

NomoRisk Sample Business Continuity Plan (BCP) for Financial Institutions

as of: February 2011

The following table of contents provides an example of a business continuity plan for a financial institution. Information provided in the BCP relating to specific departments should be given to this department only, while sections marked with "(to ALL)" should be distributed to all staff.

Timelines suggested are subject to change as per the details established in the Business Impact Analysis.

- 1 Overview of the Business Continuity Plan and Definitions (to ALL)
 - 1.1 Definitions
 - 1.2 Maintenance of the BCP
 - 1.3 Overview of the BCP Objectives
 - 1.4 Abbreviations

- 2 Roles, Responsibilities and Authorities (to ALL)
 - 2.1 The Business Continuity Management Team
 - 2.1.1 The Emergency Response Team
 - 2.1.2 The Damage Assessment Team
 - 2.2 The Business Continuity Officer
 - 2.3 The Business Continuity Co-Ordinators in departments / branches
 - 2.4 The HR Continuity Officer
 - 2.5 The Public Relationship and Communication Officer
 - 2.6 The Security Officer
 - 2.7 The Fire wardens and first aiders

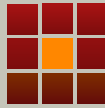
- 3 Business Recovery (to ALL)
 - 3.1 Detection, Escalation and Response of Emergencies
 - 3.1.1 Evacuation rules
 - 3.1.2 The firm's assembly points
 - 3.1.3 Accounting for any missing staff
 - 3.1.4 Protection of data and assets
 - 3.1.5 Evaluation of and first communication about the extent of the Damage
 - 3.2 Activation of the Business Continuity Plan
 - 3.2.1 Activation of the designated back-up site(s)
 - 3.2.2 Activation of the workaround processes



- 4 Procedures during Emergencies
 - 4.1 Basic disruption scenarios (to ALL)
 - 4.1.1 Procedures during electric power failure
 - 4.1.1.1 Public utility power outage
 - 4.1.1.2 Failure of an electrical component within the firm
 - 4.1.1.3 Emergency backup and protection for computer systems
 - 4.1.2 Procedures during Fire Alarm
 - 4.1.4 Procedures for Bomb Threats
 - 4.1.5 Procedures for earthquakes
 - 4.1.6 Procedures for robberies
 - 4.1.6.1 While the robbers are inside the bank
 - 4.1.6.2 After the robbery
 - 4.1.6.3 Burglaries
 - 4.1.6.5 Hostages and kidnapping
 - 4.2 Specific recovery procedures for branches
 - 4.2.1 Recovery procedures for branches a, b, c (large branches)
 - 4.2.2 Recovery procedures for branches d, e (medium branches)
 - 4.2.3 Recovery procedures for branches x, y, z (small branches)
 - 4.3 Specific recovery procedures for departments
 - 4.3.1 HR department recovery procedures
 - 4.3.1.1 Staff re-organisation during business disruption
 - 4.3.1.2 HR Recovery site
 - 4.3.1.3 Specific activities in case of business disruption
 - 4.3.1.4 Business disruption exceeding 24 hours
 - 4.3.1.5 Business disruption exceeding 1 month
 - 4.3.1.6 Switch back to normal business processes
 - 4.3.1.7 HR Call Tree and staff communication
 - 4.3.2 IT department recovery procedures
 - 4.3.2.1 General Provisions
 - 4.3.2.1.1 IT Assembly point
 - 4.3.2.1.2 IT recovery site(s)
 - 4.3.2.1.3 Special roles and covers at time of disruption
 - 4.3.2.1.4 IT Call Tree and staff communication
 - 4.3.2.2 IT recovery procedures for branches
 - 4.3.2.3 IT recovery procedures for the head office / contingency site
 - 4.3.2.4 User Workstations



