

Pershing LLC's Contingency Planning

Introducing Broker-Dealer Executive Summary

November 2008

This Pershing LLC Contingency Planning Executive Summary is confidential and proprietary to Pershing LLC and may not be duplicated, shared or otherwise disclosed to third parties or used for any purpose not expressly authorized, in writing, by Pershing LLC.

Pershing®

AN AFFILIATE OF THE BANK OF NEW YORK MELLON

Table of Contents

<i>Purpose</i>	3
<i>Goal</i>	3
<i>Basic Assumptions</i>	3
<i>Incident Management Structure</i>	4
Incident Management Team	4
Response Teams.....	6
Business Units.....	6
Line Managers.....	6
Business Continuity Team Captains.....	6
IMT Liaison.....	6
<i>Communications With Customers</i>	6
Outbound Communications	6
Inbound Communications	6
<i>Security Policies</i>	7
Data Security	7
Physical Security Access	7
<i>Business Continuity (People and Processes)</i>	7
Business Continuity Plans and Risk Assessments.....	7
Geographically Dispersed Processing.....	7
Recovery Sites	8
Testing	8
<i>Disaster Recovery (Technology)</i>	8
Overview	8
Sites	8
Systems	8
Plans and Testing	9

Purpose

The purpose of this document is to provide Pershing's customers with an overview of its business continuity and disaster recovery plans, including a high-level definition of the policies and procedures that will be employed in the event of a business interruption. Please note that this document may be amended by Pershing, in its sole discretion, as material changes are made to Pershing's infrastructure, operations, and contingency plans.

Goal

Pershing's goal is to deliver continuous, reliable service to its customers while maintaining regulatory compliance.

Basic Assumptions

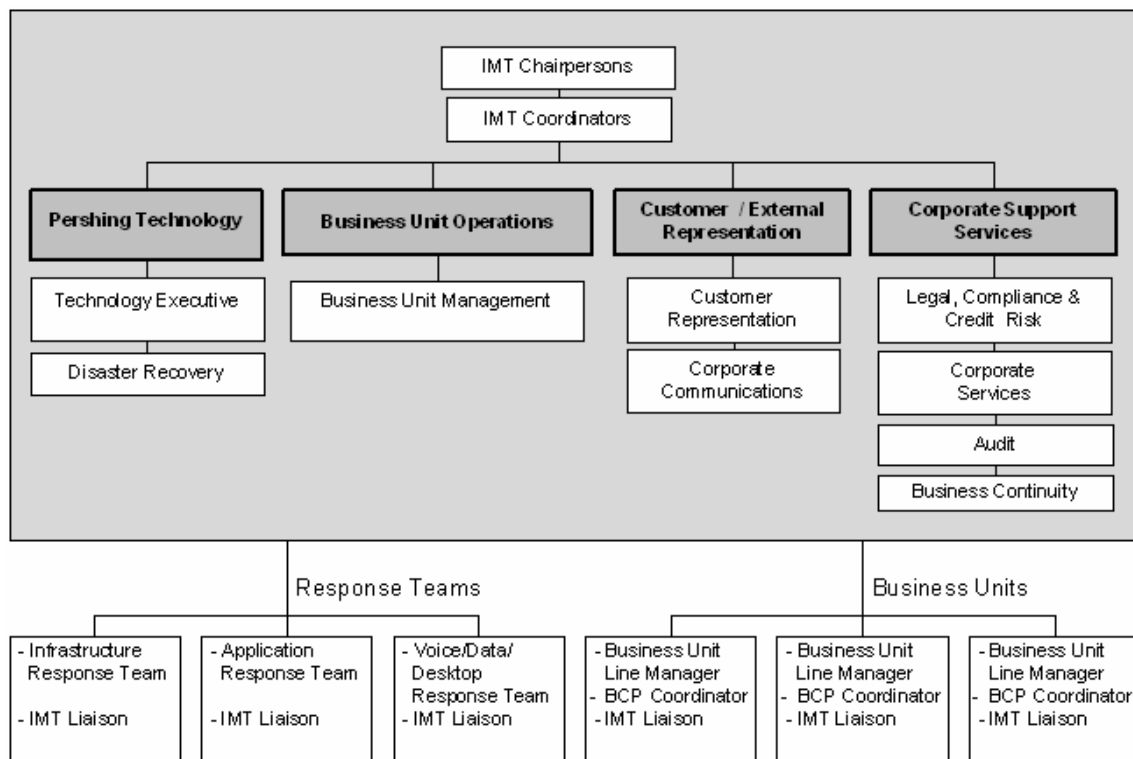
The business continuity plan is based on the following assumptions:

