

Policy and Procedure for Change Management

Policy Statement

All modifications to World Bank's production Information Technology (IT) environment, encompassing systems, applications, infrastructure, and configurations, must rigorously adhere to a formal, documented, and approved change management process. This process is instituted to minimize operational disruption, ensure the continued stability and integrity of services, and maintain the robust security posture of the Bank.

Scope

This policy is universally applicable to all IT systems, network devices, software applications (whether developed in-house or procured from third parties), and all supporting infrastructure components that have a direct or indirect impact on World Bank's daily operations, data integrity, or service delivery. This includes changes to hardware, software, system configurations, network architecture, database schemas, and operational procedures.

Roles and Responsibilities

Effective change management relies on clearly defined roles and responsibilities to ensure accountability and smooth execution :

- **Change Requester:** Any World Bank employee, contractor, or designated team initiating a proposal for a change. The Requester is responsible for providing a comprehensive justification and initial details for the proposed change.
- **Change Owner:** An individual, typically a manager or team lead, who is ultimately accountable for the successful planning, execution, and outcome of the change. The Change Owner champions the change through the process.
- **Change Manager:** A designated role responsible for the overall administration and governance of the change management process. This includes facilitating Change Advisory Board (CAB) meetings, ensuring adherence to procedures, maintaining change records, and reporting on change management performance.
- **Change Advisory Board (CAB):** A cross-functional group comprising representatives from key stakeholder areas, including IT Operations, Cybersecurity, relevant Business Units, Compliance, and Risk Management. The CAB is responsible for the formal review, evaluation, approval, or rejection of all significant and major change requests, based on assessed risk and business impact.
- **Emergency Change Advisory Board (ECAB):** A subset of the CAB, or designated senior individuals, empowered to make rapid decisions on emergency changes.
- **Implementers:** The technical teams or individuals tasked with the actual execution of the approved change according to the defined implementation plan.

- **Testers:** Designated teams or individuals responsible for validating that the change has been successfully implemented and meets its objectives without introducing unintended negative consequences.

Procedures

The change management process at World Bank is structured to ensure that all changes are systematically evaluated, authorized, implemented, and reviewed:

- **Change Request (RFC) Submission:** All proposed changes must be initiated through a formal Request for Change (RFC) submitted via the Bank's designated Change Management System. The RFC must be comprehensive, utilizing a standardized form that captures critical information. This includes:
 - A clear description of the change and its purpose.
 - Detailed justification and expected business benefits.
 - Assigned urgency and requested implementation timeframe.
 - A thorough assessment of potential impacts: technical (on existing systems and services), business (on operational processes and users), security (potential new vulnerabilities or impact on existing controls), and compliance (adherence to regulatory mandates).
 - Identification of all affected systems, applications, and Configuration Items (CIs) from the Configuration Management Database (CMDB).
 - A detailed proposed implementation plan, including step-by-step actions and timelines.
 - A comprehensive test plan outlining the testing strategy, test cases, and success criteria.
 - A robust rollback plan detailing procedures to revert to the previous stable state if the change fails or causes unacceptable disruption.
 - An estimation of required resources (personnel, budget, tools).
 - *Security Manager's Perspective:* At World Bank, any RFC pertaining to systems that process financial transactions, manage sensitive customer data (Personally Identifiable Information - PII), or affect critical infrastructure undergoes a mandatory, in-depth security impact assessment. This assessment is conducted by the Cybersecurity team and is a prerequisite for the RFC to be considered by the CAB. This ensures that security implications are proactively addressed before any change is approved.
- **Change Classification & Prioritization:** Upon submission, each RFC is classified and prioritized to determine the appropriate level of review and approval required :

