Prudential is unwavering in our dedication to delivering continuous service to our customers, rigorously safeguarding the assets entrusted to us, and ensuring the utmost protection of our associates and resources—even in the face of any disruption.

Purpose

Prudential's Preparedness Strategy is designed to provide confidence that we can continue delivering critical services through a wide range of disruptive events. This overview describes, at a high level, how Prudential approaches resiliency across the enterprise and demonstrates that our preparedness is risk-based, executable, tested, and reviewed annually.

Our Preparedness Strategy

Our strategy integrates critical business services, emergency response, operational resiliency and threat specific preparedness into a coordinated framework focused on protecting our customers, our people, and the services they rely on.

Prudential's preparedness strategy is anchored in a single objective: the continued delivery of Critical Business Services during disruptions. To achieve this, we employ an enterprise-wide approach that:

- Is risk-based, informed by internal and external threat assessments
- Is enterprise-governed, with oversight from senior management and the Board
- Focuses on end-to-end resiliency, across people, processes, technology, facilities, and third parties
- Is tested regularly through exercises and real-world events
- Is reviewed and updated annually to reflect changes in the business and threat landscape

Our preparedness capabilities are organized into an integrated framework that connects response, recovery, and continuity activities, rather than operating as standalone programs.

Operational Resilience Framework

Operational Resilience is the ability to anticipate, prevent, withstand, respond to, recover from, and adapt to operational disruptions that could impact the delivery of Prudential's Critical Business Services. Prudential's Operational Resilience program covers the full lifecycle of service delivery and integrates capabilities that ensure we can continue to operate during and after a disruptive event. This includes:

- Sustaining operations during and after a disruption
- Ensuring availability and timely recovery of critical technology services
- Preventing, detecting, and recovering from cyber incidents
- Managing risks and dependencies across our vendor and partner ecosystem
- Identifying emerging threats and reducing risks to operational stability

These efforts are organized across eight core capability areas:

- Critical Business Services
- Emergency Response
- Event Threat Management and Crisis Management
- Business Continuation
- Technology Disaster Recovery
- Third-Party Risk Management
- Health Emergency Preparedness
- Governance, Testing, and Continuous Improvement

Together, these capabilities ensure Prudential can respond to events, manage crises, and sustain operations during both localized incidents and large-scale disruptions.

Critical Business Services

At the center of Prudential's preparedness strategy is our ability to continue delivering Critical Business Services (CBS). Business services are the products and services Prudential provides to customers, clients, and market participants. Critical Business Services are those whose disruption could result in intolerable harm to consumers, threaten policyholder protection, impair market integrity, or impact the safety and soundness of the Company.

Prudential's Business Services Framework provides end-to-end visibility into these services by identifying critical dependencies across people, processes, facilities, technology, and third parties. Business leaders and business continuation professionals work together to:

- Identify and classify business services based on impact
- Map critical dependencies supporting those services
- Plan for large but plausible disruption scenarios

This approach ensures preparedness is aligned to customer outcomes rather than isolated functions.

Emergency Response

Emergency Response is managed locally and focuses on the immediate protection of people, facilities, and assets. Local leadership, facilities, security, and people management representatives coordinate on-site response actions and work closely with public sector first responders such as police, fire, and emergency medical services.

This capability is designed to address immediate life-safety and site-level impacts, serving as the first layer of Prudential's overall response to an event.

Event Threat Management and Crisis Management

Prudential's Event Threat Management program provides enterprise-level monitoring, assessment, escalation, and coordination of events that may impact on our associates, facilities, operations, brand, or financial position. Key elements include:

- Early warning and monitoring capabilities
- Analysis and assessment of domestic and international events

- Defined escalation and communication protocols
- Enterprise and local response teams
- Physical and virtual command centers to coordinate response activities

When events meet predefined thresholds, enterprise Crisis Management structures are activated. Crisis Management provides senior-level coordination and decision-making to manage enterprise impacts, align communications, and ensure consistent response across the Company.

This integrated approach allows Prudential to manage events ranging from localized disruptions to large-scale crises in a structured and coordinated manner.

Business Continuation

Prudential's Business Continuation (BC) program is designed to ensure that operations (personnel, processes, applications, and third-party services) can either continue functioning or be restored within established timeframes after any disruption.

The program is built on documented standards and a consistent planning methodology applied across businesses and corporate functions. Key characteristics of the program include:

- Identification of processes and dependencies
    - Process and dependency Recovery Time Objectives and Recovery Point Capabilities are set through formal governance, aligned to or exceeding regulatory expectations, and are regularly tested and reviewed
- Development of recovery strategies aligned to impact
- Regular testing of plans across a range of disruption scenarios
- Annual Business Executive review and approval

Business Continuation planning complements event and crisis management by focusing on sustained operational recovery, helping minimize impacts to customers, stakeholders, and employees.

Technology Disaster Recovery

Prudential's Technology organization supports preparedness by maintaining resilient and secure technology environments that enable the recovery of critical systems and data. This includes:

- 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
- Operations and Cyber Security Operations Centers that provide 24x7 intrusion detection, incident management, problem management, and centralized operations monitoring processes
- Data replication, backup, and recovery capabilities
- Multiple call centers and robust remote access capabilities to allow Global business recovery
- Use of multiple geographically dispersed data centers and cloud solutions
- Regular disaster recovery testing, including major annual exercises

Technology Disaster Recovery capabilities are aligned to the needs of Critical Business Services, ensuring systems that support customer-facing services can be restored in a timely manner following technology disruptions.

Third Party Risk Management

Prudential maintains a robust Third-Party Risk Management program to address dependencies on external service providers. Critical third-party services are assessed for alignment with Prudential's business continuity, disaster recovery, and information security requirements. Key elements include:

- Ongoing assessment of critical third-party resiliency
- Required recovery strategies if a third party becomes unavailable
- Exit and contingency planning for critical outsourced services

This approach ensures third-party dependencies are incorporated into Prudential's overall preparedness and recovery planning.

Health Emergency Preparedness

Prudential maintains preparedness for health-related disruption scenarios, including pandemics, biological events, and chemical hazards. Health emergency preparedness is integrated into our broader resiliency framework and leverages existing business continuation, workforce, and technology strategies. Planning, training, and testing activities are conducted to ensure Prudential can protect employee health while continuing critical operations during health emergencies affecting workforce availability.

Governance, Testing, and Continuous Improvement

Prudential's preparedness programs are supported by established governance, metrics, and reporting. Programs are reviewed regularly, tested through exercises and real-world events, and updated to reflect evolving risks, business changes, and regulatory expectations. This governance structure ensures Prudential's preparedness strategy remains effective, transparent, and aligned to customer and enterprise needs.

Although no company's Prepareness Plan can fully eliminate the possibility of business interruption or temporary access limitations, this plan is structured to reasonably reduce these risks and ensure the prompt restoration of critical business services.

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