**Change Control and Release Management Standards**

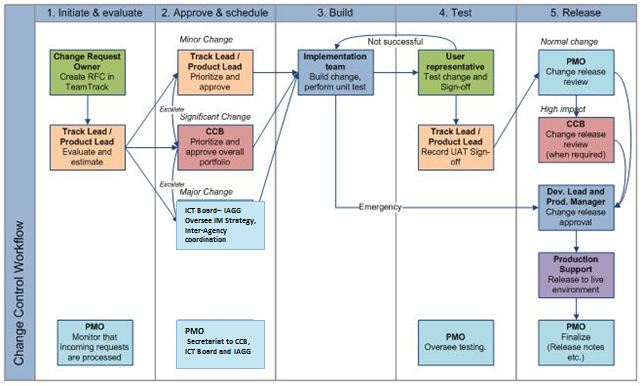
1. ICT systems and infrastructure play a critical role in the efficient operation of the organization. Changes to ICT systems and infrastructure may arise reactively as a response to problems or externally imposed requirements, or they may be proactive changes to reflect business improvement initiatives.
2. This document specifies how changes to ICT systems and infrastructure can be implemented and released into a live environment. This process exists in the context of ICT governance, as defined in the IM Strategy.
3. A comprehensive Change Control and Release Management process minimizes risks involved in introducing changes and it becomes a method of communication between stakeholders – the person requesting a change, the Change Control Manager and the team building the change. Other benefits associated with a structured Change Control and Release Management procedure include:
4. Protect the existing infrastructure and architecture
5. Ensuring that changes are aligned with a corporate strategy
6. Ensuring that proper business cases exist and that the solution is based on user requirements
7. Ensuring that changes are evaluated and benefits are measured
8. Avoiding duplication of system development
9. Ensuring changes are sufficiently tested
10. Ensuring communication and end user support and training is planned
11. Ensuring that rollback plans and contingency measures are planned
12. Identifying application release frequency
13. Validating decommission of a system
14. Communicating within and outside the effected group based on events
15. Providing a central repository for tracking all changes (including impact and risk analyses)
16. In addition, the Change Control and Release Management process assures metrics and reports that help Management judge the quality and effectiveness of Change Control and Release Management processes and tools.  A

1. The goal of the Change Control Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes – in form of change requests utilizing PHIRE— in order to minimize the impact of change-related incidents upon service quality, and consequently, to improve day-to-day operations of the organization. This includes an ICT Governance structure to ensure proper project management and quality control, as well as Performance and Risk Indicators that are mechanisms to measure the success and associated risk of changes.

**Scope**

1. The scope of Change Control and Release Management procedures involves planning, design, build, configuration, and testing of hardware and software to create a set of release components for the live environment. ICT infrastructure components subject to change control and release management include:
2. Application programs developed or customized in-house
3. Externally developed software Utility software
4. Internet domain names managed by UNDP
5. Supplier-provided systems software
6. Hardware, and hardware specifications
7. Instructions and user manuals
8. Change Control and Release Management procedures are mandatory for:
9. All ICT infrastructure items managed through UNDP Office of Information Management and Technology (ITM/BMS)
10. All corporate ICT Infrastructure items, i.e. ICT infrastructure items used by more than one Country Office or business unit.

