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 seven areas:

1. Emergency Response
2. Event Threat Management
3. Business Continuation
4. Critical Business Services
5. Disaster Recovery
6. Health Emergency Preparedness
7. Third Party Risk Management

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 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 minimize 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 of actions 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 focuses 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 we must ensure we are prepared to continue critical business operations in the event of disruptions/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 test exercises minimize impacts to the organization, stakeholders, consumers, and employees while reducing risks associated with legal ramifications, and employees.

At Prudential, Business Continuation is a living program and is updated based on changes within our organizational goals and evolving threat landscape. The Business Continuation Program, Business Service Framework 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 at 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.
- Each business and corporate function has a BC Officer accountable for implementing the BC standards within their organization.
- 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.

Each business and corporate function develops BC plans leveraging a standard process documented within the Prudential BC Standards. The process includes identifying business processes, documenting dependencies, determining criticality, planning recovery strategies and testing.

A variety of scenarios are planned and tested using different strategies based on the location and the criticality of the process. The main scenarios include:

- Unavailability or Loss of People
- Unavailability of Dependent Internal Business Processes
- Unavailability or Inaccessibility of Primary Work Area
- Unavailability of Technology
- Unavailability of Required Third Party

Critical Business Services

Prudential's Business Services Framework (BSF) is designed to broaden preparedness and focus on the ability to deliver critical services throughout complex and large-scale disruptions. Business services are products or services that Prudential provides to external end users, clients, or market participants. Critical Business Services (CBS) are those services that could cause intolerable harm to consumers or market participants; harm market integrity; threaten

policyholder protection; impair safety and soundness; or threaten the financial stability of the Company if they were be disrupted.

This program actively engages Business Leaders and BC Officers/Planners to identify business services and their criticality based on operational impacts (reputational/ legal/regulatory and financial), map critical dependencies to the CBS, plan for large but plausible events and perform annual end-to-end testing to ensure the resiliency of the CBS.

Disaster Recovery

Our Technology organization is committed to promoting a secure, efficient, and controlled data-processing environment across the enterprise. By actively managing robust data processing operations, we ensure that our technology and information assets are continuously monitored and protected. Our Security Services and Information Security Offices implement comprehensive measures to safeguard against cyber threats and unauthorized access, ensuring the integrity and reliability of our operations. These controls support the strategic goals of the enterprise. 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 at least N+1 redundancy.
- Prudential has Operations and Cyber Security Operations Centers that provide 24x7 intrusion detection, incident management, problem management, and centralized operations monitoring processes.
- All critical Prudential data is replicated/imaged between data centers and backed-up daily. A vault exists to protect production data from catastrophic cyber/ransomware events.
- Prudential technology operations employ the latest technology and processes for back-up/restoration and leverage multiple data centers and Cloud solutions providing restoration capabilities for distributed environments, (i.e., storage, database, and other components), mainframe, and network infrastructure.
- Prudential utilizes multiple call centers and robust remote access capabilities to allow Global business recovery.
- Prudential regularly conducts infrastructure disaster recovery tests, including multiple major annual data center tests.
- Our BC Officer oversees technology disaster recovery planning, coordination, and support globally. The BC Officer acts as the liaison between Enterprise Business Continuation Management, Prudential businesses and Prudential's technology, infrastructure and data product and services teams.

Health Emergency Preparedness

Prudential's preparedness in the event a reduced workforce also addresses various health emergency scenarios. A comprehensive plan that addresses the needs of both our domestic and international businesses has been developed to ensure the health of our employees and continue

business operations. This comprehensive plan has enabled us to analyze, plan, train and test procedures that address potential health threats including COVID-19, biological events, or chemical hazards.

Third Party Risk Management

Prudential maintains a robust third-party risk management program. Critical third party services are continuously assessed to ensure compliance with our business continuity, disaster recovery, and information security programs. The BC program requires recovery solutions should a critical third party be unavailable as well as exit plans for the termination of a third party. Businesses who outsource functions are responsible for reviewing third party BC plans, and having recovery solutions/procedures in place to ensure the continued viability of said function.

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