Level(3) IS NOW CenturyLink

Business Continuity Program Overview

Corporate Business Continuity Office

Version 4.5

September 2017

Subject to Change Without Notice

IMPORTANT NOTICE: This Business Continuity Program (“Program”) Overview is provided as a courtesy and may not, and should not, be relied upon by any person or entity, including, without limitation, any current, past, or prospective employee, agent, customer, or vendor of Level 3 Communications, LLC (“Level 3”) or any of its affiliates. This Program Overview may be modified or terminated at any time, without notice. The terms and conditions of any relationship between Level 3, or any of its affiliates, on the one hand, and any other person or entity, on the other, shall be governed solely and exclusively by any separate written agreements or other arrangements between the respective parties and not by this Program Overview, regardless of whether such agreement or arrangement is made before, on, or after the date hereof. Neither this Program Overview nor the delivery hereof constitutes a legally-binding commitment by Level 3 to maintain a Program in any particular manner.

Table of Contents

EXECUTIVE SUMMARY

Business continuity planning (BCP) is an essential component of Level 3 Communications' business operating model. Due to the nature of the telecommunications industry, the products and services Level 3 provides are expected by customers to meet remarkably high standards for availability. Level 3 respects this responsibility and ensures a robust Policy and Program is in place to maintain uninterrupted services whenever possible and, when necessary, to recover from unavoidable disruptions quickly and efficiently.

Introduction

The Level 3® Network, an acknowledged part of our global telecommunications critical infrastructure, was built with business continuity in mind, using physical plant components and redundant systems to support continuous, uninterrupted services for our customers. Hardware, however, is only part of the solution. Advance planning to develop and rehearse strategies that capitalize on all of our capabilities and enable us to recover our services quickly remains key to Level 3's resiliency. To engage in effective planning, a cross-functional business continuity planning structure spans across all regions of the company, adhering to the business continuity policy and framework. As a result, Level 3 plans for and works every day to deliver uninterrupted service.

Level 3's development, implementation, and maintenance of the Program's life cycle can give our customers confidence that our services will run with minimal interruptions, regardless of the event experienced.

