Avaya Corporate Security & Business Continuity
Business Continuity Program Overview

AVAYA

CONTENTS

1. Introduction

At Avaya the Business Continuity Program (BCP) is a shared management process which objectives are to identify potential risks and business impacts that threaten an organization, and to provide a framework for building resilience into the business model, allowing an effective response that safeguards the interests of our stakeholders, reputation, brand, and value creating activities.

The Business Continuity Program interacts in close relationship with the Crisis Management & Incident Response Process, which addresses the coordination of the Company's initial response to a crisis or incident in an effective, timely manner, with the goal of avoiding harm to people, and minimizing damage to the organization's profitability, reputation, and ability to operate.

Together, the Business Continuity Program and the Crisis Management & Incident Response Process, in conjunction with other specialized processes like IT Disaster Recovery and customer facing organizations Business Continuity planning, define the structure and the tools that Avaya uses to ensure resiliency and ultimately overcome the potential or actual impact of crisis situation.

2. The Corporate Business Continuity Program Model at Avaya

Per the Avaya Business Continuity Program Policy requirements, the oversight and governance of the Business Continuity Program belongs to the Avaya Corporate Security & Business Continuity Organization, while the responsibility for developing, implementing, maintaining, testing, and executing the Program belongs to the functional areas with assistance from the Corporate Security & Business Continuity Team.

While the Avaya Business Continuity Program Policy establishes that all employees play a role in business continuity, it defines clear responsibilities in planning within the company structure, for example:

- **Executive Committee Members** are responsible for allocating resources and supporting BCP initiatives.
- **Senior Business Leaders** are responsible for supporting the implementation of strategies and plans, acting as the actual owners of their Business Group BCP Program.
- **Functional Leaders** are responsible for the Business Group Plan/s development, implementation, maintenance, testing and execution.
- **Business Continuity Coordinators**, designated by the business leaders, are responsible for coordinating the planning efforts for their business group or department.
- **Avaya Corporate Security & Business Continuity** is responsible for overseeing and managing the Business Continuity Program, and providing assistance to the Business Groups globally with their efforts in the planning arena and in response to a business interruption or incident. This Team also operates as an audit function to ensure compliance with their established policy and procedures, tracking and reporting on each Business Group's progress to executive leadership as required.

The Policy also establishes specific planning requirements the Business Groups must comply with:

- Business Continuity Plans must be documented using the Sales Force based tool FUSION Risk Management.
- Per the formatting structure defined in the tool, all Plans will include as a minimum:
    - **Organization Details** – Mission statement and general description of short and long term main Recovery Strategies.
    - **Business Impact Analysis (BIA)**, which includes:
        - Identification of business processes performed, including their criticality level and the impact of not being able to perform them.
        - Identification of locations in which the processes are performed and staffing levels needed based on process criticality.
        - Identification of organizational internal, external, and technological (application) dependencies.
        - Definition of Recovery Time Objectives (RTO) for each process.
        - Definition of specific process related Recovery Strategies.
    - **General Contingency Procedures** outlining the overall generic steps involved in the response, recovery, resumption and return phases, and in any other specifically applicable scenario.
    - **Organization's contact information** (Team Rosters).
- Business Continuity Plans must be reviewed, validated and approved recurrently at least once every 365 days while they must be tested in accordance to their Recovery Strategies within the same period.

3. The Avaya Resilience Structure

As mentioned in the introduction, the Business Continuity Program interacts with other processes in order to conform what we can define as the Avaya Resilience Structure, or the Avaya resilience capabilities.

The primary goal of this concept is to enable an organization to respond and survive a disaster or business interruption and continue business operations, observing the following objectives as some of its key aspects:

- Provide for the safety of associates and people on Avaya premises.
- Sustain uninterrupted service for our customers.
- Mitigate the risk and minimize the impact of damage and losses.
- Establish authority during an emergency situation.
- Ensure effective communication and coordination.
- Identify critical lines of business and supporting functions.
- Prioritize work efforts.
- Continue critical business operations.
- Minimize the duration of a disruption.
- Reduce the complexity of the recovery effort.
- Assist with incident management.

