



**Policy Owner** Catherine McCully (mccully.c)  
**Policy Contact** Willah Magbanua (magbanua.wr)  
**Approver** Catherine McCully (mccully.c)

**Scope** Global  
**Effective Date** July 1, 2024  
**Approval Date** December 7, 2023

# IT Change Management, Service Validation & Testing Policy

**Effective Date: July 1, 2024**

Last Publish Date: October 1, 2019

## 1. Purpose

The intent of this Policy is to document management expectations of IT Service Validation, Testing & Change management standards, procedures, and guidelines across P&G.

The purpose of this policy is to ensure that 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. This includes the service validation and testing requirements so that changes do what they are supposed to do (fit for purpose) and are available and are useful as seen by the users (fit for use).

## 2. Scope

This policy applies to organizations and individuals, including third party partners, who deploy, manage, or support P&G IT applications with Business Impact Assessment of medium or high risk, data, platforms, software, networks and information systems across the entire P&G IT production environment, or where required by Corporate Quality Assurance (CQA) SOP, QAS-S-04 Computer System Validation (CSV). This applies the establishment of new computerized systems, and changes caused by Projects, Releases, Hardware, and Technical Upgrades.

Note: In addition to above, please review Good Data Integrity Practices Policy (LDR-P-04, Veeva VV-QUAL-260956), Computer Systems Validation SOP (QAS-S-04, Veeva VV-QUAL-261218), and other helpful resources/ trainings for those signing validation documents deemed in scope of CSV.

## 3. Policy Requirements

### 3.1 Change Management

P&G requires that a change management process be established for changes to IT assets— such as operating systems, applications, platforms, information systems, and networks.

Changes must be recorded, evaluated, authorized, prioritized, tested, and reviewed in a controlled manner. Please refer to the IT Change Management Standard for the detailed requirements and controls supporting this policy

The change management process shall be reviewed on an established frequency to assess its effectiveness and



**Policy Owner** Catherine McCully (mccully.c)  
**Policy Contact** Willah Magbanua (magbanua.wr)  
**Approver** Catherine McCully (mccully.c)

**Scope** Global  
**Effective Date** July 1, 2024  
**Approval Date** December 7, 2023

subsequently improve the process where necessary (e.g. modifications in response to changes in identified business risks)

### 3.2 Incident Management (Effective February 2020)

Incidents tickets, in order to be classified as critical, must be evaluated and authorized accordingly. All Incident critical priority tickets should have a Root Cause Analysis (RCA) completed and a Corrective Action Plan (CAP) published. Please refer to the IT Change & Critical Incident Management Standard for the detailed requirements and controls supporting this policy.

### 3.3 Computer System Validation (CSV)

Regulated systems and those supporting product quality and/or consumer safety must also comply with the CQA Good Data Integrity Practices Policy LDR-P-04, Computer Systems Validation SOP QAS-S-04.

## 4. Policy Compliance

### 4.1. Compliance Measurement

The IT Service Validation, Testing and Change Management 2LoD will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and consultations.

### 4.2. Exceptions

Any exception to the policy must be documented using the Global IT Compliance Exceptions Process.

### 4.3. Non-Compliance

Violating this Policy may result in disciplinary action, consistent with local laws. Employees affected by this Policy are expected to read and follow it, directing any questions to the Policy Contact.

## 5. Definitions and Terms

Item	Definition or Terms
Change	The addition, modification, or removal of anything that could impact any IT service. This includes changes to 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 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 P&G IT services changes with the primary objective of facilitating and supporting business need driven changes, while ensuring minimum disruption to IT services.



**Policy Owner** Catherine McCully (mccully.c)  
**Policy Contact** Willah Magbanua (magbanua.wr)  
**Approver** Catherine McCully (mccully.c)

**Scope** Global  
**Effective Date** July 1, 2024  
**Approval Date** December 7, 2023

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.
Computerized System	Includes hardware, software, peripheral devices, personnel, and documentation (FDA Glossary, 1995) that support a business process.
Validation	Establishing documented evidence, which provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality characteristics. (US FDA definition, 1987)
Testing	The process consisting of all lifecycle activities, both static and dynamic, concerned with planning, preparation and evaluation of software products and related work products to determine that they satisfy specified requirements, to demonstrate that they are fit for purpose and to detect defects. [ISTQB V2.1 Glossary of Terms]

## 6. Appendix or References

### 6.1. Related Standards, Policies and Processes

- NIST CSF - PR-IP-3
- ITIL – V4
- ISO/IEC 20000
- [IT Change Management Standard](#)
- [IT Change Management Procedures](#)
- [LDR-P-04 Good Data Integrity Practices](#) Policy Veeva (VV-QUAL-260956)
- [QAS-S-04 Computer System Validation SOP](#) Veeva (VV-QUAL-261218)

### 6.2. Trainings & Knowledge Base

- [IT Change Management Trainings](#)
- [Computer Systems Validation \(CSV\)/ Data Integrity \(DI\) Training](#)

### 6.3. Review and Update History

Date	Performed By	Summary of Review or Update
August 12 2019	Armando Salas – IT Change Management Governance Leader	<ul style="list-style-type: none"> <li>• Removed the controls specified section.</li> <li>• Reduced the scope of applications that have a business impact assessment (BIA) of medium or high risk.</li> </ul>



**Policy Owner** Catherine McCully (mccully.c)  
**Policy Contact** Willah Magbanua (magbanua.wr)  
**Approver** Catherine McCully (mccully.c)

**Scope** Global  
**Effective Date** July 1, 2024  
**Approval Date** December 7, 2023

September 2 <sup>nd</sup> 2019	<ul style="list-style-type: none"><li>• Armando Salas</li><li>• Tim Elftman – Incident Management Governance leader</li></ul>	<ul style="list-style-type: none"><li>• Added Document Review &amp; Revision History section.</li><li>• Added Incident Management guidance for criticality priority classification and Post Incident resolution activities.</li></ul>
April 19 <sup>th</sup> 2023	Willah Magbanua	<ul style="list-style-type: none"><li>• Update Change Management contact</li><li>• Reviewed Policy and confirmed no change.</li></ul>
November 2023	Willah Magbanua	<ul style="list-style-type: none"><li>• Use updated IT Policy Template</li><li>• Integrated the 2 Policies:<ul style="list-style-type: none"><li>- Service Validation &amp; Testing Policy</li><li>- IT Change Management Policy</li></ul></li><li>• Update References and Links</li></ul>