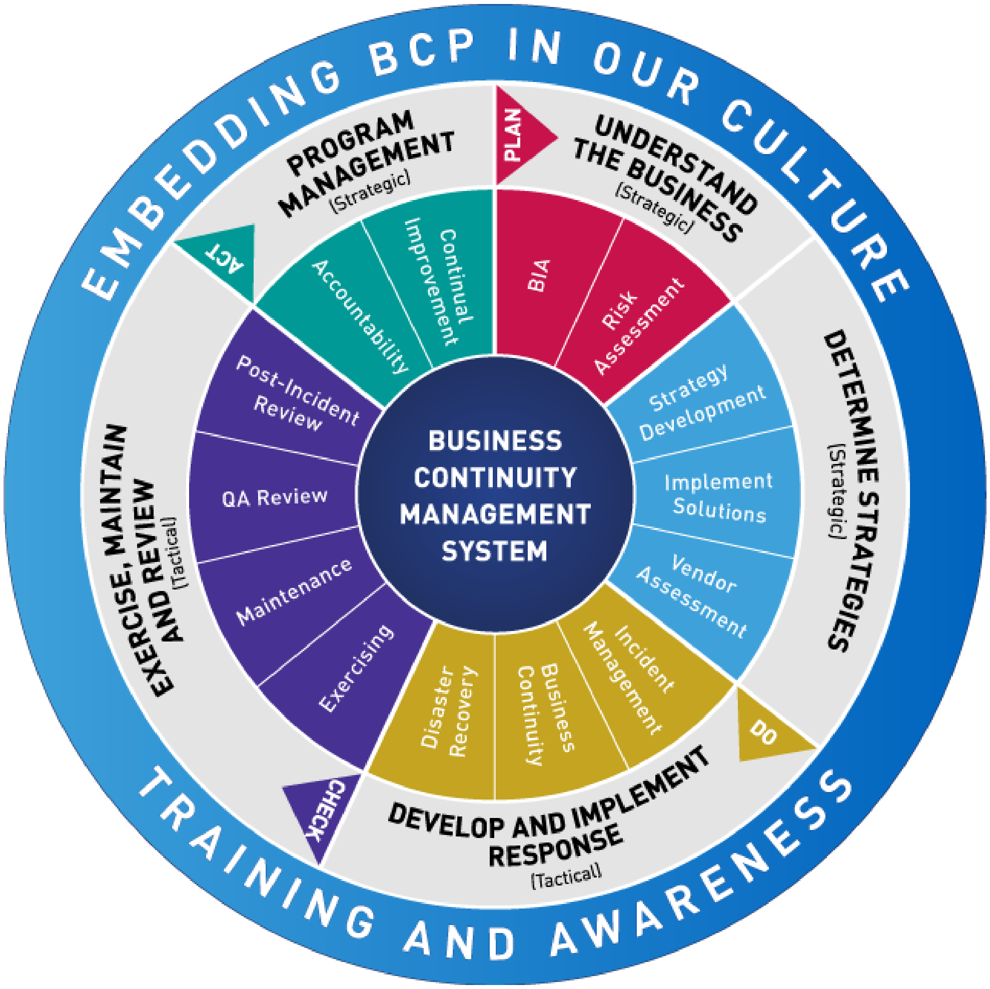


Figure 1: Life Cycle of Level 3's BCP Program

Mission

The mission of Level 3's Program is to:

- Safeguard employees, key stakeholders, and long-term market share in the event of an unplanned interruption to the business
- Identify the threats/hazards and their potential impacts and provide a framework for building enterprise resilience
- Maintain uninterrupted service whenever possible, and when necessary, effectively coordinate recovery from unavoidable disruptions quickly and efficiently
- Respond to emergency situations in a safe, effective and timely manner

Strategy

The Program has been designed to protect shareholder value by ensuring that business continuity related risk is effectively identified, assessed, managed, and where feasible, mitigated. The Corporate BCP Team is responsible for the formulation of policy, developing the framework, and governance of the Program. Each Functional Group owning critical functions is responsible for developing, maintaining, and exercising plans.

A Business Impact Analysis (BIA) identifies criticality and determines how soon after an event processes/systems need to be available. Those time intervals are then used to prioritize the recovery and implement recovery solutions for essential operations. Business continuity planning focuses on planning for the impacts that could be caused by any scenario and defining the appropriate tactical recovery.

The key principles upon which the Program strategies and capabilities are based include:

Incident Prevention – Protecting services from threats (environment, hardware/software, operational errors, malicious attacks and natural disasters)

Incident Detection – Detecting incidents at the earliest opportunity to minimize impact

Response – Responding to incidents in the most appropriate manner providing for an efficient recovery and minimizing downtime

Recovery – Implementing appropriate recovery strategies and solutions that will ensure timely and prioritized resumption of operations

Improvement – Incorporating lessons learned from incidents, exercises and tests to enhance our level of preparedness

Roles and Responsibilities

Corporate BCP Office (BCP Representatives)

- Developing and maintaining the Corporate BCP Program for recovery of business operations, facilities and applications, and response capabilities
- Developing and maintaining the procedures for how to execute the components of the program in a Corporate BCP Guidebook
- Training for roles involved in the Program and awareness for the company
- Providing guidance and support to the Executive Sponsors, BCCs, Plan Owners and Plan Builders in the coordination of Program execution and planning development
- Maintaining a quality assurance review process for reviewing plans
- Advocating and supporting BCP risk mitigation initiatives
- Tracking and reporting on program execution results, recoverability and maturity
- Maintaining, managing, and administering the BCP related tools
- Program governance

Group Heads

- Accountability for and prioritization of executing a well-defined BCP Program within their functional group
- Appointing an Executive Sponsor to implement and execute the BCP Program framework within their functional group

Executive Sponsors (SVP Level)

- Accountability for the management, prioritization and implementation of the BCP Program in their functional group
- Appointing Business Continuity Coordinator(s) (BCC) and granting them the authority to coordinate execution of the BCP Program and verify they perform their responsibilities
- Appointing Incident Management Team incident commanders to provide efficient command and control over recovery activities and concise communications to stakeholders
- Developing Program goals and objectives to measure recoverability capabilities
- Completing a BIA for their functional group to identify the critical areas of their operations and a risk assessment to identify vulnerabilities to threats and hazards
- Managing BCP risk by mitigating unacceptable risk or gaps in resiliency
- Verifying that planning for the critical areas of their organization is implemented, documented, and exercised following Program guidelines

Business Continuity Coordinators (BCCs)

