CenturyLink®

Business Continuity Management Program Overview

“Improving the lives of our customers by connecting them to the power of the digital world”

CenturyLink Key Objective

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner.

©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

EXECUTIVE SUMMARY

CenturyLink is committed to ensuring business resiliency and survivability during an incident or business disruption. Our Corporate Business Continuity Management program (“Program”), in conjunction with the Company’s culture and Unifying Principles, fosters an environment of prevention, collaboration, communication, response and recovery, ultimately ensuring our ability to serve customers, shareholders and employees in the face of disruptive events. This document summarizes CenturyLink’s BCM program and its resiliency and preparedness capabilities.

Program Goals

In Support of CenturyLink’s Key Objective, “Improving the lives of our customers by connecting them to the power of the digital world,” the goals of the Program are to:

- Evaluate the purpose and operations of the Company, identifying threats, hazards, and potential impacts to critical business priorities
- Develop strategies for mitigation, continuity, and recovery
- Maintain uninterrupted service whenever possible, and when necessary, effectively coordinate recovery from business disruptions safely, quickly, and efficiently
- Enable continual improvement by periodically reviewing Program strategy and performance

Program Governance

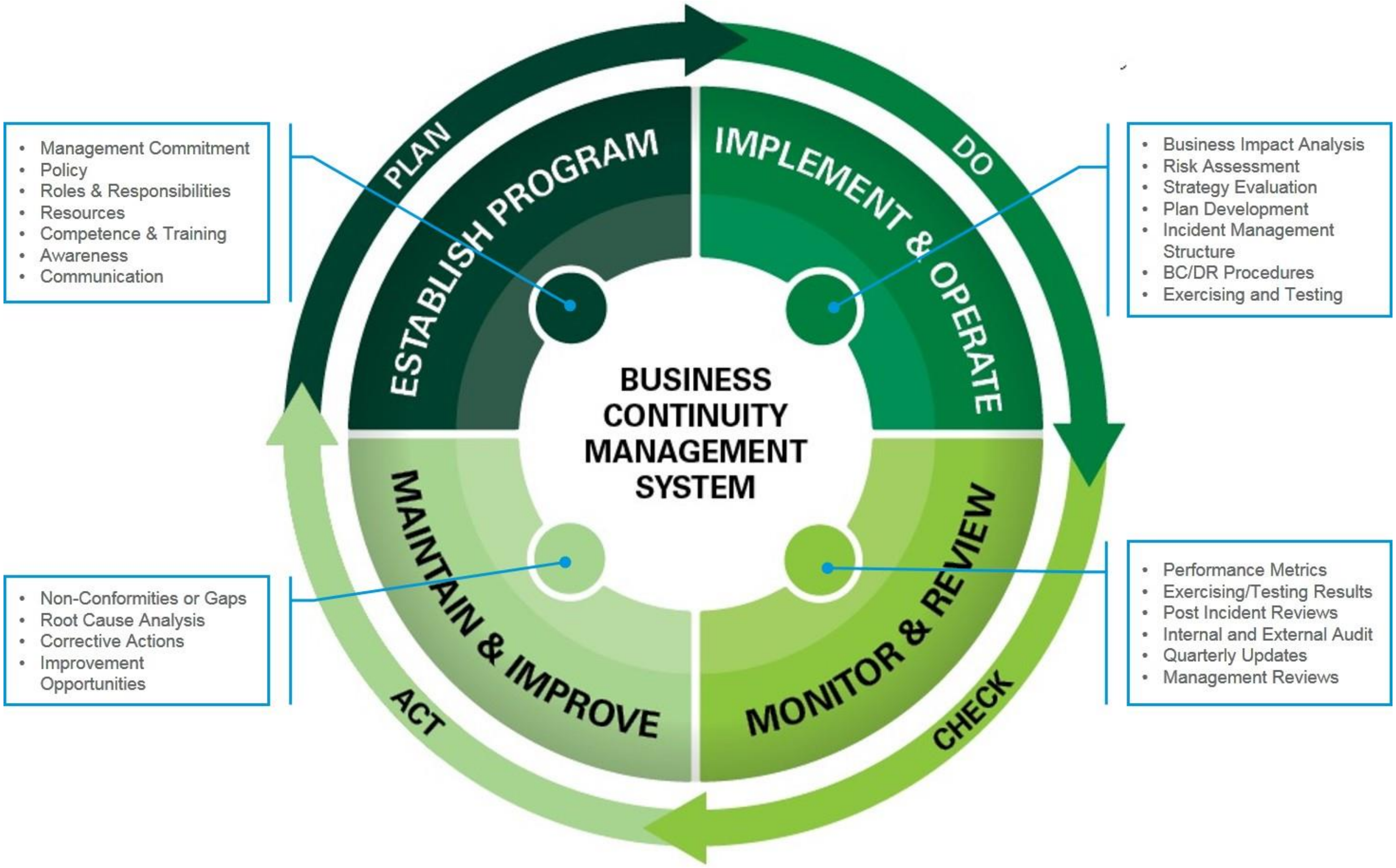
- **Standards:** In addition to a number of planning elements required by regulations, CenturyLink has aligned its Program to adhere to ISO 22301:2012, the International Standard for Business Continuity Management. In 2017, CenturyLink’s Program was awarded certification[1] to this industry standard of its BCM system and subsequent business functions supporting the SAP-HANA Enterprise Cloud for Managed Hosting Services environment.
- **Leadership:** CenturyLink Top Management supports the Program by assigning program partners to represent their organization’s interest in operational resiliency
- **Policy:** Top management establishes BCM Policy committed to maintaining a Corporate BCM team, framework, setting Program objectives, and assignment of resources to execute the Program
- **Metrics:** The Corporate BCM team maintains a dashboard monitoring completion of BCM activities
- **Scorecard:** Top Management reviews a Program scorecard at planned intervals to ensure its suitability and effectiveness
- **Audit:** CenturyLink engages internal and external audit firms to perform multiple types of assessments designed to address our customers’ diverse compliance requirements.