While all the areas of the company participate in the Business Continuity Program, the following are some of the processes interacting with it towards the accomplishment of the mentioned objectives in the customer facing front:

- Crisis Management & Incident Response.
- IT Disaster Recovery (ITDR).
- Avaya Global Support Services (GSS) Business Continuity.
- Avaya Private Cloud Services (APCS) Business Continuity.
- Customer Account Teams / Account Managers.

Crisis Management and Incident Response

While the Business Continuity Program addresses a crisis at a strategic level, the Crisis Management & Incident Response Process works more at a tactical level on the field.

This process is managed by Avaya Corporate Security and Business Continuity, and establishes Incident Management Plans (IMP) that drive the immediate response on a crisis situation impacting a specific location, area or region.

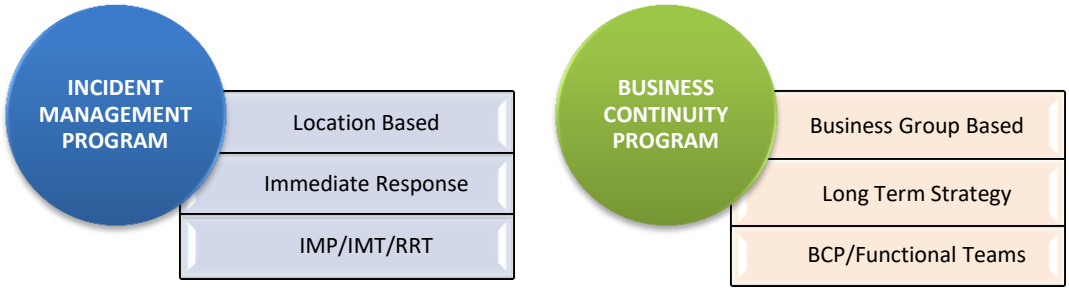
The Incident Management Plans establish basic response procedures for typical crisis scenarios that may result from natural, human-caused or utility related/technology hazards. In addition to these procedures, the IMPs outline the communication and escalation process that should be followed during the crisis response. Finally, these Plans contain important location information that goes from contact information to aspects tied to the location Risk Assessment.

To operate the IMPs, the Crisis Management & Incident Response Process establishes the designation of a Local Incident Manager that serves as initial responder and liaison with Avaya

Corporate Security & Business Continuity, and the definition of local and regional Incident Management Teams (IMT & RRT respectively). These teams include the core functions located in a particular location/region (e.g. Sales, Services, HR, Worldwide Law, Security, Facilities, etc.).

The final instance of the Crisis Management & Incident Response Process is the Executive Crisis Management Team (ECMT), which is formed by Avaya's Senior Leaders and it's activated in the event of a major business interruption impacting multiple Business Groups and/or locations.

The activation of an IMP and/or the actions of an IMT/RRT, or the ECMT, may serve as a trigger for the Business Groups to invoke their BCPs when necessary, generating a strategic relationship between both processes.



While the range of threats to operations, people and property can be infinite, both planning efforts are oriented to address integrated response and recovery efforts that are both effective and flexible and that can be used in a variety of scenarios, including:

Natural Hazards

- Geological (earthquake, tsunami, volcano, landslide, mudslide, etc.).
- Meteorological (severe weather conditions like hurricanes, snow/ice storms, heavy rain followed by flooding, tornadoes, extreme heat, etc.).
- Biological (pandemic and major contagious outbreaks).

Human-Caused Hazards

- Fire.
- Threats and Acts of Violence (threats to a person, threats to cause damage to property/workplace violence; bomb threats; suspicious mail/packages; active shooter, etc.).
- Demonstrations and Civil disturbances.
- Human-Caused Catastrophic Events (hazardous material spills or dispersals; transportation disasters; major explosions; terrorist attacks; etc.).
- Medical Emergencies.