1. Based on the redundancy and geographical dispersion of Pershing's facilities, Pershing assumes that no more than one of its critical facilities will be affected at one time and that alternate facilities will remain accessible and operational.
2. Based on Pershing's efforts to safeguard its facilities (for instance, Pershing's maintenance of redundant generators, chillers, etc.), Pershing assumes that its critical infrastructure (including electricity, water, heat, ventilation, air conditioning, etc.) will remain operational as long as the facility is accessible.
3. If an incident causes the evacuation of one of Pershing's New Jersey-based operations centers, Pershing will declare a business continuity event and activate its business continuity plan and facilities.
 - a. Pershing has reserved a four-hour recovery window to allow for the comprehensive switching of all related regional fax and voice communications to the alternate, in-region business continuity location; and to allow for the transiting of critical staff to the relocation site.
 - b. While in-region critical staff is relocating, out-of-region processing facilities and capacities will continue to provide uninterrupted service wherever possible.
4. If an incident causes the closing of the primary data center, Pershing will declare a disaster recovery event and activate its disaster recovery plan. This may result in an outage up to four hours, while our mainframe processing is transferred to the alternate data center.
5. Pershing assumes that the customer's primary or alternate facilities and supporting critical infrastructure (such as electricity, water, heat, ventilation, air conditioning, etc.) are accessible and operational.
6. Pershing assumes critical industry utilities and counter-parties (such as the Depository Trust & Clearing Corporation [DTCC], Security Industry Automation Corp. [SIAC], etc.) are operational.
7. Pershing assumes that it will have adequate staffing available during the event.
8. Pershing assumes that customer-supplied data communication lines between its primary and alternate data centers are redundant.

Incident Management Structure

Pershing's incident management response structure includes a multi-disciplined team, scripted processes, and a series of workflows developed from testing, planning, and historic response scenarios. The Incident Management Team (IMT) will be activated during any business continuity or disaster recovery event and will manage operations through recovery to business as usual (BAU).

The accompanying diagram illustrates Pershing's Incident Management Team composition.



Incident Management Team

IMT members and their alternates are key subject-matter experts whose extensive experience at Pershing allows them to understand the requirements of specific business units, while maintaining a corporate-wide, customer-focused perspective. Their responsibilities include the following:

- Obtaining the operational statuses of departments or the customer groups they represent
- Assessing incidents to determine a “right-size” response, which may include activating either the business continuity or disaster recovery plan
- Coordinating with essential business personnel, for instance managers and Business Continuity Planning (BCP) coordinators
- Ensuring the response is implemented correctly
- Ensuring departments comply with the requests of the IMT in a timely manner

- Providing timely and accurate status and recovery information to Customer Relationship Managers and Corporate Communications
- Managing the incident and recovery activities through closure
- Document post-event analyses and findings

IMT Chairperson (Leadership)

Senior Manager – focal point for IMT decision-making and the execution of strategies

- Acts as a liaison with the Executive Committee
- Coordinates activities at the corporate, business, and technology unit levels

IMT Coordinator (Incident Facilitation)

- Coordinates the flow of information to the IMT, structures meetings, documents event, etc.

