### 4.8.3 Standard Change

Diagram, engineering drawing

Description automatically generated

| **Activity** | **Description** |
| --- | --- |
| **Initiate RFC** | **Click on ‘Create New’** |
| **Select and update template** | **Requestor to select Standard Change Template**  **Short description -** Follow the given nomenclature to update the short description “**Environment-Region- CI-Description of change”**  **Category -** The domain for which the change is being raised.   * Application Software * Business Service * Database * Datacentre * End User Devices * Network/Telecom * Security * Server Computing * Storage   **Source** – Based on who is requesting for the change.  **Change Supervisor group –** The person who would be supervising the change lifecycle.  **Effect if Change Is not implemented** – What would be the consequences or how would the environment be affected if the change is not implemented.  **Change Plan** - High level overview of the change implementation plan.  **Backout Plan** - Detailed description/steps calling out the backout / rollback plan if the change implementation fails.  **Backout Duration –** Total duration required for rolling back the implemented change.  **Test Plan** – Detailed Description of the test plans performed before implementing the change, ensure the compatibility is also checked.  **Planned Start date** – Date when the planned change implementation will start.  **Planned End date** – Date when the planned change implementation will end.  Note: The above duration should include the Change implementation time + back out duration + Pre-test/Post-test + buffer time  **Implementation Plan** – Detailed step by step activity of the planned change implementation. If the implementation is going beyond 24 hrs., then day wise plan needs to be updated.  **Reference / Attached Supporting Documentation**  Include all documentation appropriate to the nature of the change Project Charter, Business Case, detailed Change Description etc.)  Note: If build-test is in-scope and approved & verified Implementation plan, back-out plan, communication plan etc. to be included at this time.  **Submit RFC for Acceptance**  Once the request is complete, submit for acceptance and update the below.  **Check for conflicts** – should be checked on all changes to ensure there are no conflicts for the CI |
| **Submit change** | **Submit change post updating mandate info** |
| **Review Change** | **Validate Change Submission**  Verify that all information required to process the RFC has been provided.  **Verify RFC**  Verify that the RFC complies with Change Management Standards and any jurisdiction-specific policies and business requirements. |
| **Change Acceptable** | **Validate RFC Acceptance**  **YES**  The Change manager reviews and assesses the change to ensure the mandate fields are updated and the documentation is up to mark.    **NO**  In case of any further amends required, the implementer is notified about it. |
| **Amend required changes** | The implementer makes the requiredamendments to the CR. |
| **Implement change per schedule** | Change is fully approved and can be implemented within planned window. |
| **Validate the change for success or failure** | Implementer validates success or failure of change |
| **Is change Successful?** | Change Manager verifies if Change Successful or not  **YES**  or  **NO** |
| **Update Implementation task & Closure Code** | **Change Successful - YES**  Implementer updates the Implement phase and the Closure Code |
| **Update Implement task as close incomplete** | **Change Successful - NO**  Implementer updates the Implement phase & Closure Code:   * Backed Out- Customer Impact * Backed Out- No Customer Impact * Implemented with Customer Impact |
| **Update PIR question** | Implementer updates the PIR questionnaire and attach the sheet to the change |
| **Review PIR & Raise PRB record** | Change Manager reviews the PIR, schedules a PIR discussion call. Create a problem record after the CR is closed. |
| **Close Change** | Ensure appropriate documentation is attached to RFC (updated instructions, PIR if applicable, related incident and problem ticket if applicable etc.), update Change Record Status as Closed and ensure closure code is updated.  **Closure Codes are as follows:**   * Successful * Successful with Issue * Cancelled * Backed Out - Customer Impact * Backed Out - No Customer Impact * Withdrawn * Implemented with Customer Impact   **In above closure codes some will be considered as failed change:**  Failed change means if the impact of the issue may be high which results in unexpected Major Incident and a business loss to the customer.   * Backed out – Customer Impact * Backed out – No Customer Impact * Implemented with Customer Impact |

## 4.9 Change Relationship with Other Process

## 

## 4.10 Key Definitions

This section describes key terminology. Definitions are provided in Glossary: Abbreviations and Definitions. There are several core definitions that the Change Management process operates around. These definitions are:

|  |  |
| --- | --- |
| **Terminology** | **Definition and Description** |
| Incident  (Part of Incident management) | **ITIL Definition:** An Incident is an unplanned interruption to an IT service or a reduction in the quality of an IT service.  **Further Description:** An incident be a user requesting help for something that is not working. For example, “I can’t print”, “I can’t access the Internet”. In any situation where something does not work, and the specific details are not known it is an incident. |
| Problem  (Part of Problem management) | **ITIL Definition:** A Problem is a cause of one or more incidents.  The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.  **Further Description:** A problem is a more specific definition of something that has gone wrong. Quite often several similar incidents are linked to a common problem. In the case where several users are not able to print a “problem” will be defined saying something like “there is a problem with the network”. A Problem is more defined than an Incident. |
| Known Error  (Part of Problem management) | **ITIL Definition:** A Known Error is a problem that has a documented root cause and a workaround.  **Further Description:** A known error is logged when the specific root cause is known for a group of problems/incidents or a single major problem. The known error record will exactly define what has gone wrong and the solution so that it does not happen again. Continuing our example, a known error would be: “There is a fault with the network card in the printer in department X that is causing the printing problems”. A Known Error is more defined than a Problem. |
| Workaround | **ITIL Definition:** A workaround is used for Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available.  **Further Description:** Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record |
| RFC– Request for change | **ITIL Definition:** Change Request CR forms are submitted to the Change Manager to gain authorization for the implementation of changes into the application or infrastructure environment. |

## 4.11 Unauthorized Changes

Unauthorized Change activity is an act of misconduct and may potentially result in dismissal or disciplinary action. Unauthorized change activity poses risk to the organization, which may cause an unplanned service disruption. All cases will be reported and escalated to management appropriately.