- **Standard Changes:** These are pre-approved, low-risk, frequently performed, and well-documented changes with a proven history of success (e.g., new user account creation based on an approved template, patching a non-critical workstation with a tested patch, replacing a failed like-for-like network switch). Standard changes follow documented Standard Operating Procedures (SOPs) and typically do not require individual CAB approval but are logged for audit purposes.
- **Normal Changes:** These are planned changes that are not standard and require a full assessment and formal approval by the CAB. They carry a moderate level of risk and impact (e.g., upgrading a departmental application server, implementing new firewall rules for a specific project, minor modifications to a non-critical financial reporting tool).
- **Major Changes:** These are high-impact, high-risk changes that often involve significant resources, extensive planning, and potential for widespread service disruption. Major changes require approval from senior management, potentially beyond the standard CAB, and involve rigorous testing and communication protocols (e.g., core banking system upgrade, data center migration, implementation of a new enterprise-wide security platform).
- **Emergency Changes:** These are changes that must be implemented with extreme urgency to resolve a major incident (e.g., system outage affecting critical services) or to address a critical security vulnerability that poses an immediate threat (e.g., zero-day exploit). Emergency changes undergo an expedited assessment and approval process, often by a designated Emergency CAB (ECAB) or authorized senior personnel. While the immediate focus is on swift resolution, comprehensive documentation, testing (where feasible), and a post-implementation review are mandatory.
 - *Use Case (Emergency Change):* A critical vulnerability (CVSS score 9.8) is publicly disclosed for the operating system used by World Bank's primary internet-facing SWIFT gateway servers. Exploits are reported in the wild. The Security Manager, in collaboration with the Head of IT Operations and the CISO, immediately convenes an ECAB. The vendor-supplied patch is rapidly assessed for applicability. A limited, isolated test is performed on a non-production gateway instance. Given the extreme risk, the patch is approved for emergency deployment to production gateways within a 4-hour window. A full RFC, detailed impact analysis, and a thorough post-implementation review are documented within 24 hours of the change.
- **Assessment and Approval:** All Normal and Major RFCs are formally reviewed by the CAB. The CAB evaluates the change based on its justification, potential benefits,

associated risks (including security, operational, financial, and reputational risks), resource availability, and alignment with World Bank's strategic objectives. The security impact analysis provided by the Cybersecurity team is a critical input to this decision-making process.

- *Security Checkpoint:* Any change that involves modifications to firewall configurations, network access control lists (ACLs), identity and access management (IAM) systems, encryption mechanisms, or other core security controls requires explicit documented approval from the Chief Information Security Officer (CISO) or a designated delegate from the Cybersecurity leadership team, in addition to CAB approval.
- **Planning and Scheduling:** Once a change is approved, the Change Owner, in coordination with the Change Manager and implementers, finalizes the detailed implementation plan and schedule. Scheduling considers business operational calendars, peak processing times, potential service impact, defined maintenance windows, and any dependencies on other systems or changes.
- **Testing:** All changes, particularly Normal and Major ones, must be thoroughly tested in a dedicated, non-production environment (e.g., development, staging, UAT) that mirrors the production environment as closely as possible, before deployment to production. Test plans must cover functionality, performance, security, and integration aspects. All test results, including evidence of successful completion, must be documented and attached to the RFC.
 - *Security Manager's Perspective:* For any changes affecting critical financial systems, such as payment processing platforms or customer account databases, World Bank mandates comprehensive end-to-end security testing. This includes automated vulnerability scans of the changed components, regression testing of existing security controls, and, for major changes, targeted penetration testing exercises to ensure no new vulnerabilities are introduced.
- **Implementation:** Approved and tested changes are implemented by the designated technical teams according to the finalized plan and schedule. All implementation activities are logged. For software changes, version control systems must be utilized to track code modifications and enable rollback if necessary.
- **Verification and Validation:** Following implementation, post-implementation testing (PIT) is conducted to verify that the change was executed successfully, achieved its intended objectives, and did not cause any unintended adverse effects on the production environment or other connected systems. Business users may be involved in User Acceptance Testing (UAT) at this stage for changes impacting their processes.
- **Rollback Plan:** A documented and tested rollback plan must be in place for every Normal and Major change. This plan details the steps to revert the system(s) to their

previous stable state should the change implementation fail or result in critical issues. The decision to invoke a rollback plan is typically made by the Change Owner in consultation with the Incident Management team and CAB, if necessary.

- **Communication:** Clear and timely communication is maintained with all relevant stakeholders throughout the change lifecycle. This includes notifications prior to implementation (detailing scope, timing, and potential impact), status updates during implementation, and confirmation upon successful completion or invocation of a rollback.
- **Documentation & Review:** All aspects of the change, including the RFC, assessment details, CAB approvals, test results, implementation logs, and verification outcomes, are meticulously documented within the Change Management System. Post-Implementation Reviews (PIRs) are mandatory for all Major changes, Emergency changes, and any Normal changes that experienced issues or required a rollback. PIRs aim to assess the success of the change, identify any lessons learned, and recommend improvements to the change management process itself.