Technology Management (Infrastructure)

- Ensures technology environments are thoroughly assessed and information is presented to IMT in a timely manner
- Establishes priorities and coordinates the allocation of Pershing's technology resources - third party technical vendors and service providers
- Ensures that IMT directives are implemented
- Acts as a liaison with third-party technical vendors and service providers

Business Unit Management (Line Management)

- Ensures that appropriate information is collected about the incident and determines the status of the business unit's operational readiness
- Assesses operational and credit risk environments to assist in determining contingency actions
- Makes decisions on contingency actions and drives implementations

Customer and External Representation (Customer Relationship Management)

- Represents the customer's interest in the decision-making process
- Ensures that communications, messages, or both, from Pershing's management and the IMT are delivered promptly and accurately
- Manages outbound communications and inbound requests for information

Corporate Support Services (Operations and Oversight)

- Provides information on impact of the incident
- Supports and facilitates the firm's contingency actions
- Ensures contingency actions undertaken are compliant with laws, rules, and regulations, and provides sufficient controls
- Acts as a liaison with industry and regulatory agencies
- Manages Pershing employee notifications

Response Teams

The Pershing Technology Group has dedicated teams of technologists to advise on and respond to events, as directed by the IMT. These teams are organized by area of expertise and relevant skill sets.

Business Units

Each of Pershing's business units has dedicated teams of associates to perform the specific recovery and resumption functions identified in their business continuity plans.

Line Managers

The Line Managers are responsible for activating their business continuity plans, as instructed by the Incident Commander.

Business Continuity Team Captains

The Business Continuity Team Captains and alternates have developed the business continuity plans and managed test scenarios. Their primary responsibility during an incident is to provide their subject-matter expertise to the Line Managers.

IMT Liaison

The IMT Liaison is responsible for communicating the statuses of the business units to the IMT and providing the Line Managers with current IMT decisions.

Communications With Customers

Outbound Communications

Pershing Account Managers, Relationship Managers, and the Customer Service Group will contact customers with information or instructions via email.

Inbound Communications

It is expected that customers will continue to use existing communication channels with Pershing.

- General status questions will be answered by Relationship Managers
- Customers who wish to notify Pershing of technology problems will continue to call Pershing's Technology Customer Service at (201) 413-2001

Security Policies

Data Security

Disaster recovery access to Pershing's systems during a disaster remains consistent with normal production access. This is achieved by using mirrored or replicated images of the security rules and systems.

Physical Security Access

If there is a security system failure at Pershing's facilities, the following guidelines will be implemented:

- Only Pershing associates and authorized vendor support personnel will be allowed access to the facility and all access will be monitored. All associates will be required to show a valid Pershing identification card and sign in with Lobby Security each time they enter the facility.
- Access to restricted areas (such as the data center) will only be authorized after the requestor of access has been verified by Security, and only if all designated approvals from accompanying department directors, senior managers, or both, are in place.
- Security will maintain an up-to-date database of all approved associates with programmed card access rights and a sign-in authorization listing for privileged access to these restricted areas.
- Any access required by associates, vendors, or consultants will require approval by their immediate department's director, senior management, or both, of the restricted areas involved.
- Vendors that must be on site in order to perform any required maintenance or repairs will be accompanied by a Pershing associate at all times while onsite.

Business Continuity (People and Processes)

Business continuity at Pershing is defined as the orderly return to normal business operations after an unplanned business interruption. Integral to the success of Pershing's business continuity program is our investment in geographically dispersed, redundant processing centers, as well as the ability to relocate associates and resume business functions at Pershing's alternate business continuity facilities.

Business Continuity Plans and Risk Assessments

Consistent with Financial Industry Regulatory Authority (FINRATM) rules (NYSE[®] Rule 446 and NASD[®] Rule 3510/20) Pershing maintains formal BC plans that detail the business continuity strategies and processes for each business unit. These plans are updated annually or whenever there is a material change to the business, or its operations or infrastructure. Additionally, Pershing's internal due diligence and policies require formal annual reviews, including business risk assessments for all business continuity plans.

