EUROBANK S.A.
8, Othonos Str., GR 105 57 Athens
GCR: 154558160000
Tel.: (+30) 210 333 7000
eurobank.gr

July 2024

Eurobank S.A. - Business Continuity Statement

Eurobank S.A. has long recognized that a wide variety of disruptive events or unforeseen circumstances can cause significant disruptions to its business operations.

The Bank is committed in mitigating this risk of business disruption in order to preserve its reputation, safeguard revenues, serve its clients and sustain both a stable financial market and customer confidence.

Therefore, the Bank has adopted a solid Business Continuity Management System (BCMS) in order not only to provide effective response to a wide variety of disruptive events(earthquakes, pandemics, natural and weather events, destruction of the Bank's infrastructure, cyber-attacks, socio-economic crises, etc.) but also to minimize their impact on the Bank's smooth and proper operation. More specifically, the BCMS is based on predefined strategies and risk assessment methodologies, is designed to identify risks, assess their impact and safeguard the continuation of critical business processes & systems.
Eurobank's S.A. BCMS has been formed under the requirements of the Central Bank of Greece at national level and is also certified with the international standards ISO 22301:2012 by TUV Hellas since 2013.

Key elements of Eurobank BCMS are:

A. Risk Assessment
The identification of threats and risk levels is accomplished, through a Risk Assessment Methodology.

B. BC Plan development
The critical business operations are identified through a Business Impact Analysis and the minimum resources required to continue critical services are defined. The identified resources are not limited to human resources & IT, but also include the identification of critical information of flows of, within and outside the Bank & critical physical and electronic documents.

C. Business Continuity Recovery Solutions
Once the BC Plan has been developed, the appropriate Business Continuity recovery method is selected. The main options are:

- **Alternative Sites**
  In the event of a BC incident, Business units have plans that include relocation to, self-managed, dedicated standby facility. This recovery site is physically separated from the primary site to prevent both from being affected by the same incident. Moreover, an IT alternative site exists, that provides the necessary infrastructure and critical systems on a hot standby basis.

- **Remote Access**

Staff has the ability to work remotely even from home in a secure manner and use all systems and tools necessary to support daily work tasks. This type of recovery solution is suited for the continuation of paperless critical business functions, while ensuring at the same time that operations performed off-premises are qualified with a system of internal controls equivalent to that running when these are performed on premise.

D. BCMS Maintenance

All BCMS components (regulatory documents, BC plans etc) are reviewed, updated and tested at regular intervals, as well as after significant changes to existing operations and/or capabilities.

E. BCMS Teams

Roles are assigned across all organizational levels, from Top Management to Business Unit level. Indicatively,

BCMS Teams at Top Management level are:

- Reviewing BCMS performance annually
- Deciding on improving coverage
  Handling BCP crisis

BCMS Custodian is the BCP Management Team that:

Designs, maintains, reviews and updates the management framework of the BCMS, while at the same time acting as a control mechanism of the correctness and completeness of the Bank's Business Continuity Plans.

On the other hand, BCP Teams on Business Unit level are:

- Performing risk assessment & identifying critical business processes
- Developing, testing & updating BC plans
- Activating BC Plans, in case of disruption etc.

F. Third Party Services

In compliance with the 178/5/2.10.2020 Executive Decision by BoG, all Critical Service Providers are contractually obliged to have Business Continuity plans in place to safeguard the proper performance of the services, if the ordinary operation of the Service Provider is disrupted. The appropriateness of their BCP is reviewed and approved by the Bank.

G. Audit

BCMS is subject to:

- an annual audit by TUV Hellas
- adhoc internal audit by the competent unit of the Bank
- adhoc audit by the Central Bank of Greece (BCG)
- adhoc audit by the European Central Bank (ECB)

More details on the BCMS cannot be provided in this notice, as the Bank keeps them confidential, in order to safeguard their effectiveness & security.

Eleftheria Papadopoulou	Ioannis Tzanos
Group Organization & Business Analysis	Group Corporate Security Officer