Utility Related/Technological Hazards

- Power outages.
- Water supply outages.
- HVAC/Heating outages in low/high temperature areas.
- Network outages (caused by infrastructure failure or cyberattacks).

IT Disaster Recovery (ITDR)

The Avaya IT Disaster Recovery Program (ITDR) Model is a corporate-wide initiative. The Program supports Avaya Data Center locations with an initial focus on domestic operations.

IT collaborates with Avaya Corporate Security & Business Continuity, Sales, Services, Operations, and Information Technology Departments to provide technology recovery solutions.

Incidents, outages and interruptions to Avaya's Mission Critical applications managed by IT are within the scope of the ITDR Program Model.

IT Disaster Recovery strategy main objective is the recovery of Avaya's Mission Critical applications and infrastructure as soon as possible to minimize the impact to the business. This strategy involves the recovery of the mentioned applications to a Data Center which is geographically distant from Avaya's other major Data Centers, the local daily backup of Mission Critical servers, applications and databases, and the replication and mirroring of our most critical data to a remote location.

The ITDR strategy is executed through a conjunction of activities that include Business Impact Analysis and DR planning, development, and recurring testing and maintenance.

Avaya Global Support Services (GSS) Business Continuity

Avaya's Global Support Services (GSS) Organization has major support centers strategically located across North America, South America, Asia-Pacific, and Europe along with procedures to redirect resources, where needed, during business emergencies.

A number of Avaya solutions are integral to the GSS Business Continuity Plan. Capabilities leveraged within the Plan include Enterprise Survivable Switch (ESS), telco redirect, IP Telephony, Best Services Routing, Look-Ahead Interflow (LAI), and vector/VDN branching/variables. The plan also includes capabilities for the following:

- Global, multi-site support for 24x7 critical operations.
- Automatic failover from Avaya IP network to PSTN.
- Best-in-class call routing and toll-free service with multiple termination points.
- Remote agent & telecommuting capabilities.
- Recovery Time Objectives (RTO) commitment, which means services will continue as contracted unless prohibited by emergency services due to the health and safety of our employees.

Note: *During a business disruption, work is prioritized based on client impact and urgency, with the highest priority for service given to First Responders (organizations involved in public safety, national defense, and/or health care). Additionally, GSS partners with our clients to determine the best options for restoration of service based on contractual Service Level Agreements (SLAs), maintenance agreements, business impact, and emergency services status.*

The GSS Business Continuity strategy includes the following activities, in adherence with Avaya Corporate Security & Business Continuity Policy:

- Business Impact Analysis.
- Planning.
- Development.
- Testing (ongoing).
- Maintenance (ongoing).

Avaya Private Cloud Services (APCS) Business Continuity

Avaya's Managed Services are based on Information Technology Infrastructure Library (ITIL®) and are delivered utilizing a global 24/7 "follow the sun" model.

APCS's delivery model incorporates a global organization with a global platform, global support groups, and global management. Work is prioritized within the platform based on impact and urgency the client faces. APCS support engineers are virtually one team but are physically located around the globe. APCS has support sites spread out in Asia Pacific, Europe, South America, and North America.

APCS support locations have been chosen to be away from shorelines and outside of known earthquake zones to attempt to avoid known natural hazards. Resources are managed directly within the support organization and if warranted, overtime, and/or additional coverage would be arranged based on the situation and under the direction of the Service Delivery Director. Other work may be deferred/transferred to other team members around the globe as applicable. Example: If a site was inaccessible, engineers may work remotely and/or work would be handled by the engineers in our other support centers.

APCS Clients may reach support via customer portal* or live phone call.

APCS uses a number of Avaya telephony solutions to ensure 24/7 coverage availability to our clients including:

- Multiple termination points for primary toll-free service to enable Avaya to swing a toll-free number from a primary point to another point.
- Look Ahead Interflow (LAI) is used when the Automatic Call Distribution (ACD) is receiving calls but agents are unable to login / receive calls enabling look ahead usage of the secondary ACD.
- Remote agent capabilities (where allowed by law).
- Ability for agents to log into a different Automatic Call Distribution system (ACD) to receive calls if primary ACD is unreachable.