Current copies of Pershing's Business Continuity Plans are maintained within each business unit, on the internal network, in IMT command centers, and in secure offsite locations.

Geographically Dispersed Processing

Pershing operates multiple redundant processing centers. Primary capacities are delivered from multiple locations in New Jersey. Additionally, Pershing has developed out-of-region capacities in both our California and central Florida locations. Critical processing is divided across these locations in an effort to minimize a business interruption in the event of an incident affecting one of the facilities or geographies.

Recovery Sites

Pershing maintains three business continuity sites for critical staff located in its primary facility. Combined, these facilities accommodate the relocation of over 1,000 trading, processing, and data center associates.

Each operations desktop or trading position is outfitted with all required application software, requisite network access, and telecommunication equipment.

The internal telephone systems have been designed to allow calls to be rerouted to Pershing's alternate business continuity facilities, out-of-region locations, or both.

Centralized fax and wire printer rooms are maintained in these locations, and are tested regularly.

Testing

Workstations in the business continuity sites are tested at least twice a year.

One annual test engages approximately 700 processing associates and 250 traders at the in-region, alternate business continuity facility. Employees log on to the business continuity desktops and phones and test all requisite functionalities.

A second annual test involves performing the area's inclusive daily work from the alternate business continuity facility.

Disaster Recovery (Technology)

Overview

Disaster recovery is defined at Pershing as the orderly return to normal technology operations at an alternate site, at the direction of Pershing's senior management, after an unplanned technology interruption at the primary site. The process includes the recovery of the technology infrastructure and the technology personnel responsible for supporting it.

Sites

Our approach begins with disaster avoidance by housing production and recovery systems within geographically dispersed internal Pershing data centers. The disaster recovery site in the Northeastern U.S. region (New Jersey) is located approximately 800 miles from the production data center located in the mid-southern United States (Tennessee). The data center is available immediately at time of disaster (ATOD) to support the initiation of recovery efforts. These centers are state-of-the-art, hardened facilities with capabilities such as separate power grids, dual power feeds from redundant substations, generator backup, secure facility access, etc. Pershing can operate indefinitely in its recovery site.

Systems

System and application backup is supported via various replication processes based on the underlying technology used in production. Methods employed include active-active/load-balanced systems, asynchronous disk-mirroring infrastructure, and database replication technology between the data centers.

The recovery process is disk/direct access storage device (DASD)-based and does not require restoration from tape. A complement of redundant virtual tape subsystems (VTS) and native automated tape libraries (ATLs) exists in both the primary and alternate sites in support of local and remote tape backups.

As a result, it is our objective that our systems can be restarted and operational in less than four hours (recovery time objective or “RTO”), with less than five minutes of data loss, (recovery point objective or “RPO”).

Linking our customers to their data is equally important, so we build internal redundancy into our network design, as well. Our North American geographically dispersed data centers are designed to support the network in the event of a disaster at either location.

Plans and Testing

Pershing’s disaster recovery plans and testing program fully comply with NYSE Rule 446 and NASD Rules 3510 and 3520.

The disaster recovery team is responsible for the creation, maintenance, and testing of all disaster recovery plans. Testing is a formal full-cycle process that encompasses scheduled quarterly tests, ad-hoc testing, and external exercises that addresses business, technology, audit, and compliance requirements. Tests are internal, customer-facing or industry-facing (or both) in scope, and include participation from internal users, our customers, and utilities or exchanges (or both). The focus of these tests is to re-create the flow of information to and from the recovery systems to the end users as seamlessly as possible.

After each test, a written assessment is prepared documenting any problem that is encountered during the test or areas where improvement may be necessary. Action plans are developed and implemented to remediate any issue that is identified. Pershing customers are invited and encouraged to participate in these important exercises.