Avaya Corporate Security & Business Continuity
Business Continuity Program Overview

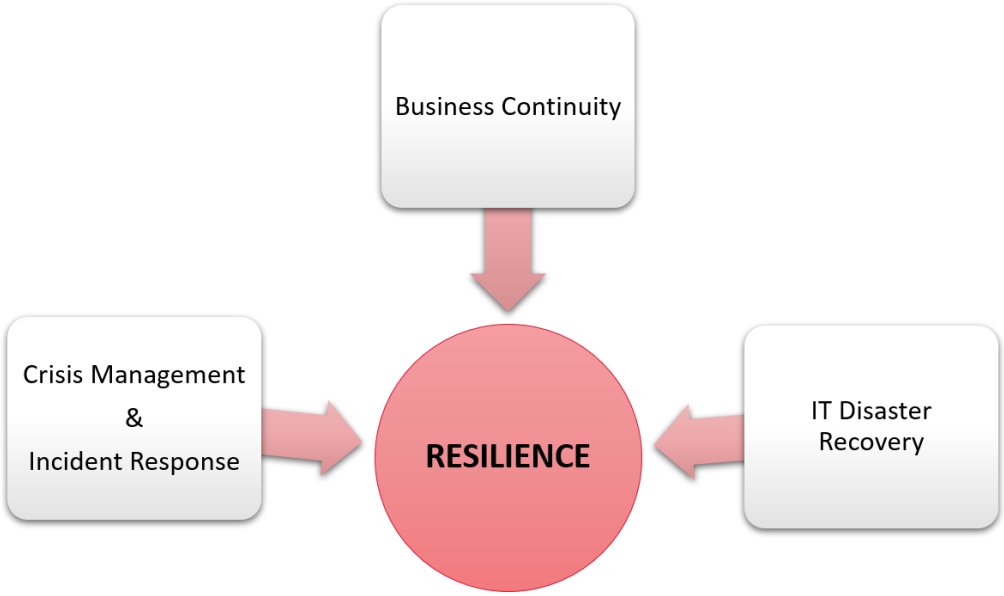
Contents

1. The Avaya Resilience Structure

The primary goal of the resilience concept at Avaya is to enable the organization to respond and survive a disaster or business interruption and continue business operations, observing the following as some of its key objectives: Safeguard human life; minimize financial loss; continue critical business operations; continue to serve customers; mitigate the negative effects disruptions can have on Avaya's strategic plans, reputation, operations, liquidity, credit quality, market positions, and ability to remain in compliance with applicable laws and regulations; minimize the duration of a serious disruption to business operations; provide effective coordination of recovery tasks and reduce the complexity of the recovery effort; make the decision-making process more efficient during a disaster; manage successfully through a disaster; and minimize any negative media coverage/receive positive media coverage as a result of advanced planning.

The following are the main Programs interacting towards the accomplishment of the mentioned objectives:

- Business Continuity
- Crisis Management & Incident Response
    - Location Incident Management Planning & Response (IMP)
    - Data Breach Incident Response Team (DBIRT)
    - Avaya Computer Emergency Response Team (ACERT)
- IT Disaster Recovery (ITDR).



Additionally, on the customer facing front, Business Continuity assurance in relation to services provided to customers is facilitated by:

- Avaya Services Delivery Business Continuity
- Avaya Managed Services (APCS) Business Continuity
- Customer Account Teams

2. The Corporate Business Continuity Program Model at Avaya

The mission of Corporate Business Continuity is to establish and maintain a documented program to protect against, reduce the likelihood of occurrence of, prepare for, respond to, and recover from disruptive incidents when they arise.

Considering that Business Continuity is defined as the capability to continue the delivery of products or services at acceptable predefined levels following a disruptive incident, the Avaya Business Continuity Program operates as a shared management system that identifies potential risks, and the business impacts of those risks, that threaten an organization, provides a framework for building resilience into the business model, allows for an effective response to mitigate the impact to people, business, the company, and ultimately Avaya's customers, and safeguard the interests of Avaya's stakeholders, reputation, brand, and value creating activities.

