Prudential is committed to providing uninterrupted service to our customers, protecting the assets they have entrusted with us and safeguarding our associates and resources.

Overview

The programs and plans we have put in place ensure the continuity of business and that we are there when our customers and business partners need us.
In support of our state of readiness, our Preparedness Strategy includes five areas:

1. Emergency Response
2. Event Threat Management
3. Business Continuation
4. Disaster Recovery
5. Health Emergency Preparedness

These areas have been built on programs, policies, standards, plans and training. We continually maintain and exercise our programs and plans according to the policies and standards. We have established objectives, metrics and reporting to provide a concise status of our readiness.

Our programs and plans leverage our diversity in personnel, locations and businesses as well as our global presence and robust/resilient infrastructure. These attributes ensure that we are prepared to address events of different sizes and scope that may threaten to disrupt business operations.

Emergency Response

Emergency Response to events is managed locally by a team consisting of local leadership, HR, facilities, and security personnel. Their role is to respond to the event in their location and minimizing impact to personnel/guests, assets and buildings. Their primary focus is safety and minimizing impact - Think of our facilities and security personnel as our internal “first responders.”

In responding to emergencies, the facilities, and security personnel adhere to their established protocols and procedures. As part of their response, they will interact with the public sector first responders (police, fire and medical).

Event Threat Management

Our Event Threat Management Program includes the monitoring, response, communication, escalation, and coordination responses required to effectively manage any event that may impact our services, associates, or resources. Our escalation process and response protocols assist us in handling any situation whether it requires our businesses continuation plans to be activated, is classified as a crisis or only requires monitoring. The following are six important elements within the Prudential Global Security Event Threat Management Program:

1. Early warning mechanisms to identify signs and triggers of events that may escalate into an incident.
2. Analysis and assessment of events to provide both tracking and trend reporting capabilities for domestic and international operations within Prudential.
3. Escalation and communication procedures to ensure that appropriate and consistent actions are taken.
4. Physical and virtual command centers to provide coordinated management of the event.
5. Event Threat Management Plans to address and document contacts and responsibilities, as well as our response, communication, escalation activities.
6. Trained teams including the Enterprise Event Threat Management Team and Local Event Threat Management Teams in both US and non-US locations.

Whenever possible and appropriate, we utilize industry accepted tools and processes. We complement these tools and processes with internally developed systems to provide reliable solutions for preparedness. For example, we utilize an emergency notification system to readily communicate with our associates via various communication devices.

We partner with public sector entities and private sector partners for situational awareness and best practices. Our Event Threat Management Program has focused on preparing for events ranging from active shooter and missing employees to civil unrest and severe weather. The Enterprise Event Threat Management Team receives information, makes decisions, and coordinates activity across the company when a significant event occurs that could impact employees, facilities, operations, interests, brand, or financials.

Business Continuation

Our commitment to providing continued service and safeguarding our customers and shareholders' interests means that we must ensure that we are prepared to continue critical business functions in the event of disruptions and outages of various types and scopes. This commitment and responsibility, down to the employee level, is documented in our standards and reinforced in our Enterprise Business Continuation Program. Where the Event Threat Management Program focuses on response and management of events which may impact our operations, Business Continuation (BC) planning is a critical preparedness component to ensure our operations can continue and recover within predefined timeframes. Planning and exercising minimize impacts to the organization, the stakeholder, the consumer, legal ramifications, and employees.

At Prudential, Business Continuation is a living program that changes based on the organizational goals and evolving threat landscape. The Business Continuation Operations and technology Disaster Recovery (DR) components are updated on an ongoing basis, taking into consideration the integration of industry best practices, technology advancements, dependencies, criticality, and business requirements. Business Continuation is the core of our Company's readiness state, and we have a solid foundation in place as illustrated by the following attributes:

- A centralized function, Enterprise Business Continuation Management (EBCM) is accountable for developing and managing the Company's Business Continuation Program and monitoring its effectiveness.
- EBCM maintains standard operating procedures for BC planning and testing and ensures they are communicated globally.
- EBCM establishes and monitors metrics for BC planning deliverables, BC planning quality and completion of testing, and exercising.
- Each business and corporate function has a BC Officer accountable for implementing the BC standards within their organization.
- Each BC Officer delivers an annual report to senior management and reviews their organization's program at the applicable business or corporate function Risk Committee.
- BC standards define required skills and training for BC Officers and BC Planners.
- Risk and control self-assessments are completed for the BC program of each business and corporate function.
- The BC Officers Council meets bi-monthly to discuss risks, issues, and program improvement areas.
- The BC Governance Council, which is comprised of senior leaders from each business and corporate function, meets quarterly to discuss BC operational risks, program initiatives and program changes.
- The Company's BC Program is subject to oversight by the Enterprise Risk Management Council, Executive Risk Committee, and the Audit Committee of the Board.

Multiple BC Planners within each business and corporate function develop BC plans leveraging a standard process, which includes six steps.

1. Identify business processes and dependencies.
2. Perform a Business Impact Analysis.
3. Validate dependency recovery objectives.
4. Analyze business impact scenarios and develop recovery solutions.
5. Develop and maintain BC plans.
6. Test BC plans and solutions.