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

[1] Certificate Number 1802753-1 by Schellman & Company, LLC; For more information, reach out to BCM@centurylink.com.

PROGRAM FRAMEWORK

The key to resiliency is the Program's framework that gives our customers the confidence that our services will run with minimal interruptions, regardless of the incident. In alignment of ISO 22301:2012, CenturyLink's Program is based on a Plan-Do-Check-Act model comprised of the following key components:



- Management Commitment
- Policy
- Roles & Responsibilities
- Resources
- Competence & Training
- Awareness
- Communication

- Business Impact Analysis
- Risk Assessment
- Strategy Evaluation
- Plan Development
- Incident Management Structure
- BC/DR Procedures
- Exercising and Testing

- Non-Conformities or Gaps
- Root Cause Analysis
- Corrective Actions
- Improvement Opportunities

- Performance Metrics
- Exercising/Testing Results
- Post Incident Reviews
- Internal and External Audit
- Quarterly Updates
- Management Reviews

ESTABLISH PROGRAM

- **Program Management:** Dedicated resources establish accountability and reinforce CenturyLink's commitment to the business continuity standards required to provide customers reliable and resilient service.
- **Competence, Training & Awareness:** The Program utilizes role-based training curriculum to ensure participants are competent to the responsibilities for executing required tasks.

IMPLEMENT AND OPERATE

- **Business Impact Analysis (BIA)** interviews are conducted to identify the Company's key operational functions and the impact(s) a disruption would have on them. This analysis provides an understanding of time-critical priorities, key resources, and interdependencies so recovery time objectives can be established, approved, and integrated into planning strategies.
- **Risk Assessment (RA)** interviews are conducted to evaluate threats, hazards, and potential causes of interruptions, the probability of their occurrence, and the impact severity when they occur.

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

- **Strategy Evaluation and Plan Development:** The BIA and RA collectively provide data integral to evaluating, developing, and implementing strategies for reducing the likelihood and impacts of disruptive incidents.
- **Incident Management and Business Continuity/Disaster Recovery Plans** provide procedures for maintaining continuity of operations and are implemented to effectively respond to and recover from Company-wide operational disruptions.
- **Exercising and Testing:** To test viability and develop a state of readiness, critical plans are required to be reviewed and exercised annually.