**Flow Chart**

​

**Use PHIRE for All Change Requests**

1. Change control planning involves generation of change requests, which should be submitted in [UNall](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fundp.service-now.com%2Funall&data=04%7C01%7Cjosephine.opar%40undp.org%7C0d505c0bb46f49bf277908d8ff6a42bc%7Cb3e5db5e2944483799f57488ace54319%7C0%7C0%7C637540179133202666%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=OlFnPG2f9Iv6WMB1jMQdLZcbnPUWwZPYrN1xjPETNUE%3D&reserved=0) or using PHIRE software. Nevertheless, please note that ATLAS is being frozen until the implementation of the NextGen ERP.
2. Include in the Change Request, for high-risk changes, all testing and validation, vendor review, peer review, and detailed configuration and design documentation. Refer to a Non-Atlas Testing Guide for testing protocols, and the Project Manager is responsible to ensure:
3. All resources are identified and in place for the change
4. A clear goal has been set and met for the change
5. Create solution templates for deployments affecting multiple sites. Include information about physical layout, logical design, configuration, software versions, and deployment guidelines
6. Document the standards for configuration, software version, supported hardware, Domain Name System (DNS), device naming, design, and services supported
7. Ensure the change conforms to all organizational standards for design, configuration, version, naming conventions, and management
8. Create rollback procedures (before each release, the Project Manager and the implementation team should identify a rollback strategy depending on the project and create one for unforeseen incidents. The Change Release specialist checks if this action is taken and in place
9. Define escalation paths
10. Define affected users and downtimes for notification purpose
11. Change planning documentation, such as maps, detailed implementation procedures, testing procedures and rollback procedures, should be created and included in the PHIRE ticket.  The level of planning is usually directly proportional to the risk level of the change.

Caveat: The technical description of a change is an important aspect of the change request and should reference any standards within the organization that apply to the change. This will help to ensure that the change conforms to the current architecture and any engineering design guidelines or constraints.

1. Complete one of the following change request type procedures:
2. Planned Changes
3. Emergency Changes
4. Standard Changes
5. Atlas Changes

**Planned Changes**

1. Planned changes are normally scheduled changes, whether big or small.  They involve the following steps, including the completion and submission of a PHIRE change request:

|  |  |
| --- | --- |
| Step | Action |
| 1. | **Business case and requirements document**  The scope of a proposed change should include a complete technical definition and the purpose of the change. In addition, the requestor should include information describing who will be affected, both during the change period and after deployment. This may include business units, user groups, servers, and applications. The estimated cost and benefits must be documented in the form of a business case.  Required templates for business case and requirements reside at the [ITM PMO site](https://projserv01.undp.org/projportfolio.aspx). |
| 2. | **Change request submission**  Once the business case and requirements document are completed and signed off by the project manager, the change request will be submitted using [PHIRE software](https://cm.undp.org/tmtrack/tmtrack.dll?LoginPage&Template=loginform&Message). |
| 3. | **Review change request**  The Track Lead or Product Lead will evaluate the business case and classify the category.  The Track Lead or Product Lead has the right to reject invalid business cases or give suggestions. |
| 4. | **Approve or reject**  The Track Lead or Product Lead has a right to approve, reject, or request further clarification. Changes are defined in the Change Magnitude Criteria below:  Minor changes are approved by Track Lead or Product Lead  Significant changes are approved by Change Control Board (CCB)  Major changes are approved by the ICT Board (IIAG for Atlas changes) |
| 5. | **Build change**  Change is developed in accordance with current architecture and any engineering design guidelines or constraints. Significant and major changes are managed as separate projects, as defined in the Change Magnitude Criteria below. Minor changes are built under the supervision of respective Development Leads.  If there is a need to significantly change the approved requirement document or specifications during the implementation period, the Development Lead or Project Manager is responsible for highlighting the change to the CCB Secretary and obtaining a new approval. |
| 6. | **Unit system and integration test**  When the development work is completed, the development team will conduct unit, system and integration testing.  The Development Lead or the Project Manager will sign-off for UAT readiness prior to the UAT session (see [Testing Guide](http://content.undp.org/go/prescriptive/ICT-Documents-/;jsessionid=afW7ByTBipf5?bbp.11.pane=0&bbp.70.row=1609933.f&bbp.16.pane=0&bbp.v=1609933&bbp.e=s&bbp.s=23&bbp.9.pane=0&bbp.10.pane=0&page_to_display=0&doc_id=1760079&bbp.12.pane=0&bbp.151.ps=10&bbp.23.s) for detailed testing phases). |
| 7. | **User acceptance testing**  The Change Release and Testing Specialist will facilitate the User Acceptance Test with testers from the business community. The Development Lead or Project Manager will provide the UAT test scripts and support the testing process on giving guidance to testers and resolving issues. Track Lead or Product Lead will record the UAT sign-off provided by End Users or Business Owners. |
| 8. | **Release**  The Change Release & Testing Specialist will review the test results, complete the [Release Process Checklist](https://intranet.undp.org/global/popp/it/Pages/change-control-and-release-management-standards.aspx#_Annex_II_-) and submit to the Development Lead and Production Manager for the migration to the Production environment. The Change Release & Testing Specialist will also provide input to the CCB on the overall statistics and exceptions for the monthly release.   The Change Release & Testing Specialist will notify the Communication team for release communication and Help Desk for support. All training materials and other relevant documents need to be updated at this phase.  The final cost and benefit will also be captured by the PMO. |
| 9. | **Change review**  The change manager will compile statistics on change requests and note if the change was successful or not (including lessons learned and any best practices). |
| 10. | **Communication**  The change request owner or Track Lead / Product Lead will ensure communication of any change through Release Notes, with automated email sent through PHIRE, and, for major changes, through a user-community email detailing the change and its implications for users. |

