Cyber Security

Introduction

Gulf International Bank considers cyber security as one of the most important factors when it comes to protecting customer's and other stakeholder's interests.

We have established a comprehensive cyber security governance framework and layered security controls with an objective of protecting GIB's customer and business information from compromise of Confidentiality, Integrity, and Availability

Cyber Security Framework Overview

GIB's cyber security framework comes under the overall enterprise risk management framework and encompasses the following major components.

a. Board delegated cyber security supervision committee, which regularly meets and oversee the effectiveness of various cyber security, operations, programs, and initiatives.
b. Cyber security department, under the leadership of Chief Information Security Officer (CISO) for each GIB entity.
c. Cyber security strategy and initiatives aligned with the Bank's business strategy.
d. Various cyber security programs that are governed by associated policies, procedures, and standards.
e. Cyber security risk management, covering risk assessment, treatment and monitoring throughout the life cycle of systems and applications.

GIB's Cyber security framework is regularly maintained in line with the regulatory requirements for the respective GIB jurisdictions and aligned with the applicable international standards.

Cyber Security Policy and Programs Overview

Our cyber security posture revolves around layered security controls which is built on the "Defense-in-Depth" approach and consists of the below mentioned (not limited to) major programs:

a. Identity and Access management
b. Data and systems security
c. Security Operations, Threat intelligence, Brand protection and Incident management
d. Third party security management and maturity assessment
e. Vulnerability management
f. Cyber security training and awareness for all stakeholders
g. Cyber security risk assessment of people, process, and technology
h. Cyber Fraud monitoring and management

GIB's Cyber security defense, both perimeter and internal, is adequately equipped with industry-leading security solutions and supported by sufficiently skilled and trained resources. We constantly thrive to identify the opportunities for improvement through various proactive initiatives and address them in a timely manner to protect the bank's information assets and, most importantly, customer information from current and emerging cyber threats.

Data Privacy

GIB respects the privacy of its employees and Third Parties such as customers, business partners, vendors, service providers, suppliers, former employees, and candidates for employment and recognizes the need for appropriate protection and management of Personal Data.

In this respect, GIB is guided by the following principles in handling personal data:

- Accountability
- Transparency
- Choice and Consent
- Limiting Data Collection
- Limiting Data Use, Retention and Disposal
- Access to Data
- Limiting Data Disclosure
- Data Security
- Data Quality
- Monitoring and Compliance

Business Continuity Framework

The Bank ensures the validity of the departments' Business Continuity Planning (BCP) through an annual testing cycle that covers multiple scenarios that focus on the alternate data centre, alternate business continuity site, the contingency power mechanisms (such as back-up generators, uninterrupted power supplies), the cyber-resilience controls, the data back-up and restoration and the overall evacuation procedures including response to natural disasters and man-made threats.

The annual testing assesses GIB's state of readiness for foreseeable operational disruptions and provides:

- Continual reassessment of risks due to the changing environment and their potential impact to the Bank's business continuity
- Identification of changes to GIB's business operations that may affect the business continuity plans of departments and the overall BCP.
- Introduction of new recovery strategies and technologies that become available.