Enterprise Business Continuity and Crisis/Incident Management

External Statement

Published: July 2022

Business Continuity and Crisis/Incident Management Program

Business Continuity and Crisis/Incident Management is a vital and integral part of the TD Bank Group's ("the Bank") normal business operations. The Bank's Business Continuity and Crisis/Incident Management Program follows internal policies and is designed to meet industry regulations. It includes the establishment of Enterprise-wide Business Continuity and Crisis/Incident Management processes that provide safeguards designed 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 Business Continuity and Crisis/Incident Management 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, Crisis/Incident Management, and Disaster Recovery Plans to address the loss or failure of any component on which critical processes depend.

The Bank's Business Continuity and Crisis/Incident Management Program combines business resumption planning, crisis/incident management, and planning for systems recovery that is appropriate for the nature and scope of the Bank's businesses and operations, considering its operational, geographical, and digital footprints. The Business Continuity and Crisis/Incident Management Program is governed by Board-approved Policies that are managed by the Bank's Operational Risk Management and Office of the Chief Information Security Officer groups and aligns with business continuity and crisis management regulatory guidelines and industry standards.

Business Continuity Planning

All business and oversight functions are responsible for implementing Enterprise Business Continuity and Crisis/Incident Management 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 for that business or oversight function. A business or oversight function's 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. A business or oversight function's Business Continuity Plans address the ability for that function to recover from adverse business disruptions caused by a loss of key technology (including cyber events), loss of facility, loss of one or more third-party service providers, and loss of an employee's ability to work (including pandemic scenarios, civil unrest, and other natural disasters). The Business Continuity Plans are supported by appropriate arrangements whether provided internally or outsourced. Our Business Continuity Plans are reviewed by business management and the Bank's Enterprise Business Continuity and Crisis Management group according to defined Bank Business Continuity and Crisis Management Standards (the "Standards") to verify the adequacy, reasonableness, quality, and compliance to those Standards.

Exercising and Testing of Business Continuity Plans

All business and oversight functions must exercise and test 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 Enterprise Business Continuity and Crisis Management group according to defined Bank Standards and Plan criticality level. Exercises and tests are required to verify that arrangements meet required continuity and recovery objectives. Criteria for exercise and test success are based on pre-established objectives to meet minimum Business Continuity Exercise Standards. Key lessons learned and action items resulting from the exercise and test are applied to plan and recovery strategies to drive continuous improvement.

Third-Party Oversight

All businesses and oversight functions must have appropriate strategies and workarounds in place to respond to prolonged service interruptions of Enterprise critical third-party service arrangements. The businesses oversee the Business Continuity Plans for alignment to Bank Standards.

Threat and Risk Assessment

Annually, the Bank conducts a review and assessment of potential resiliency risks, including support of operational and cyber scenario analysis and stress-testing activities. The assessment considers the Bank's exposure, including potential vulnerabilities to internal and external business disruption threats. The businesses and oversight functions are required to address the top threats and risks identified from the threat and risk assessment within their Business Continuity Plans.

Crisis/Incident Management (Protocols; Exercises and Tests)

The Bank maintains Enterprise- and business-level crisis and incident management protocols to establish the approach and process for responding effectively to events and/or threats that disrupt the Bank's business and operations. This includes defining crisis and incident management teams, their roles and responsibilities, decision making authority, escalation, communication procedures, and deployment of recovery protocols.

Annually, business segments and risk, governance and oversight functions conduct readiness exercises and tests of their crisis and incident management protocols to validate processes and procedures to manage and respond to crises or incidents that impact their business and operations. All business-level protocols and exercises and tests are independently reviewed and challenged by Operational Risk Management and Enterprise Business Continuity and Crisis/Incident Management.

Disaster Recovery Program

The Bank’s Disaster Recovery Program is managed from within the Office of the Chief Information Security Officer department in alignment to the Business Continuity and Crisis/Incident Management Policy, and is comprised of a comprehensive set of technical strategies and procedures designed to minimize the impacts of technical interruption, to support resilience, and to facilitate the return to normal levels of operation and service delivery.

The Program governs 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 data centers, with dedicated recovery solutions in place at proprietary recovery sites.

Disaster Recovery Plans are reviewed and tested on a frequency 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, Crisis/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.

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

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 Business Continuity and Crisis Management or Disaster Recovery Programs 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.