The Business Continuity Program interacts in close relationship with Avaya's Crisis Management & Incident Response Program, 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 and Crisis Management & Incident Response Programs, in conjunction with other specialized processes like IT Disaster Recovery, define the structure and the tools that Avaya uses to ensure resiliency and ultimately overcome the potential or actual impact of a crisis.

While the Program is managed by Avaya Corporate Security & Business Continuity, Business Continuity is a collective effort that involves all Avaya's Business Units and Support Functions. This model allows the business to focus on their critical aspects while providing coordinated and integrated planning, management and administration.

Avaya has a Business Continuity Policy in place that was designed following the ISO 22301 Standard requirements.

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

- **Avaya Executive Leadership** is responsible for allocating resources and supporting BCP initiatives.
- **Senior Business Unit Leaders** are responsible for supporting the implementation of strategies and plans, acting as the actual owners of their Business Unit BCP Program.
- **Department Managers** are responsible for ensuring the integration of the Business Continuity Program requirements into their organization's business processes.
- **Business Continuity Coordinators**, designated by the business leaders, are responsible for coordinating the planning efforts for their business group or department.
- **Plan Owners** are responsible for managing their assigned Business Continuity Plans.
- **Avaya Corporate Security & Business Continuity** is responsible for overseeing and managing the Business Continuity Program and providing assistance to the Business Units globally with their efforts in the planning arena and in response to a business interruption or incident. This Team also

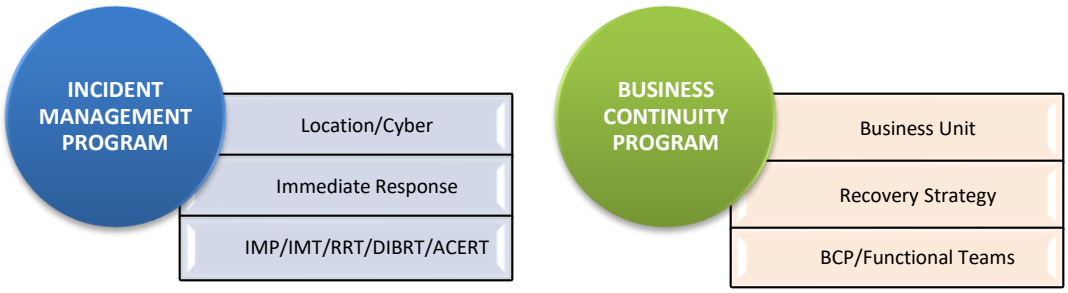
operates as an audit function to ensure compliance with their established policy and procedures, tracking and reporting on each Business Unit's progress to executive leadership as required.

The Policy also establishes specific planning requirements, which include:

- Plan documentation, administration, and review and testing requirements,
- Definition of critical or major processes,
- Risk assessments,
- Business Impact Analysis,
- Definition of Recovery Strategies,
- General Contingency Procedures,
- And Business Unit's Business Continuity Team information.

3. Crisis Management & Incident Response

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



This program is managed by Avaya Corporate Security and Business Continuity, and merges three major processes:

a. ***Location Incident Management Planning & Response (IMP)***
b. ***Data Breach Incident Response Team (DBIRT)***
c. ***Avaya Computer Emergency Response Team (ACERT)***

Location Incident Management Planning & Response

This process manages the development and implementation of Incident Management Plans (IMP) that drive the immediate response on a crisis impacting a specific Avaya location.

The Incident Management Plans establish basic response procedures for typical crisis scenarios that may affect an Avaya Major Location as a result from natural or man-made disasters. In addition to these procedures, the IMPs outline the communication and escalation process that should be followed during the crisis response at a location level. 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 Location Incident Management & Incident Response Policy establishes the designation of a Local Incident Manager that serves as point of contact 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 this 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.

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).

Data Breach Incident Response Team (DBIRT)

The DBIRT is a cross-functional team specifically created to respond to data breaches. This team, when convened, executes Avaya's Data Breach Incident Response Plan (DBIRP).

The purpose of the plan is to provide a well-defined, organized, repeatable, and documentable approach for Avaya to efficiently and effectively respond to an incident and minimize the impact of a breach of Company's or a third party's (including a customer's or a business partner's) confidential, proprietary, sensitive and/or mission critical information.