- 4.3.2.5 File Services
- 4.3.2.6 Mail Servers
- 4.3.2.7 Applications
- 4.3.2.8 Telecommunications Equipment Recovery
- 4.3.2.9 Print Services
- 4.3.2.10 Other Networking and Communication Infrastructure
- 4.3.2.11 Helpdesk service recovery
- 4.3.3 Business department recovery procedures (one section for each department!)
 - 4.3.1.1 Staff re-organisation during business disruption
 - 4.3.1.2 Department recovery site
 - 4.3.1.3 Specific activities in case of business disruption
 - 4.3.1.4 Business disruption exceeding 24 hours
 - 4.3.1.5 Business disruption exceeding 1 month
 - 4.3.1.6 Switch back to normal business processes
 - 4.3.1.7 Department Call Tree and staff communication
- 5 Communication during Disasters
 - 5.1 External Communication
 - 5.1.1 Regulator(s)
 - 5.1.2 Shareholders
 - 5.1.3 Clients
 - 5.1.4 Business partners (vendors, service providers)
 - 5.2 Internal Communication (to ALL)
 - 5.2.1 Company Staff
 - 5.2.2 Supervisory Board Members
 - 5.2.3 Mother or Holding company
 - 5.3 The end of the business disruption (to ALL)
- 6 Testing the Plan
 - 6.1 Test Cycles
 - 6.2 Test methods
 - 6.3 Test results and updates to the Plan



- 7 Distribution of the BCP (to ALL)
- 7.1 Delivery of documents to all staff
- 7.2 Business Continuity Training

Annexes

Annex I – Company Call Tree

Annex II – Emergency Response Checklist (to ALL)

Annex III – General External Contacts

Annex IV - Earthquake Attachment

Annex V – Departmental and Branch Business Continuity Coordinators



Annex II – Emergency Response Checklist (ALL)

This checklist should be printed and distributed to all staff, who should have it at hand at all times.

Disaster during the day

1. If necessary, security services to invoke emergency signal of site affected
2. If necessary, start evacuation of all people from site and gathering at assembly site. Fire wardens and Emergency Response Team / Business Continuity Coordinators to ensure all people are evacuated as necessary.
3. Inform Company Management or, if they are unavailable, Emergency Response Team / Business Continuity Management Team and Business Continuity Officer (phone numbers: 123456, ...)
4. Emergency Response Team / Business Continuity Management Team and Business Continuity Officer to gather and assess the situation
5. Analyse the situation in detail
 - a) verify reason for evacuation
 - b) find out expected duration of business disruption
 - c) assess damage to the firm (Damage Assessment Team)
 - d) assess availability of services and resources (Damage Assessment Team)
6. Report on unaccounted staff to HR (phone number of HR continuity officer: 12345)
7. Company Management or, in absence of them, Emergency Response Team / Business Continuity Management Team to decide where staff should go to (back into building, assembly site, contingency site, home, other)
8. Department heads, Branch Managers together with Business Continuity Coordinators to check for necessary end of day processes and how to execute
9. Set up conference call facility for coordination of further steps (Business Continuity Management Team members, Business Continuity Officer and all affected Business Continuity Coordinators to participate)

System outage during the day

1. Whoever detects the system outage needs to inform the Business Continuity Officer and the IT dept.
2. IT dept. and Business Continuity Officer to assess the situation to identify which services will be unavailable for how long
3. Continue with 7 above

Disaster during out of office hours

1. Whoever detects the disaster needs to inform Company Management or ERT/BCMT and the Business Continuity Officer (phone numbers: 123456, ...)
2. Company Management or Emergency Response Team / Business Continuity Management Team and Business Continuity Officer to gather and assess the situation
3. Analyse the situation in detail
 - a) find out if building is available still
 - b) find out expected duration of business disruption
 - c) assess damage to the bank (Damage Assessment Team)
 - d) assess availability of services and resources (Damage Assessment Team)
4. Invoke emergency call tree to inform all staff
5. Report on any unaccounted staff to HR (phone number of HR responsible: 12345)
6. Company Management or Emergency Response Team / Business Continuity Management Team and Business Continuity Officer to decide where staff should go to (normal building, contingency site, stay home, other)
7. Use call tree to inform all staff about changes in work time and -place
8. Department heads, Branch Managers together with Business Continuity Coordinators to check for necessary start of day processes and how to execute
9. Set up conference call facility for coordination of further steps (Business Continuity Management Team members, Business Continuity Officer and all affected Business Continuity Coordinators to participate)