APCS also utilizes tools for re-routing toll free numbers to provide alternate ACD coverage during outages of facilities or telephony services. If the ACD is not reachable by clients, the toll-free number and the agents may be redirected to a secondary ACD.

Note: *Although Avaya does its best to ensure availability, there may be short timeframes where client calls may not be processed due to an outage. In this situation, APCS Clients may contact their Service Delivery Manager to address the issue at hand or utilize the on line APCS Managed Services Portal*.*

Note on Language Support: *If regional CFT is not available, the CFT management team will reach out to the external language support vendor as needed.*

(*) Login required.

Customer Account Teams / Account Managers

As a general rule, Account Managers and Field Technicians will reach out to customers directly to determine the potential or actual impact of a crisis situation, and the needs resulting from it. Client Service Managers, Field Support Managers, and Territory Service Managers have discretion and authority to proactively contact their clients and business partners as appropriate.

Note: *During a regional disaster where multiple customers are impacted, Avaya will continue to strive to meet service-level agreements and contractual obligations. Each situation and customer is unique, and our strategy must be flexible in order to meet the specific needs of our customers.*

4. Customer Planning and Preparedness

As an Avaya Customer, you will not be alone when crisis hits. We will continue to strive to meet service-level agreements and contractual obligations, and will do our best to provide you with best in class assistance.

It is important to prepare in advance for a crisis situation; the following aspects will help you to interact with Avaya if that moment comes:

- **Avaya Account Information**
  - Have your active customer number available to provide to Avaya Support.
  - Know who your service point of contact is and how to reach him/her.
- **Know your inventory**
  - Keep a detailed inventory of all your locations. A detailed inventory is a complete, up-to-date and accurate record of every single network element including special features on each of those elements, circuits, data, etc. organized by its physical location.
- **Prepare to provide to Avaya:**
  - An accurate description of service impact, environmental conditions, and essential information for assessment of disaster situation.
  - Technical and Management primes to work with Avaya staff.
  - Recommendations to what the primary and secondary recovery strategies should be addressed.
  - Network Engineering primes and resources to implement alternative network configurations until restoration methods are implemented or the crisis scenario has passed.
  - Any other useful aspect according to your own Business Continuity Program/Plan.

Note: *During a regional disaster where multiple customers are impacted, Avaya will continue to strive to meet service-level agreements and contractual obligations. Each situation and customer is unique, and our strategy must be flexible in order to meet the specific needs of our customers.*

APPENDIX A – Avaya Business Continuity Policy

Avaya Security Policy

Policy 11.0 Requirements for Business Continuity Planning/Program

Purpose

Business Continuity is a shared management process that identifies potential risks and business impacts that threaten an organization and provides a framework for building resilience into the business model, which allows for an effective response that safeguards the interests of Avaya's stakeholders, reputation, brand, and value creating activities.

Policy

Oversight and governance of the Business Continuity Program (BCP) belongs to the Avaya Corporate Security & Business Continuity Team.

Responsibility for developing, implementing, maintaining, testing, and executing the program belongs to the functional areas with assistance from the Corporate Security & Business Continuity Team. Funding and Coordination Staff assignment is the sole responsibility of the Business Groups.

Roles and Responsibilities:

All employees play a role in business continuity; however, the following individuals play a critical role in planning:

- Executive Committee – Allocate resources and support initiatives.
- Senior Business Leaders – Support implementation of strategies and plans.
- Functional Leader – Is responsible for the Business Group Plan/s development, implementation, maintenance, testing and execution.
- Business Continuity Coordinators - Coordinate planning efforts for a Business Group or Department.
- Avaya Corporate Security & Business Continuity – Oversees and manages the Business Continuity Program. Provides assistance to the Business Groups.