Framework Alignment

The World Bank's Change Management Policy and Procedures are designed to align with internationally recognized best practices and standards, including:

- **ISO/IEC 27001:2022:** Specifically, Annex A control 8.32 (Change Management) , which mandates that changes to information processing facilities and systems be controlled. The 2022 version consolidates previous controls (A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4 from ISO 27001:2013) into a more holistic change management control.
- **ITIL (Information Technology Infrastructure Library):** The process incorporates core ITIL change management principles, such as RFCs, CAB, change classification, and PIRs.
- **NIST Special Publication 800-128 (Guide for Security-Focused Configuration Management):** This NIST guidance emphasizes the importance of formal change control processes for maintaining secure configurations of information systems.
- **FFIEC Guidelines:** Financial industry regulations implicitly require robust change management to ensure the stability and security of IT systems supporting financial operations.

Real-World Example (Normal Change)

The Core Banking System (CBS) team at World Bank proposes an upgrade to a new minor version of the database software underpinning the CBS. An RFC is submitted through the central Change Management System.

- **RFC Details:** The RFC details the vendor's rationale for the upgrade (security patches, minor performance enhancements), the specific database version, a list of affected CBS modules, and the proposed weekend maintenance window. It includes a risk assessment identifying potential data migration issues (low risk for minor version) and temporary service unavailability during the upgrade (planned). The test plan outlines functional testing of all critical CBS transactions (loan disbursement, fund transfers, account inquiries) and specific security regression tests on authentication and authorization modules. The rollback plan involves reverting to a full system snapshot taken immediately before the upgrade.
- **CAB Review:** The CAB, comprising representatives from IT Operations, CBS Business Unit, Cybersecurity, Risk Management, and Compliance, reviews the RFC. The Cybersecurity team confirms that the security patches included in the new database version address several known medium-severity vulnerabilities. The CBS Business Unit confirms the maintenance window is acceptable and has communicated it to internal stakeholders.
- **Approval & Testing:** The CAB approves the change. The upgrade is first performed in the dedicated CBS staging environment, which is a close replica of production. All functional and security tests are executed, and results are documented as successful.
- **Implementation:** During the scheduled weekend maintenance window, the IT Operations team, guided by the CBS technical team, performs the database upgrade on the production system. Progress is communicated to stakeholders via the established channels.
- **Verification & PIR:** Post-upgrade, the CBS is brought online, and a predefined set of critical transactions is executed to validate functionality. System performance metrics and security logs are closely monitored for 48 hours. A Post-Implementation Review is conducted one week later, confirming the success of the upgrade and noting the successful mitigation of the identified vulnerabilities.

Table: Change Management Workflow by Change Type

Change Type	RFC Required & Detail Level	Risk Assessment Level	CAB Approval Required	ECAB Approval (if applicable)	Testing Rigor	PIR Required
Standard	Yes (Simplified/Pre-auth)	Low (Pre-assessed)	No (Pre-approved SOP)	N/A	Low	No (Periodic review of SOPs)
Normal	Yes (Full Detail)	Medium	Yes	N/A	Medium-High	For failed/problematic changes
Major	Yes (Extensive Detail)	High	Yes (Senior Mgmt+)	N/A	Extensive	Yes (Mandatory)
Emergency	Yes (Post-facto if needed)	High (Expedited)	No (ECAB/Delegate)	Yes	Limited/Post	Yes (Mandatory, within 24-48 hrs)

- **Value of Table:** This table provides an essential, at-a-glance summary of how different types of changes are processed within World Bank. For a financial institution of this scale, where changes can range from routine administrative tasks to major system overhauls with significant financial and operational implications, such a clear delineation is vital. It ensures that the level of scrutiny, approval, and testing applied to a change is directly proportionate to its potential risk and impact. This structured approach supports regulatory compliance by demonstrating a consistent and risk-aware change management process, helps in resource allocation for change activities, and ensures that all changes, regardless of their nature, are managed within a controlled framework, thereby safeguarding the Bank's operational stability and security.