Avaya Computer Emergency Response Team (ACERT)

The Avaya Computer Emergency Response Team serves as the central point for monitoring, assessing, alerting, and leading all Avaya response to vulnerability, incident, alerts, warnings, intrusion, and artefacts. This team works to assure the timely securing of Avaya computing through assessment, communication, patching, anti-virus, firewalls and many other products or techniques.

The main objective of the ACERT is to prevent or reduce impact from vulnerabilities, malicious attacks, and Virus, Worm, Trojan, Spy and Adware.

To accomplish this objective, the team is supported by a Security Information and Event Management (SIEM). Avaya's Security Information and Event Management (SIEM) is provided by McAfee, Intel Security.

The SIEM takes a holistic approach to managing Avaya's environment. SIEM conducts security analysis of security event logs information to baseline and correlate data from multiple devices and device types. From the information gathered, SIEM provides notification of prioritized events based on their risk to Avaya and the ability to mitigate them.

SIEM include event feeds from many management systems as defined by ACERT to provide a more holistic view of the network from multiple device types as well as event feeds from the associated security infrastructure devices (including firewalls, IDS/IPS etc. by correlating firewalls and IDS/IPS alerts, the SOC can focus on prioritized actionable items, not raw data.

4. IT Disaster Recovery (ITDR)

Avaya's Disaster Recovery Planning (DRP) Program 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 Business Continuity, Sales, Services, Operations, and Information Technology departments to provide technology recovery solutions. Incidents, outages and interruptions to Avaya's Mission Critical applications are within the scope of the DRP Program Model.

IT is accountable to develop and maintain a sustainable Disaster Recovery management program and strategy. The program goal is to deliver viable recovery of mission critical applications and technologies.

The policies, plans and procedures addressed in the corporate wide Disaster Recovery Program Model include: Disaster Recovery Planning, Maintenance, Testing, and Training and Awareness. The methodologies also include:

- Strategy Development
- Strategy Implementation
- Project Initiation
- Review of Business Impact Analysis conducted by BCP and/or DRP
- Risk Mitigation

Avaya's policy states that critical applications must have documented DRP plans in place. The plans outline the processes, procedures, vital records and people necessary to recover those critical applications.

Avaya's 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.

5. Avaya Services Delivery Business Continuity

Avaya's Services Delivery 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.

Several Avaya solutions are integral to the Services Delivery Business Continuity Plan. Capabilities leveraged within the Plans 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.*

6. Avaya Managed Services - 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.

The Avaya Managed Services Business Continuity Plan is ISO22301 Certified.

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 online 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.

7. 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.*

8. ISO 22301 "Business Continuity Management System" Certification

Avaya currently holds the ISO 22301 certification for the following Business Continuity Plans:

d. ***Avaya Corporate Security & Business Continuity*** (*)
e. Avaya Managed Services (APCS)

(*) The Avaya Corporate Security & Business Continuity Plan contains the Corporate Business Continuity Management and the Crisis Management & Incident Response Processes, including the DBIRT administration.

9. 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; 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

1.0 Overview

This policy was developed to align with other corporate policies at Avaya. This policy will be reviewed as it is deemed appropriate, but no less frequently than once a year.

Avaya is committed to conducting business in accordance with all applicable laws, regulations and standards. Specifically related to Business Continuity, Avaya designed this policy following the ISO 22301 – 2012 International Standard. Considerations are given to general liability, life and safety, security, and vital records statutes.

2.0 Purpose

This policy outlines the requirements for the Avaya Business Continuity Program (ABCP) to establish a documented program to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

3.0 Scope and Objectives

Considering that Business Continuity is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident, the Avaya Business Continuity Program shall operate as a shared management system that identifies potential risks and business impacts that threaten an organization, provides a framework for building resilience into the business model, which allows for an effective response to mitigate the impact to people, business, the company, and ultimately our customers, and safeguard the interests of Avaya's stakeholders, reputation, brand, and value creating activities.

Specific objectives of the Program include: Safeguard human life; minimize financial loss; continue critical business operations; continue to serve customers; mitigate the negative effects disruptions can have on Avaya's strategic plans, reputation, operations, liquidity, credit quality, market positions, and ability to remain in compliance with applicable laws and regulations; minimize the duration of a serious disruption to business operations; provide effective coordination of recovery tasks and reduce the complexity of the recovery effort; make the decision-making process more efficient during a disaster; manage successfully through a disaster; and minimize any negative media coverage/receive positive media coverage as a result of advanced planning.

This policy applies to all Avaya's Business Units and Support Organizations.

4.0 Policy

4.1 Oversight and governance of the Avaya Business Continuity Program belongs to the Avaya Corporate Security & Business Continuity Organization.

4.2 Each Business Unit (BU), must have Business Continuity Plans aligned with the requirements of this policy. The specific plans to be implemented will be determined between the BU BC representative and ABCP representative. Responsibility for developing, implementing, maintaining, testing, and executing these Business Continuity Plans belongs to the BU in which those plans reside supported by the ABCP representative. Funding, coordination, and staff assignment is the sole responsibility of the Business Unit.

4.3 Management Commitment and Roles & Responsibilities

4.3.1 All employees play a role in business continuity; however, the following individuals play a critical role in the Avaya Business Continuity Program:

- **Avaya Executive Leadership** – Allocate resources to, and support for, the Avaya Business Continuity strategy and its related activities and initiatives.
- **Senior Business Unit Leaders** – Ensure the integration of the Business Continuity Program requirements into their organization's business processes; designate a Business Continuity Coordinator and ensure that the resources needed to satisfy the requirements of the Business Continuity Program as they apply to their organization are available and properly trained; communicate the importance of effective business continuity management and conforming to the ABCP requirements; ensure all the interested parties within the Business Units are aware of the Business Unit's Business Continuity Plan and their role in it; ensure policy compliance and that the application of the ABCP within their organization achieves its intended outcome(s); direct and support persons to contribute to the effectiveness of the ABCP; promote continual improvement; and support other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.
- **Department Managers** – Ensure the Business Continuity Plans that apply to their Department are developed, implemented, maintained current, tested, reviewed and approved within the terms established by this policy. Provide to the Business Unit Leaders requirements and report planning status to accordingly.
- **Business Continuity Coordinators** – Serve as the primary point of contact between their Business Unit or Department, BU Plan Owners, and Avaya Corporate Security & Business Continuity. Coordinate the planning efforts for their Business Unit or Department. Provide requirements of the Business Unit Leadership and Department Management.
- **Plan Owners** – Manage their assigned Business Continuity Plans according to the requirements of this policy.
- **Avaya Corporate Security & Business Continuity** – Oversee and manage the Avaya Business Continuity Program. Assist the Business Units in complying with the ABCP requirements. Provide training and awareness as applicable.

4.4 Business Continuity Planning Requirements

4.4.1 Business Continuity Plans must be documented using the Salesforce-based tool, Fusion Risk Management.

4.4.2 Plans must cover critical and/or major processes (Process) performed by the Business Unit or Department. The definition of these processes must be documented by a Process Criticality Mapping.

4.4.3 For accurate planning purposes, Business Unit Business Continuity Coordinators and Plan Owners should support and complement their risk considerations by the use of appropriate Risk Assessments. Avaya Corporate Security & Business Continuity performs annual risk assessments on major or specially considered locations. Summarized copies of these can be provided upon formal request. If a risk assessment over a geographic area or location not covered under the Avaya Risk Assessment portfolio is needed, Avaya Corporate Security & Business Continuity can assist with this requirement upon formal request.

4.4.4 Per the structure defined in the tool, all Plans will include:

- Purpose, scope, and objectives.
- A Business Impact Analysis (BIA) covering each defined Process. The BIA will include:
  - Process name and description.
  - Frequency in which the process is being performed.
  - Relative Criticality, measured as Low, Medium, or High.
  - Indication about if the process is customer facing.
  - Recovery Time Objective (RTO), which can vary from less than 24 hours to 1 week or greater.
  - Indication of Financial, Operational, Compliance/Regulatory, Reputational, and Customer Service Impacts, both at and beyond the RTO timeframe from day 1 to after 1 week, all measured as Low, Medium or High.
  - Process Internal Dependencies, meaning the other major internal organizations that are being served or serve the process (input and output)
  - Process External Dependencies, meaning the critical external parties (partners, vendors, etc.) that serve the process.
  - Process Application Dependencies (Required Applications), outlining the applications that are critical to run the process, and if there are alternate or manual procedures to meet the RTO in case the application is unavailable, or an RTO gap has been identified.
  - Process Required Resources, including any hardware or equipment that is critical to operate the process.
  - Process Sites (Recovery Strategies), outlining the number of resources operating the process at each site, and the strategies that will be applied to continue operating. These strategies may include work from home, transfer work, or deploying to an alternate location.
- Activation criteria and procedures to manage a disruptive incident to continue the activities based on the recovery strategies identified in the business impact analysis.
- Roles, responsibilities and Business Unit Members critical to the Business Continuity effort.