Business Continuity Planning Requirements:

Business Continuity Plans must be documented using the Sales Force based tool FUSION Risk Management.

Per the structure defined in the tool, all Plans will include as a minimum:

- Organization Details – Mission statement and general description of short and long term main Recovery Strategies.
- Business Impact Analysis (BIA), which includes:
    - Identification of business processes performed with indication relative criticality (High, Medium or Low) and the impact of not being able to perform them.
    - Identification of locations in which the process is performed and staffing levels needed based on process criticality.
    - Identification of organizational (internal and external) and technological (application) dependencies, including if applicable, alternate procedures to support services/application disruptions (*).

  - Definition of Recovery Time Objectives (RTO) for each process.
  - Definition of specific process related Recovery Strategies
- General Contingency Procedures outlining the overall generic steps involved in the Response, Recovery, Resumption and Return Phases, and in any other specifically applicable scenario.
- Organization's contact information (Team Rosters).

Business Continuity Plans must be reviewed, validated and approved at least once every 365 days. Business Groups are responsible for keeping their Plans always current and up to date.

Business Continuity Plans must be tested in accordance to their Recovery Strategies at least once every 365 days.

Organizations that are unable to comply with this Policy must obtain written Vice President (VP) approval using the BCP Exception Request Form and submit it to Avaya Corporate Security & Business Continuity. Approved Policy Exception Forms must be renewed and validated by the applicable VP and re-submitted to Avaya Corporate Security and Business Continuity every 90 days until compliant status is achieved. Risk cannot be solely accepted if there is impact to other groups within Avaya.

Organizations deviating from this Policy or found non-compliant with the Business Continuity Program are susceptible of being reported to the Executive Committee. Avaya Corporate Security & Business Continuity may enforce compliance or, if the Business Group is unable to comply, request a Policy Exception Form to be completed.

(*) Alternate Procedures implementation related to applications must ensure compliance with Avaya's Security Policy and Information Security Standards.

APPENDIX B – Definitions

Application Criticality: The level of criticality of an application is given by the negative impact caused by that application's disruption or unavailability. Application criticality levels for Avaya IT supported applications are based on the cumulative BIA responses and categorized as Gold, Silver and Bronze. These levels will drive the Recovery Time Objective (RTO) for each application.

Avaya Corporate Security & Business Continuity: The mission of Corporate Security and Business Continuity is to enhance Avaya's business by safeguarding human, physical and information assets while ensuring resiliency through planning and incident management.

Avaya Global Support Services (GSS) / Avaya Private Cloud Services (APCS): GSS and APCS are the premier providers of comprehensive technical support to enable the productivity and continuity of our clients' communications. GSS/APCS experts restore over 90% of Total Outages within 2 hours, over 70% of incoming requests are solved through self-service, and a true omni-channel experience helps customers to resolve their issues with seamless transition from the Avaya virtual agent (Ava) to our Avaya support engineers via Avaya Web Chat, Web Talk, and Web Video.

Knowing our global customers and partners, anticipating their needs, and delivering exceptional support services through our people, services support, software, and best practices helps GSS and APCS to differentiate and create higher value within the marketplace.

Business Continuity: Capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident (BS ISO 22301:2012).

Business Continuity Plan: Documented procedures that guide organizations to respond, recover, resume, and restore to a predefined level of operation following a disruption (BS ISO 22301:2012).

Business Continuity Program: Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management (BS ISO 22301:2012). At Avaya the Business Continuity Program (BCP) operates as a shared management process which objectives are to identify potential risks and business impacts that threaten an organization, and to provide a framework for building resilience into the business model, allowing an effective response that safeguards the interests of our stakeholders, reputation, brand, and value creating activities.