**Emergency Changes**

1. Emergency changes are urgent changes required to address problems. The number of urgent, proposed changes should be kept to an absolute minimum, because they are generally more disruptive and prone to failure. The procedures that are in place to handle emergency changes should be flexible enough to facilitate rapid resolution of Production problems, including documentation of who is authorized to make emergency changes, and how to contact these individuals.

1. A sufficient number of people should be available who can resolve emergencies, or those people should be easily accessible at all times to prevent a roadblock in the problem resolution process.
2. It is imperative that both communication and the integrity of documentation are maintained through an emergency change.  This is the time when documentation is needed most, so documenting the steps taken to resolve the problem is of utmost importance.
3. Finally, when considering changes, it must be determined if the change will resolve the existing problem and if it will cause other problems. Below are the steps that are critical for an emergency change process, including the completion  and [submission of a PHIRE change request](https://intranet.undp.org/global/popp/it/Pages/change-control-and-release-management-standards.aspx#_To_submit_a):

|  |  |
| --- | --- |
| Step | Action |
| 1. | **Requirements document**  The scope of a proposed emergency change needs to be created and submitted, indicating the technical definition and the purpose of the change as well as the reason for the urgency and the impact of delaying the change.  Required templates for business case and requirements reside at the [Project Portfolio Server Project Management site](https://projserv01.undp.org/projportfolio.aspx). |
| 2. | **Change request submission**  Once the business case and requirements documents are completed and signed off by the project manager, the change request will be submitted using [PHIRE software](https://cm.undp.org/tmtrack/tmtrack.dll?LoginPage&Template=loginform&Message). |
| 3. | **Approve or reject**  The Track Lead or Product Lead approves the changes based on the following points:   1. An immediate Severity 1 or Severity 2 Production problem (see [Severity Level Definitions](https://intranet.undp.org/global/popp/it/Pages/change-control-and-release-management-standards.aspx#_Emergency_Changes_%E2%80%93)) 2. An evolving problem that would rapidly lead to a Severity 1 or Severity 2 production problem if it is not immediately prevented   The Development Lead will analyze the change and give clearance to the Development team for implementation of the changes. |
| 4. | **Change is built**  Change is developed in accordance with current architecture and any engineering design guidelines or constraints. |
| 5. | **End-to-end testing by Implementation Team**  When the development of the new change is complete, testing of urgent changes should be carried out by the Implementation Team. Completely untested changes should not be implemented.  The Development Lead or Project Manager is responsible for this task (see [Testing Guide](http://content.undp.org/go/prescriptive/ICT-Documents-/;jsessionid=afW7ByTBipf5?bbp.11.pane=0&bbp.70.row=1609933.f&bbp.16.pane=0&bbp.v=1609933&bbp.e=s&bbp.s=23&bbp.9.pane=0&bbp.10.pane=0&page_to_display=0&doc_id=1760079&bbp.12.pane=0&bbp.151.ps=10&bbp.23.s) for detailed testing phases). |
| 6. | **Release**  Change Release and Testing Specialist will approve the change. |
| 7. | **Post-emergency documentation**  Updating documentation is critical to ensure valid, up-to-date information. During emergency changes, it is easy to forget to make updates because of the frantic nature of emergencies.  However, undocumented changes often result in increased downtime if the solution is unsuccessful.  Therefore, the respective project manager is responsible for all emergency changes documents update after the fact. The Change Release & Testing Specialist will also inform CCB on monthly reports. |
| 8. | **Change review**  The Change Release & Testing Specialist will compile statistics on change requests and note if the change was successful or not (including lessons learned and any best practices). |
| 10. | **Communication**  The change request owner or Track Lead/Product Lead will ensure communication of any change through Release Notes, with automated email sent through PHIRE, and, for major changes, through a user-community email detailing the change and its implications for users. |

**Emergency Changes: Severity Level Definitions**

|  |  |  |  |
| --- | --- | --- | --- |
| Severity Levels | Definition | Scope | *Examples* |
| 1. Critical business impact | A major production outage, major performance degradation, or instability causing significant impact to many users and/or time-critical data processing. | Many or most users are unable to function. Mission critical system down.  Mission critical application down.  Mission critical server or connection down. | *E-mail not available*  *Impossible to process payment* |
| 2. Major business impact | Large number of users is impacted. Entire group or department is experiencing a similar problem. Small number of customers can’t use a mission critical application. | Multiple users unable to function.  Major performance issues.  Multiple users running on contingencies or workarounds. | *Application not working* |
| 3. Minor business impact | Individual unable to use application(s). | Customer can work with minimal impact to their productivity.  Customer having difficulty, but basically operational.  Customer unable to carry out their necessary tasks. | *Bug in application* |
| 4. Normal request | Individual request or problem that does not block usage of systems. | Customer needs information or a standard service.  Customer has simple question or problem.  How-to's or Procedural questions. | *Minor bugs*  *Questions* |

**Standard Changes**

1. A standard change is an accepted solution to an identifiable and relatively common set of requirements, where authority is effectively given in advance of implementation. For each ICT infrastructure item, the change request owner can approve a list of defined standard changes. These changes can be initiated and executed without requiring explicit approval in each individual case.
2. The Change Control Board (CCB) will review the approved list of standard changes at regular intervals.

**Atlas Changes**

1. Please refer to the [Atlas Change Control Manual](https://intranet.undp.org/global/documents/it/AtlasChangeControlManualv1.4.docx) for specific protocol procedures, and details on Atlas-specific release management.

**Testing**

1. Please see System Testing Guides for detailed testing information, as follows:

**Non-Atlas** [**Testing Guide**](http://content.undp.org/go/prescriptive/ICT-Documents-/;jsessionid=afW7ByTBipf5?bbp.11.pane=0&bbp.70.row=1609933.f&bbp.16.pane=0&bbp.v=1609933&bbp.e=s&bbp.s=23&bbp.9.pane=0&bbp.10.pane=0&page_to_display=0&doc_id=1760079&bbp.12.pane=0&bbp.151.ps=10&bbp.23.s)

|  |  |  |
| --- | --- | --- |
| Testing Phases | Objectives | Test & Sign-off |
| 1.  Unit Testing | Verify the business transactions related to a specific development object (e.g., a program) function as designed and meet the specified business requirements accurately | Developer |
| 2. System Testing | Validate functionality within the module, or across a subset of modules | Functional & Technical Team |
| 3.  Integration Testing | Verify the major functions of the system operate together in a cohesive manner | Functional & Technical Team |
| 4.  Users Acceptance Testing | Confirm the applications and processes meet end-user requirements, and operate within the applicable technical environment | End Users |
| 5. Performance Testing | Validate the technical components of the system and infrastructure while providing acceptable performance for typical production loads | Technical Team |