Unauthorized changes may include but are not limited to the following scenarios:

|  |  |
| --- | --- |
| **Scenario** | **Description** |
| Change Request was not approved by all approvers | Implementer performed in scope change activities without obtaining all the required approvals. |
| Change implementation occurred without a change record. | Change activity was performed without a change request in place.  Exception would be a qualifying Emergency change record which would be submitted retrospectively post verbal approval from Service Owner/CI Owner |
| Change implemented is different than what was agreed/approved | Change implementation includes additional unapproved change activity that was not originally within scope of the approved change request. |
| Change was implemented outside of the agreed window | Change implementation exceeded the agreed upon window without preauthorization from the Service Owner or Change Management. |
| Misuse of Emergency Changes | Emergency change which was not utilized for addressing or preventing a high impacting incident. |

Unauthorized changes will be reviewed and processed through the UCR process. Implementer completes a set of questionnaires in the UCR Form and uploads in ServiceDesk+ and Change Manager reviews the answers.



## 4.12 Post Implementation Review (PIR)

PIR is mandatory for all High, Critical, Normal and Emergency changes and for all changes where implementation was unsuccessful. PIR report should be taken, prepared, and shared within two business days.

for any failed Change Advisory Board-approved changes, conduct a post-implementation review within seventy-two (72) hours and present the findings to the stakeholders.

## 

## 4.13 4 Eye Check

## 4 Eye check is a peer review process to ensure quality assurance. Below checklists needs to be filled before and after implementing a Change and uploaded in SD+ (attach in RFC) for all Normal Changes.

## 

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| Change | Any action either physical or procedural which modifies or impacts the production or defined aspects of the non-production environment. |
| Change Advisory Board (CAB) | A group of people who are tasked with evaluating changes to the IT environment. The CAB is comprised of technical staff and key decision makers. |
| Change Owner | The person owning a Change Request from start to end (i.e. when CR is closed) |
| Change Manager | The person responsible for processing change requests, chairing Change Authority Board meetings, coordinating Changes and reporting change activity to management |
| Change Schedule | A schedule for the controlled Deployment of authorized Changes |
| Configuration Item (CI) | A component of an IT infrastructure. CI's may vary widely in complexity, size and type – from an entire system (including all hardware, software and documentation) to a single software module or a minor hardware component. |
| Configuration Management | The process of identifying and defining the CI’s in a system, recording and reporting the status of CI’s, and verifying the completeness and correctness of CI’s. |
| Key Performance Indicator (KPI) | Key Performance Indicators are clearly defined objectives with measurable targets, set to judge process performance |
| Process | A connected series of actions, activities or operations performed with the intent of satisfying a purpose to achieve a goal. |
| Request for change (RFC) | A form or screen, used to record details of a request for a change to any component of an IT infrastructure or application |
| Service Desk | The IT provider’s organisational unit, function or process that makes the IT provider accessible to IT users. |
| Configuration Management Database (CMDB) | A repository within the ITSM tool that contains all information about the hardware and software components used in an organization's IT environment and the relationships between those components.  A service component, application or infrastructure that needs to be managed to ensure the successful delivery of services. CI's may vary widely in complexity, size and type – from an entire system (including all hardware, software and documentation) to a single software module or a minor hardware component |
| Development Environment | IT environment used by developers to build and test solutions prior to UAT and Production deployments. |
| Failover Environment | IT environment which mimics the Production environment used to quickly recover IT services and/or data in the event of a disaster |
| IT infrastructure | The sum of an organization’s IT-related hardware, software, data communication facilities, procedures, and people. |
| IT service | A described set of facilities, IT and non-IT, supported by the IT service provider that fulfils one or more needs of the Netradyne’s supports. |
| IT Service Management (ITSM) | Term used to refer to the ITIL Processes such as Incident, Problem, Change Management, CMDB |
| Process | A connected series of actions, activities or operations performed with the intent of satisfying a purpose to achieve a goal. |
| Production Environment | IT environment where software and other products are in use for operational purposes. |
| Service Owner | An individual accountable for a specific IT Service or Application. Also known as Service Manager. |
| Users | Staff, Contractors, Service provider’s staff who work from Netradyne or their own organization facility for providing services to Netradyne. By providing services to Netradyne, they are expected to have access to Netradyne’s information in Digital or non-Digital form. |
| User Acceptance Testing (UAT) Environment | IT environment used to test software solutions prior to Production implementation. End users will test whether the solution meets expectations. |
| UCR (Unauthorised Change review) | Used for reviewing Unauthorised change implemented in an environment. |

# References

## Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=mRSIq4)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=RbfEhO)

[Netradyne Information Technology Policy and Procedure.pdf](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FInfoSecDocumentGovernanceRepository%2FShared%20Documents%2FHIPAA%202024%2FDocumentation%20Evidence%20HIPAA%2FApprovedDocumentFolder%2FIT2024%2FNetradyne%20Information%20Technology%20Policy%20and%20Procedure%2Epdf&parent=%2Fsites%2FInfoSecDocumentGovernanceRepository%2FShared%20Documents%2FHIPAA%202024%2FDocumentation%20Evidence%20HIPAA%2FApprovedDocumentFolder%2FIT2024)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

## Process/Procedures

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=xTyHtp)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=eCZUy6)

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=N697w0)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=Nzo34K)

[Netradyne IT Incident Management.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Netradyne%20IT%20Incident%20Management.pdf?csf=1&web=1&e=BPO1b6)

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |