Policy Owner: CF - Information Technology (IT)	**Approval Date:** October 31, 2018
Approver: Javier Polit	**Effective Date:** March 2018
Contact: Debbie Prado	**Scope:** Global

IT Risk Management Policy

1.0 Intent

The intent of the IT Risk Management Policy is to reinforce P&G's commitment to manage risks arising from Information Technology (IT) assets, so that we continue to win in the marketplace while maintaining an acceptable risk posture.

2.0 Scope

This policy applies to Information Technology risks as captured in the P&G Enterprise Risk Map and to all P&G organizations and individuals owning IT assets, including risks arising from third parties involved in the management of our IT assets.

3.0 Policy Requirements

A Risk Management process must be established to handle Information Technology risks. Each organization owning IT Assets must ensure:

1) On-going risk management is performed on Critical IT Assets via a formal and periodic organization wide risk assessment, which must include established standards covering:
    - Methodology for Critical Assets identification
    - Process roles and responsibilities
    - Methodology for risk assessment & prioritization
    - Approach to risk identification
    - Risk assessment frequency
    - Type of response strategies in relationship to risk scores and risk tolerance
    - Ownership for tracking and monitoring of risks
    - Risk register
    - Risk monitoring
2) An IT risks assessment should be performed when introducing new IT assets, or when significantly modifying existing IT assets. Each organization must have documented decision criteria to determine all cases where the assessment is applicable. Examples: i) new technologies ii) major change or expansion to existing IT Asset iii) business services outsourcing.

4.0 Definitions

Information technology (IT) Assets	Information Technology Assets are a sub-set of the Company Assets and can be any company-owned information, system, hardware, data, or device that is used in the course of business activities, or anything that connects to the P&G internal network directly.
Critical IT Assets	IT assets defined by the owning organization as **High** in Business Impact assessment based on confidentiality, integrity or availability,
Risk	The likelihood of a threat agent exploiting a vulnerability, and the corresponding business impact.
Risk Management	The act of determining which threats an organization faces, analyzing vulnerabilities, assessing the threat level, and determining how it will deal with the risk. Some of the major parts of risk management include developing the risk-management team, identifying threats and vulnerabilities, placing a value on the organization's assets, and determining how the organization will deal with the risk uncovered.
P&G Enterprise Risk Map	Identification and definition of risks starts with the P&G risk map. The map includes four types of risk: Strategic, Operational, Financial, and Compliance. These risk types are further divided into 16 risk categories. Each category is further broken down into individual risk themes. Each risk theme is distinct and is clearly defined. IT Risk category is under Operational risk type.
Risk Register	A repository for all risks identified; includes additional information about each risk, e.g. nature of the risk, reference and owner, risk response measures, etc.

5.0 Reference

5.1 Other Related P&G Internal Policies

- Business Continuity
- Asset classification

5.2 Frameworks

- ISO/IEC 27002
- NIST SP800-53
- ITIL