MONITOR AND REVIEW

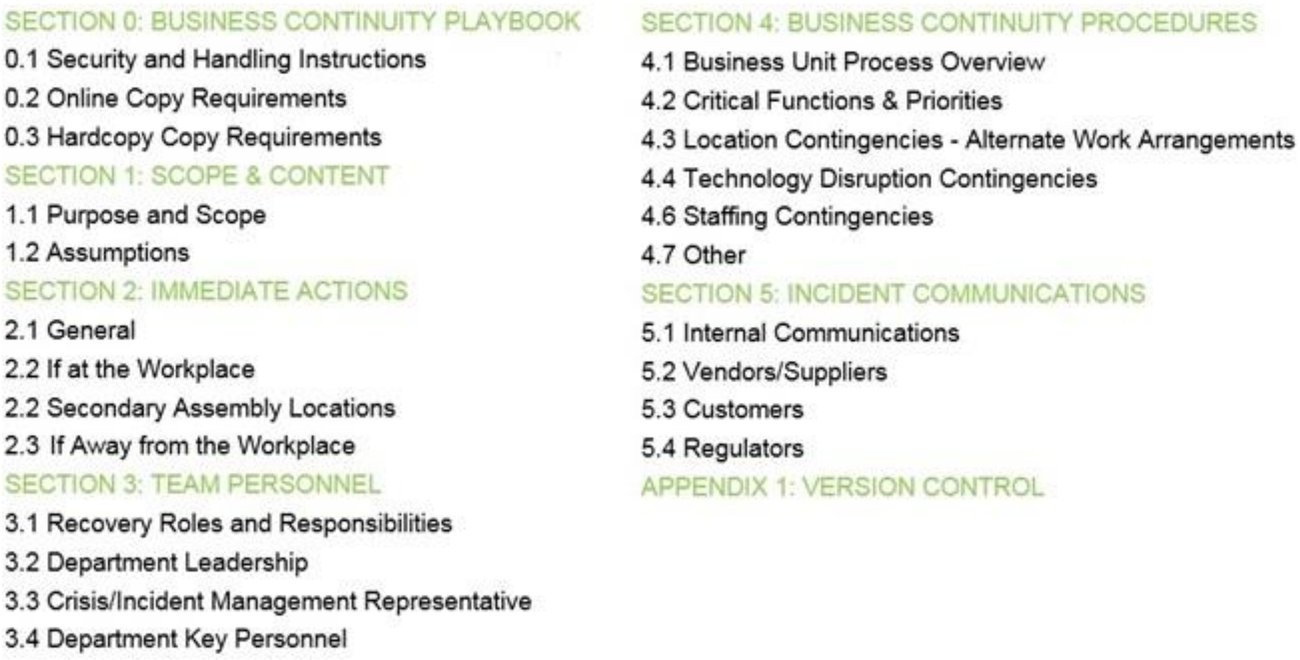
- **Tracking Performance Metrics:** The progress of each organization's compliance with the Program objectives and requirements is continually tracked and communicated out to key Program personnel on a quarterly basis.
- **Post Incident Reviews (PIR)** provide impacted/activated groups an opportunity for recovery process feedback, reflection on lessons learned and address any issue(s) which may require follow up action.
- **Management Reviews** are conducted annually, or when significant business changes occur, to review the state of the Program and ensure alignment with Company strategy and operational initiatives.

MAINTAIN AND IMPROVE

- **Non-conformities, Corrective Actions, and Improvement Opportunities** are tracked and periodically reviewed to ensure findings or gaps are addressed and to enable continual improvement of the Program.

