

May 2017

Dear Client,

Deutsche Bank (DB) recognizes that significant business disruptions are a possibility. We have in place comprehensive business continuity procedures designed to minimize the impact of any significant business disruption. This letter summarizes the measures DB has taken through our global Business Continuity Management Program to respond to significant business disruptions.

Deutsche Bank's Business Continuity Management Program

Deutsche Bank is committed to protecting its staff and ensuring the continuity of critical Group businesses and functions in order to protect the Deutsche Bank franchise, mitigate risk, safeguard client services and sustain both stable financial markets and customer confidence.

Deutsche

Bank has developed, implemented and continues to test and maintain its global Business

Continuity Management (BCM) program to ensure it attains these objectives.

The BCM Program outlines core procedures for the relocation or the recovery of operations in

response to varying levels of disruption. A number of scenarios are considered including; staff

unavailability, complete loss of a single production site, loss of vendor services and loss of

application software. These procedures provide information for responsible DB personnel to

evaluate the business disruption and initiate appropriate action, including:

- Safeguard employees' and DB property,
- Communicate between DB and our employees, regulators, and clients,
- Provide you, our client with access to your funds and securities, and
- Protect DB books and records and recover/resume normal operations.

Each of our core businesses functions and infrastructure groups construct and maintain their

business continuity plans (BCPs) to ensure a continuous, reliable service.

BCPs are based on

predefined strategies, roles and responsibilities. BCPs are designed to ensure provision of the

critical business processes and IT systems within predefined recovery time frames. BCPs are

reviewed, updated and tested annually or when significant changes occur.

In support of our BCM Program, DB maintains technical disaster recovery plans to protect and

recover applications, information assets and technical infrastructure in the event of a facility failure

or technology outage. In addition and because of specific identified vulnerabilities,

contingency measures are undertaken in India, the Philippines and Tokyo against complete loss

of a city.

Roles & Responsibilities

The BCM Program has defined roles and responsibilities, which are documented in corporate

standards (including the Technical Disaster Recovery Standard).

This fosters a constant and

effective approach to the provision of resiliency throughout DB and results in an efficient fit-for-purpose

business continuity capability. The BCM Program is staffed and managed within each

region by specialists who co-ordinate preparedness efforts with BCM-trained staff embedded in

each business and infrastructure area. The Regional business continuity teams provide expertise

and guidance to all business functions within DB in developing, implementing, testing and

maintaining effective BCPs and recovery processes.

Standards are implemented regionally by Group Technology.

Similarly, the Technical Disaster Recovery

The DB Management Board has delegated responsibility for Business Process Disruption Risk to

the Global Head of IRRM (Information & Resilience Risk Management).

The DB Management Board and Executive Directors of legally autonomous entities retain overall

responsibility for policy setting, supervision and effective implementation of the BC Policy.

Chairman of the Supervisory Board: Paul Achleitner.

Management Board: John Cryan (Chairman), Marcus Schenck, Christian Sewing, Kimberly Hammonds, Stuart Lewis, Sylvie Matherat, Nicolas Moreau, Garth Ritchie, Karl von Rohr, Werner Steinmüller.

Deutsche Bank Aktiengesellschaft domiciled in Frankfurt am Main;

Local Court of Frankfurt am Main, HRB No 30 000; VAT ID No DE114103379;

www.db.com

further

Compliance with DB's corporate standards is monitored regionally by Regional Business

Continuity Council reporting on a quarterly basis through the Global Business Continuity Council.

Crisis Management & Implementation

DB's Information & Resilience Risk Management division ensures that DB has a clearly defined,

documented and tested crisis management process for assessing, escalating and managing any

business disruption that may affect DB's ability to continue its critical business operations. This

includes a crisis contact and escalation process which is tested on a regular basis. In addition,

DB's BCPs are designed to be implemented in response to varying levels of business disruptions.

The nature of the business disruption will affect whether all or only parts of our plans are

executed.

Business Continuity Recovery Solutions

DB has a broad recovery program in place to deal with the impact of incident or crisis. The Bank

has a number of customized recovery solutions designed to facilitate the quickest possible

resumption of work for the critical businesses and support functions.

Examples of these are:

- Alternate Sites

DB has self-managed, dedicated standby facilities. These recovery sites provide

dedicated recovery seats and infrastructure to provide for the needs of the business.

Additionally, DB retains recovery sites contractually through service providers who

concentrate on business resiliency. All recovery sites are physically separated from

normal business locations to prevent both sites being affected by the same incident.

- Reciprocal Agreements

Some businesses have partnership agreements with other business units regarding

the allocation of a required number of recovery seats or the ability to transfer work.

The receiving business unit provides the necessary infrastructure, hardware facilities

or staff.

Both normal business locations are geographically separated from each other to prevent both sites being affected by the same incident.

- Displacement Strategy

Certain business processes can be switched from one location to another and in the

longer term key staff can move to another location unaffected by the incident.

- Remote Access

Staff may work remotely, where permitted, in the event of a disruption accessing DB systems via VPN and can divert their telephones to a home or mobile number. Service Providers

Service Providers are contractually obliged to have business continuity capabilities in place to ensure continuity of services provided to DB if the ordinary operation of the Service Provider is disrupted and to modify their work stream in order to adapt with the business continuity organization of Deutsche Bank. A very robust and thorough vendor risk management process is in place to ensure compliance.

Pandemic Planning

DB maintains a risk-based approach to pandemic planning, using as a guide the World Health Organization (WHO) definitions of pandemic phases.

Customer Access to Funds and Securities

If your usual access to funds and securities is impacted by a significant business disruption, we will advise you of the appropriate DB contacts through expedient means at www.db.com.

Audit

DB's BCM Program is subject to regular reviews by internal and external audit, and regulatory authorities.

Regulatory Obligations

In the case of conflict between the Business Continuity Policies and Standards or the Technical

Disaster Recovery Standards and local regulatory obligations, the stricter obligation is adhered to.

Sincerely yours,

Information & Resilience Risk Management

Deutsche Bank

Please note that this information is subject to modification.