PSBank
PHILIPPINE SAVINGS BANK
Metrobank Group

INFORMATION TECHNOLOGY (IT) GOVERNANCE FRAMEWORK

Philippine Savings Bank's Information Technology (IT) governance framework defines the roles and responsibilities of the individuals and groups to ensure the alignment of IT strategy, IT infrastructure, performance, policies and guidelines with the Bank's overall business direction. The governance framework is implemented in accordance with the BSP's rules and regulations on IT Governance and Risk Management , recommendations of the Internal Audit Group and the COBIT standards.

The Bank's IT Steering Committee (ITSC) is tasked to cohesively monitor IT performance and institute appropriate actions to ensure the achievement of desired results. It is also accountable for designing and implementing the Board-approved Information Technology Risk Management System (ITRMS) and ensures that the Bank has long-term framework or vision of technology that promotes consistent and well-integrated technologies. ITSC provides periodic report to the Board on major IT projects, IT operational issues, IT capabilities, current issues and emerging technologies that may provide good business opportunities for the Bank.

Information Security Governance

PSBank's Information Security Governance provides assurance that information security strategies are aligned with and supports the business objectives and the strategic direction of the Board and Senior Management. It aims to continually strengthen the Bank's security landscape by implementing security controls and establishing a robust information security culture.

Information Security Division's (ISD) main responsibility is to protect the Bank's information assets at all times from unauthorized use by deploying multi-layered security solutions that preserve the confidentiality, integrity and availability of customer data without adversely affecting the business processes. The ISD is part of the enablers of the business that allows the business to grow and continue to be profitable while keeping the Bank's security risks properly managed and in check. It accomplishes this by implementing security policies, security awareness training, security risk management, security testing of applications and infrastructure, and the management of access control, data security and security incidents. ISD periodically reports to Management on the Bank's information security posture with updates on performance metrics and status of security projects.

Business Continuity Plan (BCP) Framework

The Bank's Business Continuity Governance process and effectiveness is managed and monitored by the Emergency Committee (EMCOM). The BCP aims to provide the Bank the capability to continue its critical functions and processes by identifying, assessing and managing emergency scenarios and other business interruptions. This includes IT Emergency Support Team consisting of a Team Leader and Assistant Team Leaders whose role revolve around Maintenance of the Business Recovery Center (BRC), making sure that critical data is being backed up both on site and off site and provision of assistance to other units to address IT-related requirements during emergencies or BCP testing. It also has planned contingencies for impact-based scenarios depending on financial, reputational, compliance, health and safety, operational and internal impact which are defined under the IT General Response Plan.