- Establishing the structure within the functional group to coordinate execution of the Corporate BCP Program
    - For larger groups, seek associate business continuity coordinators (ABCCs) to support Program execution activities
- Obtaining on-going training and education necessary to design, implement and maintain the Program’s desired execution outcome
- Coordinating the execution of the Functional Group’s execution activities:
    - Ensuring owner/builders receive on-going training on their roles and responsibilities
    - Ensuring plans are developed, implemented and reviewed
    - Exercising and maintaining plans
    - Supporting coordination of Functional Group’s role in incident management activities
    - Executing the Program’s maturity requirements and deliverables
- Escalating Program issues or risk to Executive Sponsor/functional group management and Corporate BCP Representatives
- Ensuring that any BCC transition takes place appropriately including a “clean hand-off” between the old BCC and the newly assigned BCC by providing all the tools and information about the BCP Program

Plan Owners / Incident Commanders

- Responsible for the development, approval and distribution of plans
- Verifying plan recovery strategies are implemented, maintained and exercised
- Obtaining on-going training and education necessary to design, implement and maintain their business continuity plans
- Assigning Plan Builders (subject matter experts) with the breadth of knowledge of the plan unit operations to support the development and maintenance of plans
- Communicating BCP risk and issues to the functional group Executive Sponsor and BCC
- Mitigating unacceptable risk in plan vulnerabilities
- Revising plan(s) as business conditions require (i.e., changes in roles, environment, technology, and operations)

- Activate plans when pre-defined triggers have been met and recover the critical activity within its recovery time objective.

Plan Builders

- Supporting Plan Owner in developing and maintaining plan in LDRPS (planning repository)
- Assisting Plan Owner with any maintenance, exercise, and QA activities

Audit and Quality Assurance Services

- Review of the BCP Program or planning for compliance with the Corporate BCP Policy

GLOBAL BUSINESS CONTINUITY PROGRAM

The Program is a holistic process designed to provide a methodology for identifying and assessing threats and hazards, understanding their impacts to Level 3 operations, and developing a framework for planning and responding to unavoidable disruptions. The components of the Program are outlined here:

Program Management

Program Accountability: Program management is the heart of the BCP Program. Accountability of the Program is held at the senior management level so it receives the proper focus and alignment with enterprise priorities for a successful implementation. Program management includes making sure goals have been met and providing for a continual review of the Program to ensure its continuing suitability, adequacy and effectiveness.

Resource Commitment and Training: Based on the results of the BIA and Risk Assessment, management commits the resources to execute the Program and makes sure they are trained and competent. The Program utilizes role-based training modules to train its employees. The instructional modules are designed to provide training on the Program objectives as well as an explanation of how to complete the tasks to meet the requirements.

Embed BCP into Culture: The participation of senior management is key in making sure that the BCP Program is correctly introduced, adequately supported and is properly embedded as part of Level 3's culture.

Understanding the Business

Business Impact Analysis (BIA): A BIA is conducted to identify the impacts resulting from business interruptions and provide the criteria to quantify and qualify those impacts to determine what is most critical to our operations. This analysis identifies time-critical functions, their recovery priorities, and interdependencies so recovery time objectives can be established and approved. This data then drives the priorities for continuity planning and developing/implementing recovery strategies and solutions to support the recovery time objectives.

Risk Assessment: A Risk Assessment is conducted to evaluate the threats and hazards and identify potential causes of interruptions, the probability of their occurrence, their severity and their impact when they do occur. Measures can then be identified to reduce the probability of occurrence or reduce the impact of an incident.

Risk Management: After the risk to operational disruptions is assessed and understood, Level 3 evaluates the risks and impacts it can control or influence. Management can then make informed decisions on managing unacceptable levels of risk.

Determine Strategies

Strategy Development and Implementation: The results from the BIA and Risk Assessment are used to assess and implement appropriate strategies to reduce the likelihood and impacts of incidents or disruptions. This requires identifying continuity strategies that will improve Level 3's resiliency to a disruption by ensuring critical activities continue at, or are recovered to, an acceptable level and meet agreed upon recovery timeframes. The strategies define the required resiliency solutions so that controls around incident prevention, detection, response, recovery and restoration are put into place.

Vendor Resiliency Management: Level 3 analyzes the resiliency of its vendors that support critical functions/processes, facilities, and systems to proactively manage unacceptable levels of risk.

Develop and Implement Response

Incident Management Response Structure: Level 3 employs a multi-layer scalable response structure to efficiently respond to disruptions that span its global operations.

Plan Development: Level 3's resiliency planning concentrates on sustaining its critical business operations and its supporting infrastructure (i.e., network, people, systems, facilities, vendors, etc.). Planning focuses on the impacts that could be caused by any scenario and provides the procedures for maintaining the continuity of operations.

