IT Change Management Policy

Policy Owner: CF - Information Technology (IT)	**Approval Date:** March 1, 2017
Approver: Linda Clement-Holmes	**Effective Date:** April 1, 2018
Contact: Eugene Kholodenko	**Scope:** Global

1.0 Intent

The intent of the Change Management Policy is to formally document management expectations and ensure consistent and appropriate development and implementation of IT change management standards, procedures, and guidelines across P&G.

The purpose of this policy is to ensure that all changes to the IT production environment are managed through established standards and processes so that changes are applied correctly and do not compromise the security and availability of business applications, computer systems or networks.

2.0 Scope

This policy applies to all organizations, individuals, including third party partners, who deploy, manage, or support P&G IT applications, data, platforms, software, networks and information systems across the entire P&G IT production environment.

3.0 Policy Requirements

P&G requires that a change management process must be established for all types of changes for all IT assets, -- such as operational systems, applications, platforms, software -- information systems and networks.

The change management process shall be reviewed on an established regular basis to assess its effectiveness, and subsequently provide improvement updates to the process where necessary (e.g. modifications to processes in response to changes in identified business risks)

All regulated systems that will undergo changes must also comply with the Validation and Change Management Standard Operating Procedure (SOP), in addition to these change management (see References).

3.1 Change Management

i. Changes must be recorded, evaluated, authorized, prioritized, tested, and reviewed in a controlled manner.
ii. There must be documented standards and procedures for managing all change types.
iii. Formal responsibilities and procedures must be in place to ensure satisfactory control of all changes.
iv. The personnel involved in the change management process must be competent on the basis of appropriate education, training/certification, skills and experience to properly execute the change.

3.1.1 Change Request

i. All requests for change must have a valid record opened, processed, and tracked in the approved system of record.
ii. Proposed changes must have a designated P&G owner.
iii. P&G change owner is responsible for ensuring that the change management process is followed and that all relevant information is captured and documented.
iv. Clear segregation of duties must be maintained between the change owner and the change manager.
v. Change requests must have a valid justification (e.g. Legal, business, operational, regulated or security related) and be reviewed for appropriateness.

vi. Change requests must document the test plan, migration plan, test results, implementation plan, and back-out plan in the system of record.

vii. A schedule containing details of the changes and their proposed deployment dates must be communicated to interested parties.

viii. Change requests must include documentation of a complete quality assurance review.

ix. Change requests must include specific configuration items identified in the configuration management database.

x. Change requests must comply with the relevant *Service Asset and Configuration Management Process*.

xi. Change requests must be analyzed at regular and systemic intervals to identify trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.

Note: Regulated computer systems must also comply with Validation SOP QAS-S-04 requirements for change control.

3.1.2 Change Risk Management

i. A P&G Change Owner must be in place and must be accountable overall for risk management for all IT production changes (including risk identification, assessment, and mitigation).

ii. Changes must be thoroughly assessed for risk using the P&G Change Risk Assessment Standards. This assessment must be documented within the system of record.

iii. The result of the change risk assessment must determine the mandatory change approval process and requirements. The change must not proceed for implementation if these approvals and requirements are not met.

iv. Segregation of duties must be maintained between the developer and the person responsible for transferring the change to the production environment.

3.1.3 Approval

i. Each organization must be covered by a Change Advisory Board reflective of its operational model to review, confirm, and approve proposed IT changes.

ii. All changes must undergo P&G approval before their implementation

iii. All approvals must be documented within the system of record.

3.1.4 Testing

i. Changes must be tested according to the P&G testing standards and frameworks prior to implementation.

ii. The level of test scope, effort and sequencing and test environment and test data requirements must be defined based on risk.

iii. Test results for changes must meet all agreed success criteria for the change to be approved.

3.1.5 Release and Deployment Management

i. A release management process must be developed and documented covering all IT systems across P&G.

ii. All changes to IT systems must go through a documented release management process.

iii. Documentation containing details of the approved changes and their proposed deployment dates must be established and communicated to interested parties. This schedule of change shall be used as the basis for planning the deployment of releases.

3.1.6 Post-Implementation

i. All post-change implementation artifacts (change success/failure results, test results, approvers, etc.) must be documented according to all relevant documentation standards.
ii. Immediate post-change validation must be performed to ensure that changes are made correctly and securely, and that there is no adverse impact on P&G's operations or security.
iii. All changes must be evaluated using P&G post-implementation review standards, prior to closure.
iv. Systemic periodic checks must be performed to identify unapproved changes.

3.1.7 Back-out plans

i. The activities required to reverse or remedy an unsuccessful change must be planned, tested, and documented within the system of record to understand the full extent of possible risk.
ii. The change must be fully reversed or remedied if unsuccessful.

4.0 Definitions

Change	The addition, modification, or removal of anything that could have an effect on any IT service. This includes changes to all systems (platforms, networks, applications, hardware, software) architecture, processes, tools, metrics and documentation, as well as changes to IT services and configuration items.
Change Advisory Board	A collegial body that assesses, reviews, approves, and prioritizes requested changes.
Change Manager	An individual accountable and responsible for controlling the lifecycle of all P&G IT services changes with the primary objective of facilitating and supporting business need driven changes, while ensuring minimum disruption to IT services.
Change Management	The process responsible for controlling the lifecycle of all P&G IT services changes with the primary objective of facilitating and supporting business need driven changes, while ensuring minimum disruption to IT services.
Change Owner	A P&G individual who initiates a request for a change, and is accountable and responsible for the success of the change end-to-end.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT Service, an aggregation of work products that is designated for configuration management and treated as a single entity in the configuration management process. This aggregation consists of all required components: hardware, software, and other items that comprise a baseline. Examples include but are not limited to: applications, software, operating systems, platforms, servers, databases, firewalls, switches, routers, and etc. A configuration item does not include the settings, parameters, attributes needed to ensure the running of a system or its hardware.
IT Production Environment	A controlled IT environment containing live IT services (including applications, systems, networks, platforms, hardware and software) used to deliver IT services to the business.
IT Service	A service provided to an IT consumer, by an IT service provider. An IT service supports P&G's business processes and is made of a combination of people, processes and technology.

Segregation of Duties	Controls designed to prevent error and fraud by ensuring that at least two individuals are responsible for separate parts of any task.

5.0 References

- NIST CSF - PR-IP-3
- ISO 38500 – 5.2; 5.5
- ISO27002-2013 - 12.1.2; 10.1.2
- ISF – Standard of Good Practice – CF7.6
- ITIL – V3 (2nd edition 2011)
- ISO/IEC 20000 – Version 1
- Service Validation and Testing Policy & Standards
- Release and Deployment Policy & Standards
- Validation SOP QAS-S-04
- Validation Policy QAS-P-03
- Change Management—WQA Reference Document - QAS-R-03 – version 1
- Standard for Change Control of a Regulated Computerized System