KEY PLAN ELEMENTS

While business continuity plans are proprietary, CenturyLink uses a company-wide planning model that incorporates information as outlined in the plan's Table of Contents below:



SECTION 0: BUSINESS CONTINUITY PLAYBOOK

0.1 Security and Handling Instructions

0.2 Online Copy Requirements

0.3 Hardcopy Copy Requirements

SECTION 1: SCOPE & CONTENT

1.1 Purpose and Scope

1.2 Assumptions

SECTION 2: IMMEDIATE ACTIONS

2.1 General

2.2 If at the Workplace

2.2 Secondary Assembly Locations

2.3 If Away from the Workplace

SECTION 3: TEAM PERSONNEL

3.1 Recovery Roles and Responsibilities

3.2 Department Leadership

3.3 Crisis/Incident Management Representative

3.4 Department Key Personnel

SECTION 4: BUSINESS CONTINUITY PROCEDURES

4.1 Business Unit Process Overview

4.2 Critical Functions & Priorities

4.3 Location Contingencies - Alternate Work Arrangements

4.4 Technology Disruption Contingencies

4.6 Staffing Contingencies

4.7 Other

SECTION 5: INCIDENT COMMUNICATIONS

5.1 Internal Communications

5.2 Vendors/Suppliers

5.3 Customers

5.4 Regulators

APPENDIX 1: VERSION CONTROL

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

PROGRAM ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Corporate Business Continuity Management Office	CenturyLink's Program is managed by full-time business continuity professionals who govern and support the Corporate BCM Program. Responsibilities include: • Developing and maintaining the Program methodology and framework for recovery of business operations, facilities, applications, and the incident response structure. • Maintaining a BCM Guidebook containing the detailed procedures for how to execute the components of the Program • Facilitating Incident Management activities, to include: − developing and maintaining program structure and processes - team membership, role-based training, and exercises − facilitating and managing event communications with interested parties − conducting Post Incident Reviews and tracking action items to closure • Tracking and reporting execution results to determine recoverability and maturity • Directing and supporting continual Program improvements • Conducting reviews with management on BCM capabilities • Maintaining, managing, and administering the BCM related tools (i.e. planning repositories, incident communications, training modules, etc.)
Top Management	CenturyLink's highest level of leadership, representing all major organizations of the Company. Responsibilities include: • Championing the Program and instilling the values of the Program within the organization • Appointing an Executive Sponsor(s) to implement and execute the Program framework within their organization and subsequent functional group(s) • Identifying unacceptable levels of BCM risk
Executive Sponsors	• Accountability for the management, prioritization, implementation, and continual improvement of the Program in their functional group/organization • Appointing Business Continuity Coordinators (BCCs) and granting them the authority to coordinate execution of the Program and verify their responsibilities • Appointing Incident Management Team Commanders to provide efficient command and control over recovery activities and concise communications to stakeholders
Business Continuity Coordinators (BCCs)	• Establishing the structure within their functional group to coordinate execution of the Program • Obtain on-going training and education necessary to design, implement, and maintain the Program's desired execution outcome
Plan Owners / Incident Commanders	• Responsible for the development, approval, and distribution of plans • Verifying plan recovery strategies are implemented, maintained, and exercised • Revising plans as business conditions require (i.e., changes in roles, environment, technology, or operations) • Assuming command over an appropriate response structure • Activating plans when pre-defined triggers have been met and recovering the critical activity within its desired timeframe
Plan Builders	• Support Plan Owner in developing and maintaining plan in the required planning repository • Assisting Plan Owner with any maintenance, exercise, and QA activities
Incident Management Teams (IMTs)	IMTs are comprised of team members representing key functional groups that may serve a critical role during life safety incidents or business disruptions. • Primary team members are paged out for all activations and secondary teams are paged out if they are impacted or needed to support an incident. • Each team is accountable for the overall command, control, and communication within their functional group during recovery.
General Employees	• Complete Program awareness training on an annual basis and other additional training as needed by periodic objectives, projects, or initiatives

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner.

©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

MANAGING AND RESPONDING TO AN INCIDENT

Defining an Incident

CenturyLink defines an ***incident*** as a man-made or naturally occurring disruptive event where the impacts affecting its employees, assets, or critical business operations meet predefined activation triggers. Activation triggers would include life threatening situations (severe weather, natural disasters, pandemic epidemic, workplace violence), extended outages or security breaches for top critical systems or applications, or extended evacuations due to building infrastructure failures or environmental emergencies.