Level 3's BCP Program includes the following suite of plans:

- Enterprise Business Continuity Plan – Company overarching strategies
- Crisis Management Plan – protect Company brand
- Incident Management Plans – provide command, control and coordination over recovery teams
- Business Continuity Plans – continue critical operations
- Facility Recovery Plans – recover critical infrastructure of facilities
- Application Recovery Plans – recover applications
- Pandemic Plans – recovery of influenza outbreaks

Exercising, Maintaining and Reviewing Response

Exercise and Maintenance: Business continuity and incident management planning is annually exercised and maintained to validate their viability. Level 3 exercises its plans to develop teamwork, competence, and confidence among its recovery teams. Plans are maintained in a state of readiness.

QA Reviews: To maintain a consistent level of Program execution, Level 3 conducts QA reviews on planning.

Post-Event Review: Level 3 assesses its response to and recovery from events to measure the effectiveness of its response and recovery capabilities. Post-event reviews provide the impacted/activated groups with an opportunity to seek feedback on their recovery and their incident management performance. A summary of the event incorporates any corrective actions for improvement which become part of ongoing detection, analysis, and elimination of actual or potential causes of disruptions.

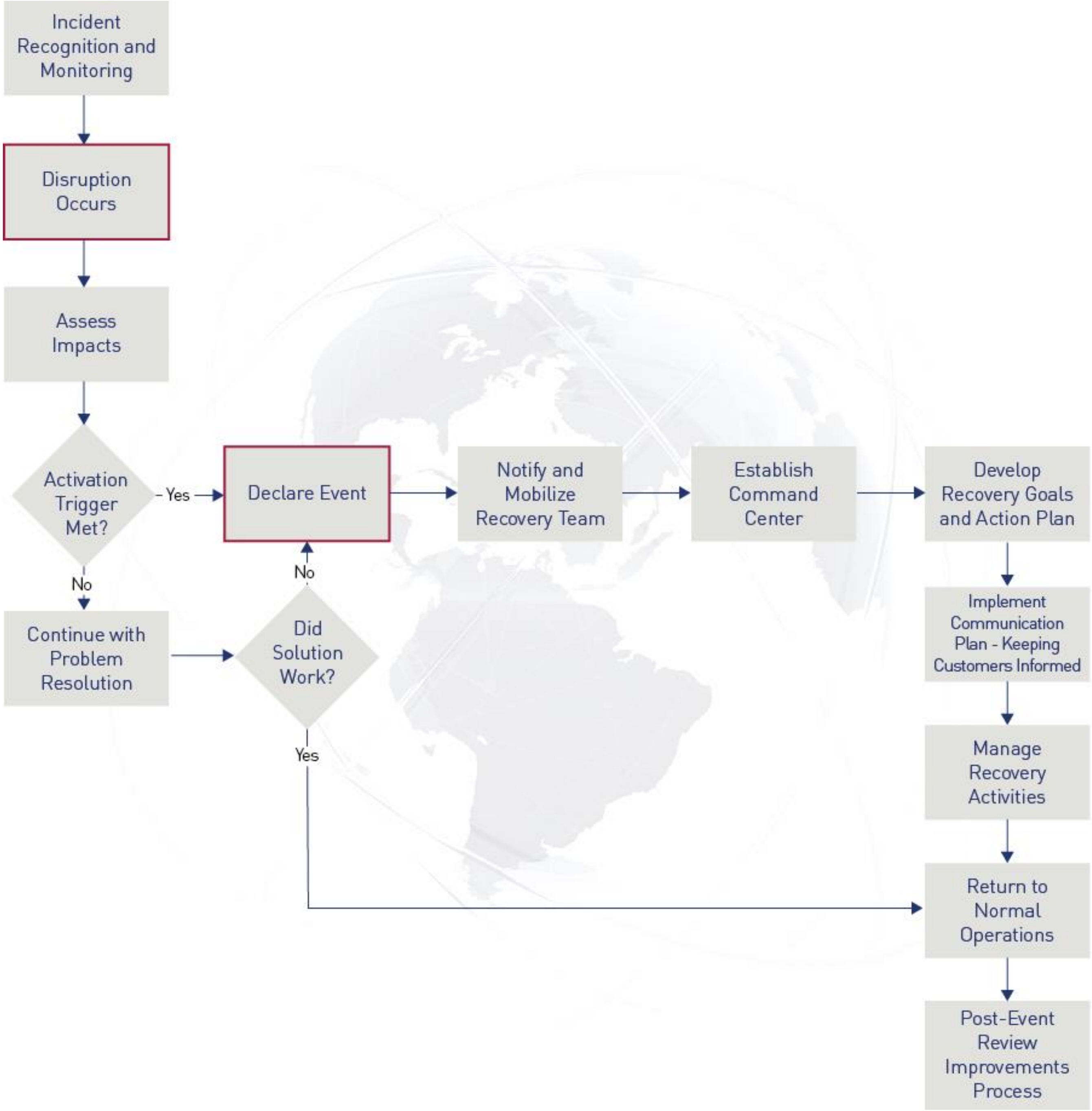
Standards and Practices

Level 3 utilizes the following standards for modeling its BCP Program:

- British Standards Institution (BSI), BS 25999: "25999-1:2006 Business Continuity Management. Code of Practice" and "BS 25999-2:2007 Specification for Business Continuity Management"
- British Standards BS ISO/IEC 27031:2011: "Information Technology – Security techniques – Guidelines for information and communication technology readiness for business continuity"
- International Standard ISO 22301: "Societal security – Business continuity management systems – Requirements"
- American Society for Industrial Security (ASIS) "Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery"
- American Society for Industrial Security(ASIS) /British Standards Institution (BSI) ASIS/BSI BCM.01-2010 "Business Continuity Management Systems: Requirements with Guidance for Use"
- NFPA 1600: "Standard on Disaster/Emergency Management and Business Continuity Programs" 2013 Edition
- NIST Special Publication 800-34 Rev 1. "Contingency Planning Guide for Federal Information Systems"
- BSI PAS 200:2011: "Crisis Management – Guidance and Good Practice"
- The Homeland Security Exercise and Evaluation Program (HSEEP)
- Disaster Recovery International Institute: "Professional Practices for Business Continuity Practitioners"

CONCEPT OF OPERATION – RESPONSE AND RECOVERY