4.4.5 Plans must be reviewed, updated and approved at least once annually. This review

must include validation of the Business Impact Analysis for each process within the plan.

4.4.6 Approvals must be obtained through Fusion's approval feature and will include the Business Unit Business Continuity Coordinator, the Corporate Business Continuity representative who will operate as an independent reviewer, and the Department Manager. A plan will be considered fully approved and current only after the Department Manager approval was obtained.

4.4.7 Plans must be distributed to those with a need to know role every time they are updated annually, or when they are subject to a change that affects a major procedure, recovery strategy, or contact information. While the need to know threshold can vary, the plan distribution list must always include as a minimum the Plan Owner, the Business Continuity Coordinator, the Department Manager, and the members defined in the plan Team Roster.

4.4.8 Plans must be tested in all their Process Recovery Strategies at least once annually. Since it's not necessary to test everything at once, a testing schedule is recommended. Actual incidents leading to an activation of the Plan are acceptable as testing evidence.

4.5 Incident Response/Testing Documentation

4.5.1 All incidents and tests must be documented by using the Incident Module of the Fusion Risk Management tool and must be associated with their applicable Plan.

5.0 Training, Governance & Enforcement

5.1 Training & Awareness

5.1.1 The Business Unit is responsible for ensuring Avaya Corporate Security & Business Continuity is notified upon the designation of new Business Continuity Coordinators and Plan Owners, so they can receive appropriate training.

5.1.2 The Business Unit is responsible for ensuring that all the applicable resources within their organization are aware of the Department Business Continuity strategies, plans, and their role in them.

5.1.3 Avaya Corporate Security & Business Continuity will provide training to the Business Unit Business Continuity Coordinators and Plan Owners upon request or as required in accordance to the needs of their roles.

5.2 Policy Enforcement & Compliance Exceptions

5.2.1 Organizations that are unable to comply with this Policy must obtain written Vice President (VP) approval using the ABCP 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.

5.2.2 Organizations deviating from this Policy or found non-compliant with the Avaya Business Continuity Program are susceptible of being reported to Executive

Leadership. Avaya Corporate Security & Business Continuity may enforce compliance or, if the Business Unit is unable to comply, request a Policy Exception Form to be completed.

5.3 Organizational Support & Guidance

5.3.1 All inquiries related to the Avaya Business Continuity Program and this Policy, including but not limited to general questions, customer support, risk assessments, planning, policy exceptions, etc., must be directed to Avaya Corporate Security & Business Continuity to security@avaya.com

5.3.2 Specific guidance on how to comply with each section of this policy can be found in the Avaya Business Continuity Planning Guidance.

APPENDIX B – Definitions

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 shared management system that identifies potential risks, and the business impacts of those risks, that threaten an organization, provides a framework for building resilience into the business model, allows for an effective response to mitigate the impact to people, business, the company, and ultimately Avaya's customers, and safeguard the interests of Avaya's 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 point of contact 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 24 Hours
Medium	48/72 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 Units use these Risk Assessments, or others provided as part of the Program for their Business Continuity planning purposes.

BUSINESS CONTINUITY PROGRAM RELATED INQUIRES

If you are an Avaya actual or potential customer, inquires related to the Avaya Business Continuity Program should be directed to your Account Team, Contract Manager, or Contract Negotiator.

Internal Avaya requests related to customer inquiries must be directed to the ***Customer Security Request Team*** via e-mail to csrteam@avaya.com

Internal Avaya inquires related to the Avaya Business Continuity Program can be directed to:

Maximiliano Lacobara
Global Business Continuity Program Manager
mlacobara@avaya.com

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