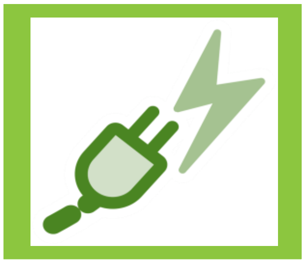
Weather/Nature

- Floods
- Tornadoes
- Hurricanes
- Earthquakes
- Ice/Snow
- Wild Fires
- Volcanoes

Man-Made

- Workplace Violence
- Civil Unrest
- Work Stoppages
- Acts of Terrorism
- National Security
- Criminal Behavior

Equipment/Infrastructure



- Extended Outages
- Equipment Failures
- Technology Disruptions
- Unsafe Facilities
- Security Breaches

Health/Environmental

- Pandemics
- Epidemics
- Hazardous Materials

Activating Incident Management Teams (IMTs)

CenturyLink IMTs are operational 24x7 and convene virtually when any member becomes aware of an actual or impending situation within their support area. Incident Commanders are engaged to determine if the incident has met an activation trigger or threshold and will coordinate activation and deliver the incident assessment if the situation warrants. The IMT(s) reconvene at agreed upon time intervals to provide status updates on their team's tactical recovery and any resources or logistics requirements. Incident Status Reports are updated and distributed after each meeting and disseminate appropriately to Top Management, functional groups and other interested parties. A post-incident review incorporating lessons learned and after-action items from all activated teams will be created to ensure action items are tracked to closure.

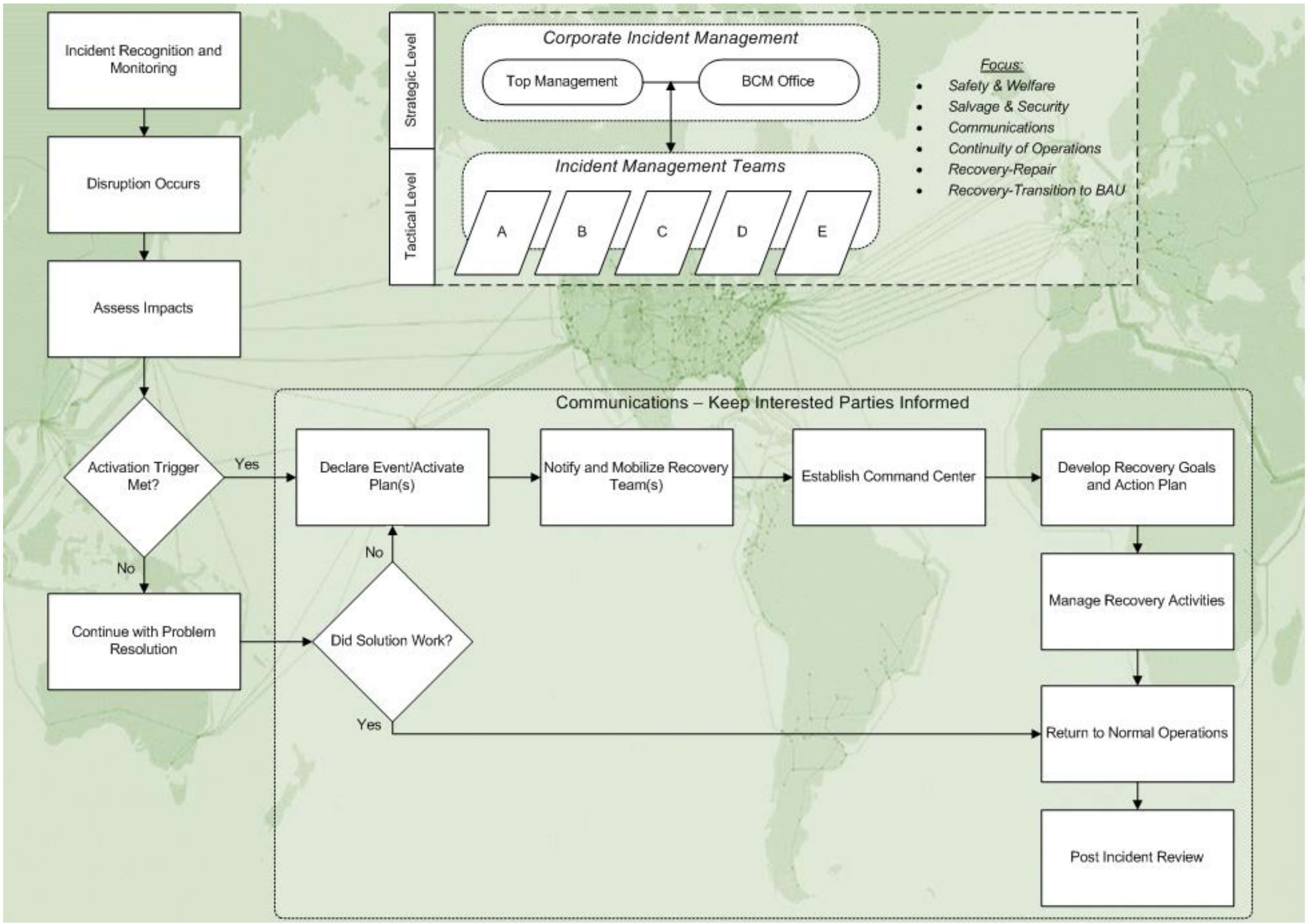
CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