**Communications**

1. Once a change has been approved, details of the change must be communicated, by setting expectations, aligning support resources, detailing operational requirements, and informing users. PHIRE has e-mail notification and the Change Release Specialist will trigger the e-mail notification (sending Release Notes). See the Authority section for all communications points within the process. The risk level and potential impact to affected groups as well as scheduled downtime as a result of the change will dictate the communication requirements.

**Conclusion**

1. Change Control and Release Management is an essential part of all organization’s overall security posture. Failure to properly manage change can result in vulnerabilities as well as lost time from a lack of control for both planned and unplanned changes can lead to opportunity for hackers and/or people with ill intent to damage or gain unauthorized access to systems. The process of defining/implementing control policies/procedures for change is continuous, like the changes to an environment.

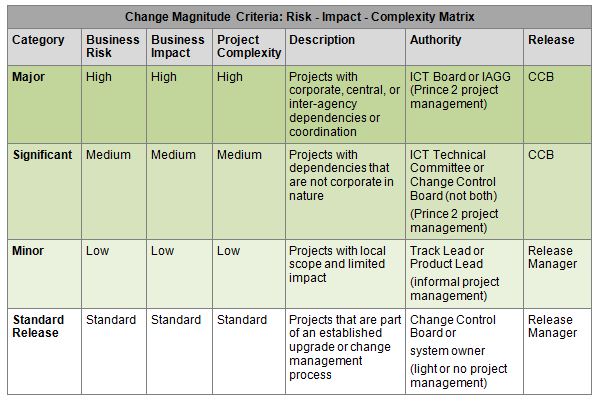
**Structure Element - Inputs**

1. Resources, especially PHIRE,  and sites are available at the following location: [Change Release and Testing Management](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.undp.org%2Funit%2Foolts%2Foimt%2Fpmo%2FSitePages%2FCR_TM.aspx&data=05%7C01%7Cemiliana.zhivkova%40undp.org%7Cece25dd6c49640c9db7408dace045ec9%7Cb3e5db5e2944483799f57488ace54319%7C0%7C0%7C638048815417296752%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=W2KuI%2FZPj9z6wSAp7URF%2BNDpxe4autguOGz1QlF4%2Fho%3D&reserved=0)

Note: The IAGG may depute to the CCB requests on changes in Atlas where it feels the purview of IAGG is not necessary.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Change Request Process – User Definitions and Process Steps** | | | | | | |
| Authority | Process Steps | | | | | |
| Initiating -  Approval before work starts  (Project Portfolio Oversight) | Running – Build the change (Change Request Tracking) | Running – Approve the built change | Running – Release the change into live environment | Closing – Communicate to users | Closing - Change Review |
| ICT Board - Transitional Committee (for Atlas: Inter-Agency Governance Group - IAGG) | Oversee implementation of IM strategy, Inter-Agency coordination |  |  |  |  |  |
| PMO Office | Assist with project documents preparation | Oversee project management  process |  |  |  |  |
| Project Manager | Finalize business case and requirements documents | Oversee change request implementation | Follow up on project implementation and testing |  | Monitor project progress  Draft Release Notes | Review in PHIRE |
| Implementation Team under supervision of Development Lead |  | Implement and test change request. Update PHIRE |  | Raise Release Service Request |  |  |
| Change Request Owner (sponsor) | Draft business case and requirements documents | Submit change request | Follow up on implementation |  | Close change request |  |
| Track Lead  or Product Lead |  | Reviews change request and assigns change size category | Signs off on testing (UAT) and follows up on build implementation |  |  |  |
| Change Control Board (CCB)\* | Review overall portfolio of initiatives and recommend prioritization |  | Approval of Monthly release schedule; post facto review of emergency approval. |  |  | Assess-ment and quality of recent changes |
| Change Release & Testing Specialist | Review Change Request | Perform all CCB Secretariat functions | Coordinate testing (UAT) and sign-off | Prepare and validate Release Process Checklist | Implementation Team (PHIRE)  Inform appropriate Help Desk (e-mail)  Email and post Release Notes | Review in PHIRE |
| Development Lead and Production Manager |  |  | Emergency change sign-off | Approve release in PHIRE |  |  |