Business Impact Analysis (BIA): Process of analyzing activities and the effect that a business disruption may have upon them (BS ISO 22301:2012). Identifies all business processes performed and determine the impact of not being able to perform them as a result of a business interruption or outage. Identifies resources (e.g. staffing, applications, equipment, etc.) required to support business processes. Identifies locations which the process is performed at and staffing levels needed based on process criticality. Defines Recovery Time Objectives (RTO) for each process. Defines specific process related Recovery Strategies.

Contingency Procedures: An alternative to the normal procedures; triggered if an unusual but anticipated situation arises. Contingency procedures as part of a Business Continuity Plan define steps for each phase of the crisis (response, recovery, resumption and return) and/or any other specific scenario outlined in the Plan (e.g. Pandemic).

Crisis Management & Incident Response: Overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding harm to people, and minimizing damage to the organization's profitability, reputation, and ability to operate.

Executive Crisis Management Team (ECMT): Final instance of the Crisis Management & Incident Response Process, which is formed by Avaya's Senior Leaders and it's activated in the event of a major business interruption impacting multiple Business Groups and/or locations.

Incident Management Plan (IMP): Plan used by the Local Incident Management Team to minimize the risk and impact of a local disruption that may have an effect on the safety of Avaya employees and/or the ability to continue business. IMPs establish basic response procedures for typical crisis scenarios that may result from natural, human-caused or utility related/technology hazards. In addition to these procedures, the IMPs outline the communication and escalation process that should be followed during the crisis response. Finally, these Plans contain important location information that goes from contact information to aspects tied to the location Risk Assessment. IMPs are reviewed, validated and approved recurrently at least once every 365 days.

IT Disaster Recovery: Disaster Recovery Program led by Avaya IT Security. It provides the strategy and planning for the recovery of mission critical IT managed applications, servers, databases and infrastructure.

Local Incident Management Team (IMT): Team formed with representatives from the core functions located in a particular location. These Teams are responsible for assisting with response and recovery efforts, reporting back to their business groups, and executing recovery activities as needed.

Local Incident Manager: Designated individual that serves as initial responder and liaison with Avaya Corporate Security & Business Continuity within the application of a Local Incident Management Plan.

Mission Critical: Any component of a system or infrastructure (including applications, databases, network, software, etc.) that is essential to the core business operations. The extended disruption of mission critical systems or infrastructure will result in serious impact on our company's business.

Process Criticality: The level of criticality of a process is given by the negative impact caused by that process disruption. Process criticality levels will vary between high, medium and low, and will drive the definition of the Recovery Time Objective (RTO).

Recovery Strategy: Strategy to recover process related resources through the duration of a disruptive incident. This strategy is driven by the process criticality and RTO demands, and may include alternate options like instruct resources to work from home, transfer work, or deploy to a certain location.

Recovery Time Objective (RTO): Period of time following an incident within which a product, service or activity must be resumed, or resources must be recovered (BS ISO 22301:2012). As a general rule, Avaya establishes the following generic RTO requirements business process criticality:

PROCESS CRITICALITY LEVEL	RTO
High	Less than 24 to 48 Hours
Medium	72 Hours to less than 1 Week
Low	1 Week or Greater

Regional Response Team (RRT): Extension of the Local Incident Management Teams. RRTs are usually activated when the scope of the event is beyond the capability of the Local Incident Management Team.

Risk Assessment: Overall process of risk identification, risk analysis and risk evaluation (BS ISO 22301:2012). Risk Assessments are an integral part of the Local Incident Management Plans (IMP) outlining location infrastructure and assessing potential risks for natural, human-caused or utility related/technology hazards (both from a likelihood and vulnerability standpoints).

BUSINESS CONTINUITY PROGRAM RELATED INQUIRES

Inquires related to the Avaya Business Continuity Program should be directed to your Account Team, Contract Manager, or Contract Negotiator.

In case you need to contact Avaya Corporate Security & Business Continuity directly, please address your questions to:

Maximiliano Lacobara
Senior Manager – Avaya Corporate Security & Business Continuity
mlacobara@avaya.com

Timothy Ryan
Director – Avaya Corporate Security & Business Continuity
tr@avaya.com