ADT Business Continuity (BC) / Disaster Recovery (DR) Plan

February 2023

Table of Contents

1. Purpose

This document provides an overview of ADT's business continuity program (BCP) which is designed to protect and restore operations and ensure the availability of critical services following an interruption to, or failure of, critical business processes and systems. ADT's Business Continuity Management Office (BCMO) maintains a single framework of best practices, tools and standard methodology for planning, implementing and reporting on all aspects of business continuity management based on company requirements and industry standards (i.e., ISO22301).

The BCMO is responsible to provide guidance and direction towards a comprehensive all-hazards program to ensure an optimized response, recovery, and resumption effort for any unplanned event that disrupts normal business operations.

The purpose of this document is to describe how ADT's BCM program supports the organizations' resilience. It outlines at a high level how ADT protects its customers, employees, assets and locations by developing, implementing, and exercising BC plans and recovery processes which assure the delivery of consistent, reliable, and responsive services. This BC overview, along with other ADT policies, procedures, processes, and documentation maintained by the BCMO, create a comprehensive set of tools available to respond to a disaster event.

2. ADT BC Standards Overview

2.1 Business Continuity Management

The key aim of ADT's BC Program is to proactively assist in preventing, where possible, events which disrupt the organization's critical services. Subsequently, ADT's BCMP provides a framework for identifying and prioritizing the organization's services, minimizing the risk of exposure to internal and external threats, and ensuring procedures are in place to facilitate effective response to multiple threat types that can impact the business including but not limited to natural disasters, cyber-attacks, data breaches, and pandemics.

Secondarily, but equally important, the program is designed to minimize the potential impact of any unavoidable disruption by containing it to a predictable and pre-determined acceptable period of time, and to have tested procedures in place to respond and recover from events.

Business Continuity Management preparedness include the following areas:

- Vulnerability, Risk & Business Impact Analysis (BIA)
- Disaster Recovery/IT/RTO-RPO
- Mitigation Strategy Planning (BCP)
- Company Incident Response Tiers
- Crisis Management and Incident Response with established Teams and Roles (CMP)
- Testing and Exercising
- ISO 22301 Business Continuity Management Program Standards (Compliance)

2.2 BIA Approach

The Business Impact Analysis (BIA) is a critical aspect of business continuity. The BIA is developed as part of the contingency planning process for ADT and encompasses the analysis of the criticality of the process and associated dependencies, and any associated vulnerabilities and risks. Specific steps include:

- **Determine mission/business processes and services, and recovery criticality:** Mission critical business processes and services are identified, and supporting systems are identified along with the impact of a disruption. Outage impacts and estimated downtime are considered as part of the assessment. The downtime reflects the maximum that the business can tolerate while still maintaining an acceptable pre-defined level of service.
- **Identify resource requirements:** To craft realistic recovery efforts, a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible is made and documented. Examples of resources include facilities, personnel, equipment, software, data files, system components, and vital records.
- **Identify recovery priorities for system resources:** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels are established for sequencing recovery activities and resources.
- **Establish Disaster Recovery Tier classification:** With Criticality and Maximum Tolerable Outage requirements collected from Business Teams, the information is provided to to the EOC Availability Management Team. The following is the BC/DR Tier Categorization and the associated RTO and RPO:

Disaster Recovery Tier Classification	MTO (Maximum Tolerable Outage Objective)	RTO (Recovery Time Objective)	RPO (Data Recovery Point Objective)
Life Safety	Service(s) Restored within – 2 Hours or Less	Continuously Available	Less than15 minutes
Mission Critical	Service(s) Restored within – 1 Day or Less	Up to 1 day	15 minutes to 1 day
Business Critical	Service(s) Restored within – 1-3 Days	1-3 days	Greater than 1 day
Business	Service(s) Restored within – 4 or More Days	7+ days	Greater than 1 day

Table 1 - Recovery Tiers

2.3 BCP Recovery Strategies Overview

As part of the all-hazards planning approach, ADT's BCP recovery strategies and procedures are based on the information gathered during the BIA assessment. Leveraging the details of the process and associated dependencies as well as the accompanying recovery criticality and timeframes, a realistic recovery plan is designed that is independent of event type. Generally, ADT's BCPs take into consideration the following key loss scenarios depending on the nature of the process/services and environment:

- **Loss of Facilities:** This scenario assumes physical destruction and/or inaccessibility of the facilities. Examples include structural damage due to earthquake, flood, fire, etc., inaccessibility due to nearby chemical spill, bomb scare, gas leak, power outage, etc. Business recovery

strategies and activities are invoked to support the loss of availability or access to a facility or work area.