1. Change Magnitude Criteria



1. Change Request Risk Assessment - Each change request should be assigned one of the following categories:
2. High – Changes have the highest impact on user groups or particular environments and may even affect an entire site.  Change rollback is time-consuming or difficult.  Management must be aware of the change and its implications, and all users must be notified
3. Moderate – Changes can critically impact user environments or affect an entire site, but change rollback is a reasonably attainable scenario.  Users may be notified of a moderate-risk change
4. Low – Changes have minor impact on user environments and change rollback is easy.  Low-risk changes rarely require more than minimal documentation and User notification may be unnecessary

|  |  |  |
| --- | --- | --- |
| Level | Definition | Testing and Validation Requirements |
| 1 | High potential impact to large number of users or business-critical service because of the introduction of new product, software, topology, or feature; change involves expected network downtime | Lab validation of new solution, including documented testing, validation, and what-if analysis showing impact to existing infrastructure  Completion of an operations support document  Rollback plan, implementation plan, and adherence to the change process  Recommend solution pilots and a preliminary design review prior to testing |
| 2 | High potential impact to large number of users or business-critical service, because of a large increase of traffic or users, backbone changes, or routing changes; change may require some network downtime | What-if analysis performed in lab to determine the impact to existing environment in regards to capacity and performance  Test and review of all routing changes  Rollback plan  Implementation plan  Adherence to change process  Design review for major routing changes or backbone changes |
| 3 | Moderate potential impact to smaller number of users or business service, because of any non-standard change, such as new product, software, topology, features, or the addition of new users, increased traffic, or non-standard topology, change may require some network downtime | Requires engineering analysis of new solution, which may require lab validation  Implementation plan  Adherence to change process |
| 4 | Low potential impact, including adding new standard template network modules (building or server switches, hubs, or routers), bringing up new WAN sites or additional proven access services, and all Risk Level 3 changes that have been tested in the production environment.  Change may require some network downtime. | Implementation plan  Adherence to change process |
| 5 | No user or service impact, including adding individual users to the network, and standard changes.  No expected downtime | Optional adherence to change process |

1. Performance indicators provide the mechanism to measure the success of the change control management process.  The indicators should be reviewed periodically to ensure that change planning and change control management are working well.

|  |  |
| --- | --- |
| Performance Indicators | |
| Change Control Management metrics by functional group | Includes the percentage and quantity of change success by functional group and risk level. Emergency changes should be identified separately in the metrics by functional group, including the success rate for attempted fixes.  Functionality groups include any ICT teams making changes, possibly including server administration, network administration, database groups, application teams, and facilities.  Risk level is important because generally higher risk changes fail or create incidents.  A change failure may be defined as any change that is rolled back or causes a problem incident resulting in user downtime. |
| Change success rate | To target change success, start with a baseline of Change Management metrics.  The CMA can then identify potential issues and set overall goals.  A reasonable overall goal for change success should be 99 percent across all functional groups.  If the organization is experiencing a higher rate of change failure, it should be targeted for improvement. |
| Change rate per system | The Change Release Library will be used for archiving the change history.  The information can be used to investigate change rates in general for overall planning purposes.  The Change Release Manager should archive the Change Planning history in the Change Release Library. |
| Undocumented change audit | The quantity and risk level of undocumented changes should be investigated.  Undocumented change is a common problem in almost all organizations.  It must be continually reiterated that team members are required to use the required change control process, even though it adds time and efforts. |