Communicating During an Incident

CenturyLink implements redundant communications capabilities utilizing alternate carriers. Primary and backup conference bridges are supplied by separate vendors using diverse networks and routes. The Company owns and maintains an automated paging system, utilized for activating its Incident Management teams and notifying registered employees of disruptive events or critical situations. Additionally, in times of network congestion or domestic emergencies affecting normal telecommunications means, CenturyLink critical personnel are afforded priority access through the Government Emergency Telecommunications Service (GETS) for public switch telephone networks (PSTN) and the Wireless Protection Service (WPS) for cellular phones.

Recognition, Response, and Recovery Flow

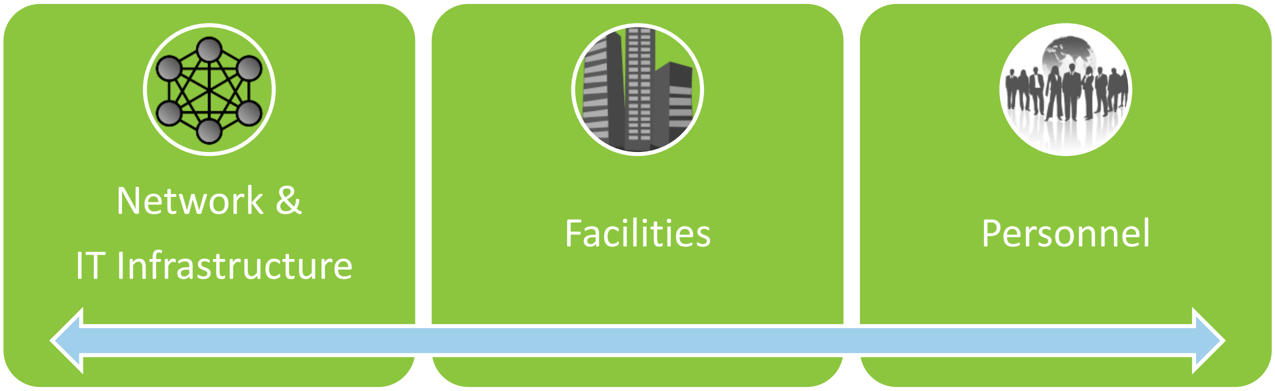
The figure below illustrates how the Incident Management process unfolds and interested parties are kept informed.


Incident Recognition and Monitoring
Disruption Occurs
Assess Impacts
Activation Trigger Met?
Yes
No
Continue with Problem Resolution
Strategic Level
Tactical Level
Corporate Incident Management
Top Management
BCM Office
Incident Management Teams
A
B
C
D
E
Focus:
Safety & Welfare
Salvage & Security
Communications
Continuity of Operations
Recovery-Repair
Recovery-Transition to BAU
Communications – Keep Interested Parties Informed
Declare Event/Activate Plan(s)
Notify and Mobilize Recovery Team(s)
Establish Command Center
Develop Recovery Goals and Action Plan
Manage Recovery Activities
No
Did Solution Work?
Yes
Return to Normal Operations
Post Incident Review