- **Loss of Personnel:** This scenario assumes impact to personnel's availability to perform work. Examples include personnel and/or their families impacted due to an earthquake, civil unrest, epidemic, etc. Business recovery strategies and activities are invoked to support a reduction of personnel available for work.
- **Loss of Vendor Services:** This scenario assumes unavailability of a key vendor. Examples include loss of vendor dependencies due to various scenarios impacting the vendor. Business recovery strategies and activities are invoked to support a loss of availability or access to vendor provided services.
- **Loss of Technology:** This scenario assumes physical destruction and/or inoperability of critical systems. Examples include data center damage, partial or full network/system failure, email inaccessibility, etc. Business recovery strategies and activities are invoked to support the loss of availability or access to internal applications and network services.

2.4 Disaster Recovery Management

ADT recognizes and acknowledges that reinstating the critical systems/applications is a major responsibility to safeguard the interests of its employees, shareholders, and communities that it services.

Disaster Recovery (DR) is an area of resiliency planning that is established to protect the organization from the effects of significant technology disruptions. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster. The DR process includes planning and testing and may involve a separate physical site for restoring operations. ADT's DR plan includes the following areas:

- Proactive & Reactive Response Plans
- Business & Customer Resumption Planning
- Unified Objectives & Consolidated Action Plans
- DR Resource Management
- Integrated Communications
- Incident Management (real-time) Coordination & Status Reporting

3. Crisis Management and Incident Response Overview

Each ADT site is required to maintain a current incident response plan. The plan must be updated at least annually unless site changes dictate more frequent updates. The following diagram provides an overview of the Incident Management Team Structure that is consistently followed by all sites:

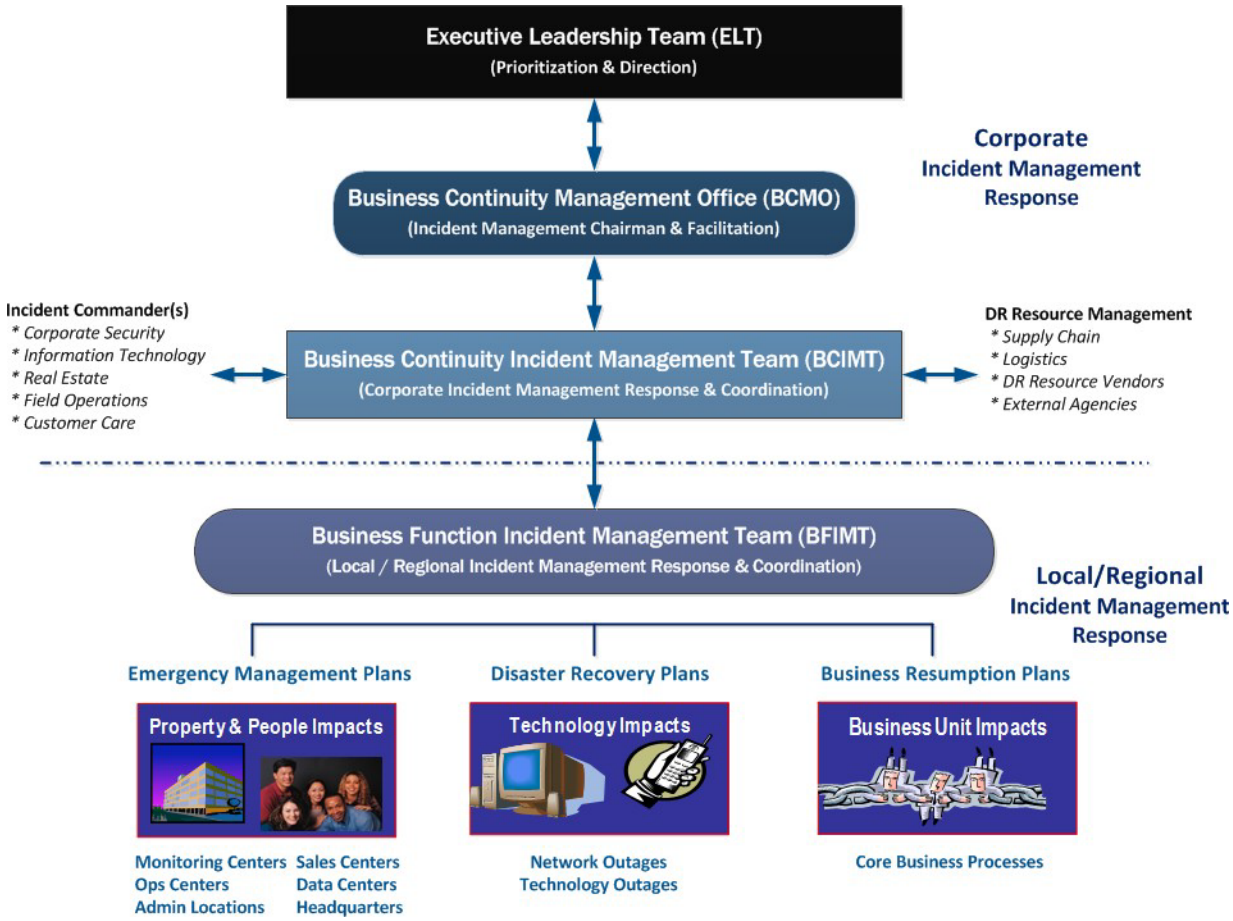

Figure 1 - Incident Management Team Structure

3.1 Incident Management Team Responsibility

The Incident Management Team is responsible for performing an assessment of the critical event utilizing the ***Site Assessment Checklist*** and providing guidance to the responsible Executive Leadership Team member concerning site vulnerability. This team consists of the following core members:

- Business Continuity Team Leader
- Site Leadership (RVP, Location Mgr.)
- Operations Field Leadership
- Human Resource Business Partner
- Region Mgr., Environment, Health, & Safety
- Deputy General Counsel, Labor & Employment
- Corporate Communications
- Facilities Manager / Landlord / Property Manager
- Corporate Security

3.2 Executive Leadership Team (ELT) Responsibilities

The ELT is responsible for reviewing the site assessment information provided by the Incident Management Team and making the final decision concerning how to operate the location during a critical event. The respective ELT member will consider the following key priorities in their decision:

- Employee safety
- Customer services and support
- Asset protection

3.3 Incident Management Team Roles and Responsibilities

IM Team	Incident Support Functions	IM Team	Incident Support Functions
BCM Office	Vulnerability monitoring Incident Management Facilitation Incident performance management & reporting	**Corporate Security**	Security Policies & Incident Plans Security Investigations Security Vendor Procurement External Agency Coordination
Legal	Legal Advisory Contract Review Stakeholder Communications	**HR**	Employee Compensation Employee Assistance & Benefits Employee Policies Employee Accountability
Corporate Communications	Employee Communication Social Media Communications External Crisis Communication	**Finance**	Incident Expenditures
IS/IT	Network/Application/System Availability	**Field Operations**	Incident Response & Coordination Incident Response Management Customer Service Calls Local Area Agency Coordination
Operations Support Center	System Support Customer Impacts (Small Business & Residential)	**IT Support Desk**	Desk Top Solution Connectivity Solution Access & Privileges
Sourcing	Vendor Management Resource Management Procurement	**Facility Management**	Site Facility Management Real Estate Management Resource & Vendor Management
Fleet Management	Fleet Management Fuel Management	**Risk Management**	Insurance Policy Management Deductibles Claims and Adjustments
EHS	Employee Incident Safety Plans Contamination and Spill Containment Safety Agency Coordination	**Customer Care/NRD/ Customer Experience**	Customer Support Customer Communication Customer Adjustments Customer Impacts
Marketing	Customer Retention Coordination & Response Competitive Intelligence Product Analysis and Pricing	**Sales**	Sales Support Sales Communication Sales Impacts

3.4 Communication Protocol

The objective of the communication plan is to define who will provide key communications during an incident, and the content, recipients, schedule, method of delivery, frequency, and priority of the communication. By outlining communications in advance, ADT will mitigate the effect of a crisis on employees, reduce the impact of bad publicity, maintain customer service, bolster relations with suppliers, and address the concerns of other key stakeholders. The below sections detail how ADT manages incident communication up, down and across the organization.

3.5 Incident Notification and Escalation

The BCPs detail the notification and escalation procedures including information about employee accounting, situation assessment, leadership notification, and other related procedures. Notification and escalation procedures address the following:

- **Account for employee safety.** Procedures followed for determining employee safety and well-being following an event and for determining associate availability to report to work.
- **Perform situation assessment.** Procedures to be followed for assessing the impact of the event and the resulting anticipated length of down time/disruption. Considerations include:
    - What is the current status?
    - How many locations have been affected?
    - Were there any injuries? If so, has Human Resources been notified?
    - Are emergency authorities on scene?
    - What current priorities and deadlines might be affected by the event?
    - Does the team have sufficient resources available to respond?
    - Could any legal liabilities result from this incident?
- **Notify leadership.** Procedures for communicating and escalating to the executive leadership team.
- **Notify key business partners.** Procedures for communicating to third parties that may be impacted by the event or that are critical in the response and recovery efforts.