Important elements of the BC Planning process include:

- Conducting a Business Impact Analysis (BIA) to identify people, processes, and technologies necessary for response, recovery, and resumption efforts.
- Processes labeled with recovery time objectives (RTO) based on factors that determine the level of criticality, and alignment to supporting dependencies.

- Mission-critical supporting dependencies such as applications are reviewed and tested annually.
- Each business impact analysis and BC plan are approved by the applicable Department Head annually.
- Business and corporate function BC Officers oversee BC planning for their organizations.
- BC Officers conduct annual quality reviews of BC plans.
- Gaps between the recovery objectives of business processes and their dependencies are identified and addressed.
- BC plans are tested and exercised according to established frequencies.
- Communication tools, plans, procedures, and call lists are reviewed and tested regularly to ensure appropriate levels of internal/external communications will take place during, and after major events.
- Employees receive annual awareness training on their BC plans.
- There are a number of scenarios that are planned and tested with different strategies depending on location and criticality of the process. Listed below are the primary scenarios:
    - Unavailability or loss of people.
    - Unavailability of dependent internal business processes.
    - Unavailability of dependent internally hosted technology services.
    - Unavailability or inaccessibility of primary work area and regional events.
    - Unavailability of required third parties.

Disaster Recovery

Our Technology promotes a secure, efficient, and controlled data-processing environment across the enterprise. Prudential's Technology Organization manages robust data processing operations, keeping our technology operations safe and secure. Key highlights include:

- Tier 3 highly secure data centers deliver an extremely resilient environment for business-critical applications and data. Multiple layers of electrical power, cooling, and network paths each designed with a least N+1 redundancy.
- Prudential has state-of-the-art, round-the-clock Operations and Cyber Security Operations Centers that provide 24x7 intrusion detection, incident management, problem management, and centralized operations monitoring processes.
- Prudential technology operations employ the latest technology and processes for back-up/recovery and leverage multiple data centers and Cloud solutions providing recovery capabilities for distributed environments, (i.e., storage, database, and other components), mainframe, and network infrastructure.
- All critical Prudential data is replicated/imaged between data centers and backed-up daily.
- Prudential utilizes multiple call centers and remote access capabilities to allow Global business recovery.
- Prudential conducts infrastructure disaster recovery tests on a regular basis, including several major data center tests in the U.S. annually.

- Our Technology Enterprise Resiliency Governance BC Officer provides technology disaster recovery planning, coordination, and support globally. The Technology BC Officer serves as the liaison between Enterprise Business Continuation Management and Prudential's technology/infrastructure product and services teams.
- The Global Technology Organization manages the Enterprise IT infrastructure and Data Centers supporting business continuation and disaster recovery for Prudential's various lines of business.

Prudential's Information Security Office ensures that Prudential's information is kept safe and secure. Highlights of the Information Security program include:

- Enhanced controls to stay a step ahead of emerging threats including State-of-the-Art data protection and monitoring tools with 24x7 incident response capability.
- Ongoing virus and malware protection and email filtering.
- Robust vulnerability management and response readiness.
- Recurring network-level and application-level penetration testing.
- Ongoing phishing and awareness campaign with social engineering focus and recurring testing and real time user "coaching".
- User and event analytics program to proactively detect and address anomalous patterns potentially indicative of risk.
- Continual growth in correlation and intelligence capability to quickly defend against targeted malware.
- Detailed code review workflow within application development process to identify & remediate potential vulnerabilities during code development as well as routine scans of production code.
- The Information Security Office has focus on ransomware and Distributed Denial of Service accounts.
- Tabletop exercises around cyberthreats, and other technology security protocols are held with the technology and business leaders as well as annual testing of defensive controls to continue to raise awareness across the company.

Health Emergency Preparedness

Prudential's preparedness in the event a reduced workforce also addresses various health emergency scenarios. In 2005, Prudential formed a Pandemic Preparedness Planning Team that has matured into an Enterprise Health Emergency Team. This group has developed a comprehensive plan that addresses the needs of both our domestic and international businesses. This comprehensive plan has enabled us to analyze, train and test to address potential health threats including COVID-19, a new severe strain of the influenza virus, biological events, or chemical hazards. The following are key elements of the plan:

- Monitoring of health concerns around the globe and early warning mechanisms.
- Response protocols based on severity levels and phases.
- Screening tools, social distancing procedures and cleaning/sanitizing protocols to limit exposure and spread.

- A web-based health tool to assist associates with health-related questions and provide information to help them prepare in the event of a health emergency.
- Prudential's 24-hour Facilities Status extranet site and Facilities Status Hotline, which provides continuous updates to employees regarding Company information or building closures.
- Utilization of Event Threat Management and Business Continuation programs and personnel to respond to a health emergency.
- Prudential's Employee Assistance Program offers several support resources for employees and their family members during times of crisis.

For more information on Prudential Financial Preparedness Strategy and individual programs, contact-

Prudential's Enterprise Business Continuation Management:
email Enterprise.BCM@prudential.com
OR
Prudential Global Security Command Center (staffed 24x7):
973-802-6675/email GSCC@prudential.com