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

RESILIENCY AND PREPAREDNESS CAPABILITIES

As a leader in global communications and IT services, CenturyLink's preparedness capabilities and resiliency strategies include, but are not limited to:



Network & IT Infrastructure

Facilities

Personnel

Network & IT Infrastructure

NETWORK FOOTPRINT

CenturyLink provides services in over 60 countries across the globe, with network and fiber capabilities that connects more than 350 metropolitan areas with 100,000+ on-net buildings. This globally diverse network, including approximately 450,000 route miles of fiber, enables a broad range of services and solutions to meet customers' evolving demands for capacity and reliable connectivity.

NETWORK RELIABILITY

Geographically disbursed network operations centers are staffed 24x7x365 to monitor, identify, and isolate causes of potential network disruptions, and efficiently coordinate resolution of system outages. During a network outage or event, this may include opening event tickets, tracking and correlating events, running event bridges when required, and providing status to interested parties.

NETWORK SECURITY

To support the security of the Company's information and networks, CenturyLink utilizes a team of subject matter experts with diverse technical expertise from Operating Systems, Web Applications, Networking, Computer Forensics and Cryptography. These investigation and response capabilities are maintained 24x7x365 to protect CenturyLink assets from all sorts of cyber threats.

IT OPERATIONS

CenturyLink owns and self-manages geographically dispersed data centers, which are equipped with infrastructure, environment and connectivity to support the Company's processing capabilities and essential business functions. Access to data centers is restricted and backed up by battery and generators when commercial power is disrupted. Information Technology (IT) partners with BCM Program personnel to ensure

Page 8 of 9

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

management of recovery plans for critical applications and hardware, as well as integrating communication activities during an incident.

Facilities

All critical facilities have plans for recovering their critical infrastructure from loss of access, power, HVAC, etc. Periodic inspections and evacuation drills are conducted to protect the safety of our employees, customers and vendors.

FIRE AND LIFE SAFETY

CenturyLink is committed to ensuring the safety of its employees and guests, protecting Company assets, ensuring continuity of Company operations and complying with applicable regulations and codes. Fire and Life Safety plans and subsequent procedures are customized according to each facility.

CORPORATE SECURITY

The Corporate Security group establishes security policies, manages access control systems, and coordinates security improvements to CenturyLink properties. This group manages the 24x7 Security Command Center which responds to alarms, monitors video, monitors global events, supervises security officers and serves as the central point of contact for all security related events.

ALTERNATE WORK ARRANGEMENTS

During a disaster or emergency related event, CenturyLink utilizes an alternate work space process and team to address the needs of business units which occupy impacted facilities. Additionally, CenturyLink deploys remote access strategies providing the ability for employees to work remotely in support of minimizing the impact to customers during disruptive events.

Call center recovery at an alternate site after tornado damage to primary facility

Personnel

With over 50,000 globally located employees, CenturyLink has incorporated into its planning a methodology to address potential or significant disruptions in staffing levels, focusing on the following areas:

- Ensuring mission critical functions remain operational
- Personnel remote access and staff reduction contingency strategies
- Providing an appropriate level of awareness for our employees and customers
- Anticipating and responding to our customer’s needs and possible disruptions to our supply chain

HEALTH AND SAFETY

CenturyLink is committed to protecting the health and safety of our employees, customers and communities we serve by conducting our business in a safe and environmentally responsible manner. Health risks and/or pandemic preparedness is integrated into the planning process of the Business Continuity Program, where health and safety policies and staff provide support and guidance during significant business disruptions or disasters.

SUPPLIERS AND VENDORS

To minimize risk and ensure supplier accountability, multiple CenturyLink groups collaborate for negotiating and executing the contractual agreement terms of sourced products and/or services. This provides CenturyLink the ability to assess the control measures of our suppliers, vendors, and business partners and ensure resiliency strategies are adequately implemented to address service level commitments and continuity of operations.

CenturyLink may modify or terminate this overview at any time, without notice. Neither this overview nor the delivery thereof constitutes a legally-binding commitment by CenturyLink to maintain a Program in any particular manner. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.