3.6 ADT Emergency Alerting System

An emergency alerting system has been implemented across ADT. Automatic notifications are sent based on the employees' assigned office location. Geo-enabled notifications are also available if the employee installs the mobile app on their smartphone, In addition to severe weather alerts, notifications based on potential risk situations will be sent from the BCMO team and include alerts such as law enforcement events (i.e. crime scene, active shooter, terrorist, bomb threat, etc.), civil unrest (i.e. riots), technology power outage, local area power outage, Environmental Protection Agency, and infectious disease. Information regarding office closures and employee actions to take due to any of the above are included with the messaging.

3.7 Plan Activation

Not all responses to a disruption will necessarily or automatically translate into the formal declaration of a disaster. The Incident Management Team will determine and direct the appropriate level of response and recovery actions required for the unique situation. It is up to the plan owner to determine if a plan will be activated and it is their responsibility to notify the Incident Management Team of the activation, and to maintain recovery action communications with the team until the plan is deactivated.

3.8 Disaster Declaration Procedures

The declaration procedures include information about the decision support mechanism required to declare a disaster versus a less severe interruption that may or may not include plan activations. This assessment will include coordination with other impacted teams and related procedures as outlined below.

- **Identify the authority to activate plan(s) and declare disaster (for plans that rely on dedicated recovery space).** The plan identifies the primary and alternate individuals who have authority to activate the BCP, to declare the activation of the recovery site, and the specific procedures required for invoking the hot site.
- **Define the trigger points.** The plan defines the level or duration of service outage that constitutes a disaster or triggers the activation of the recovery plan, including time allotted for triage and critical deadlines pertinent to making an activation decision.
- **Notify the teams.** The plan details a process to notify teams impacted by the declaration. This could include the teams that will need to relocate, the teams that will transfer work, the teams that will receive/take on that work, the teams that are involved in the recovery/restoration efforts, and the teams that will need to coordinate with third parties, etc.
- **Define the types of declarations.** The plan defines the types of declarations that may be made at different levels and the hierarchy of declaration (i.e., where one team can supersede another team's decision to active or not activate their respective plans).

4. BC/DR Testing Overview

Exercising and testing the BC/DR Plans is vital to ensure the continuous effectiveness of recovery strategies in anticipated disaster situations. The ADT BCMO Program Policy provides the Framework Requirements (Program Minimum Requirements) for plan review and exercise type and timing.

At ADT, all business groups are responsible for testing and validating their key business function disaster recovery and incident plans. Orientation/education, tabletop, walk-through, functional, and full-scale exercises are typical testing and plan validation processes.

Within the DR testing schedule, "Mission Critical" plans must be tested and/or validated semi-annually and Business Critical" plans annually. To meet the annual testing requirements as set by the BCMO, an exercise or test may be scheduled following the annual program requirement, or a team may document an event as an exercise, also known as an unscheduled event. Thus, if a team experiences a disruptive event which occurs during the normal course of operations, the team will fully analyze and document the findings with the intent to improve the content of the plan and any associated recovery strategies. This analysis should take place within two weeks of the actual event.

ADT conducts several DR exercises per year, each focused on different families of applications supporting different areas of ADT's diverse business. ADT's most critical set of applications (Life Safety) that support underlying alarms and signals are excluded from these exercises as these applications are synchronized across multiple data centers and are regularly switched to run from one location to another. Additionally, because the data centers are geographically dispersed, it is unlikely that a single disaster incident would impact both locations. Backups of the data are performed regularly and are secured and stored in two different geographic locations.

After any exercise or test, a lesson learned/debrief is hosted and documented. The exercise type, plan test objectives, action items, as well as success and/or failure results are documented, tracked, and reported to the BCMO. Any changes to the plan are completed during plan maintenance or completed immediately if required.

5. Plan Maintenance

It is the responsibility of the Plan Owner to annually review and update the plan. However, if there are any organizational changes that impact the business continuity planning, a plan is modified to reflect the changes. On an annual basis, the plan will be fully reviewed and updated by the Plan Owner to determine if any strategy, reference, assignment, or contact information requires update or reconsideration.

Typical changes which could warrant immediate review of BC plan includes:

- Location openings and closures
- Location risk profile change
- Business process change
- Vendor/vendor service level changes
- Application system changes
- BIA refresh
- Personnel changes
- Organizational changes or realignment