Enterprise Business Continuity and Incident Management

External Statement

Published: March 2020

Business Continuity and Incident Management Program

Business Continuity and Incident Management (BCCM) is a vital and integral part of the TD Bank Group's ("the Bank") normal business operations and follows internal policies and are designed to meet industry regulations. It includes the establishment of Enterprise-wide Business Continuity and Incident Management processes that provide safeguards to minimize the likelihood, cost, and duration of disruptions to business processes and services.

In preparation for, and during, incidents that could disrupt our business and operations, the Enterprise-wide Program supports the ability of Senior Management to continue to manage and operate their business, and provide customers access to products and services. Our robust Program includes formal Incident Management protocols and continuity strategies. The Bank regularly maintains and exercises Business Continuity and Disaster Recovery Plans to address the loss or failure of any component on which critical processes depend.

The Bank's Business Continuity and Incident Management Program combines business resumption planning, incident management, and planning for systems recovery. It is governed by Board approved Policies that are managed by the Bank's Operational Risk Management and Technology Solutions groups and aligns with professional practices of the Business Continuity industry.

Business Continuity Planning

All business and oversight functions are responsible for implementing Enterprise Business Continuity and Incident Management (EBCCM) practices and developing business-specific procedures, test plans, and protocols. All business and oversight functions must assess their risk tolerance and sensitivity to a business disruption by completing the Business Impact Analysis (BIA) process to establish an Enterprise criticality rating, which then determines recovery targets and the rigour of Business Continuity activities. The recovery strategy considers the nature, scale and complexity of the business to verify that it can reasonably continue to function and meet its various obligations in the event of an interruption. The Business Continuity Plans address the ability to recover from adverse business disruptions caused by a loss of key technologies (including cyber events), facilities, Third Party service providers, and employees' ability to work (including pandemic scenarios) and are supported by appropriate arrangements whether provided internally or outsourced. Our Business Continuity Plans are reviewed by business management and the Bank's EBCCM Group according to defined Bank Standards and Plan criticality level to verify reasonableness, quality, and compliance.

Exercising of Business Continuity Plans

All businesses must exercise their Business Continuity Plans in accordance with the Business Continuity and Crisis/Incident Management Policy. All exercise and test results are reviewed by the business management and the EBCCM Group according to defined Bank Standards and Plan criticality level. Exercises are required to verify that arrangements are sufficient to meet required continuity and recovery objectives. Criteria for exercise success are based on pre-established objectives to meet minimum Business Continuity Exercise Standards.

Crisis/Incident Management (Protocols and Exercises)

The Bank maintains an Enterprise Operational Crisis Management Protocol to facilitate effective oversight, ownership, and management of crises and incidents affecting the Bank; coordinated through the EBCCM group. Escalation and communication protocols are established, exercised, maintained, and coordinated in combination with business management to support appropriate decision-making, effective internal and external communications, and media-handling occur. All major Business Segments, as defined by the EBCCM Group, must maintain and exercise their Incident Management Protocols in accordance with established EBCCM standards. The EBCCM Group is responsible for maintaining and exercising the Bank's Enterprise Crisis Management Protocol.

Disaster Recovery Program

The Bank's Disaster Recovery Program is managed from within the Bank's Technology Risk Management and Information Security department and is comprised of a comprehensive set of technical strategies and procedures designed to minimize the impacts of technical interruption, and to facilitate the return to normal levels of operation and service delivery.

The Program is intended to govern disaster recovery to minimize the risk of, and provide confidence in, the recoverability of the Bank's systems, applications, and data; including, infrastructure and networks. Applications are housed within hardened internal data centers, with dedicated recovery solutions in place at a proprietary recovery site.

Frequency of Disaster Recovery Plan reviews and testing is commensurate with the Disaster Recovery Risk and are documented in confidential internal reports.

Regulatory Compliance

The Bank's EBCCM Program is designed to meet requirements of various regulatory, governmental, supervisory agencies, and industry standards including:

The Office of the Superintendent of Financial Institutions (OSFI), Autorité des marchés financiers (AMF), the Federal Financial Institutions Examination Council (FFIEC), the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), Financial Industry Regulatory Authority (FINRA), The Financial Conduct Authority, Prudential Regulation Authority, Netherlands, Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS). TD's EBCCM Program also aligns with international standards such as the ISO22301

Conclusion

The Bank's Business Continuity Plans, Incident Management Protocols, and Disaster Recovery Plans are documented, exercised and tested, of which, the results[1] are subject to regular independent audit. The Business Continuity and Disaster Recovery Programs apply the Three Lines of Defence model to Risk Management.

The Bank does not obtain a periodic SSAE18 audit; however, pursuant to Section 404 of the Sarbanes-Oxley Act, our independent auditors have audited the effectiveness of the Bank's internal controls over financial reporting, results of which are publicly available as part of the Bank's consolidated financial statements.

Our intent is to exercise commercially prudent and reasonable efforts to assure business continuity for the Bank and its customers; however, no representation or warranty is made or implied that certain events will not affect the Bank's systems. This document is intended as a guide to the Bank's EBCCM/DR Program and nothing in this document modifies, amends, supplements or supersedes, in any way, any agreement, warranty or representation with respect to the Bank's products or services; including availability of such products or services. The Bank reserves the right to change the procedures and disciplines described in this document without notice, as it deems appropriate.

[1] Please note that the Bank's internal and vendor assessments are not available for public review.