Level 3 utilizes the following process for monitoring, declaring and managing recovery from events. Keeping our customers apprised of unavoidable disruptions is a high priority when triggered events require us to implement a communication plan.


Incident Recognition and Monitoring
Disruption Occurs
Assess Impacts
Activation Trigger Met?
Yes
Declare Event
Notify and Mobilize Recovery Team
Establish Command Center
Develop Recovery Goals and Action Plan
No
Continue with Problem Resolution
No
Did Solution Work?
Yes
Implement Communication Plan - Keeping Customers Informed
Manage Recovery Activities
Return to Normal Operations
Post-Event Review Improvements Process

RESILIENCY AND PREPAREDNESS CAPABILITIES

Level 3’s preparedness capabilities and strategies include, but are not limited to:

Level 3 Network

The Level 3 network is fully route-diverse and is designed with complete “ring” protection. This design helps ensure that our protected services are fully path-redundant and are not susceptible to outages. The core design characteristic driving Level 3’s high-level of network reliability is geographic network diversity. Each city along the network is served by two, or in some cases three, diverse paths, thus ensuring that a fiber cut along any one route will not isolate a city from the network, ensuring continuity of service.

Network Operating Centers

Redundant Network Operating Centers (NOCs) geographically disbursed enable Level 3 to identify and isolate causes of potential network disruptions, and quickly coordinate resolution of system outages.

Network Facilities

All critical facilities have plans for recovering their critical infrastructure from loss of access, power, HVAC or employees, etc. We also conduct evacuation drills to protect the life safety of our employees, customers and vendors.

Network Security

Level 3 is dedicated to providing you with 24 x 7 business continuity. Thanks to the size and sophistication of our global network, we have access to a massive amount of security threat data, enabling us to help protect you from attacks before they affect your business.

Technical Support Centers

Technical Support Centers are geographically disbursed and staffed 24 x 7 to provide dedicated support to our customers.

Data Centers

Alternate Processing Site: Level 3 owns and self-manages a geographically dispersed alternate data center, which is utilized when the primary processing capabilities are not available. The alternate data center is a hot site that is comparable in size, power capacity, and HVAC capacity to the primary data center. The alternate data center is equipped with the infrastructure, environment and connectivity to support recovery of its critical systems and applications for essential business functions within their recovery time objectives.

Alternate Storage Site: Numerous data replication strategies are employed by Level 3 to manage data storage in a safe and secure manner. Data from our primary data center may be replicated through various technologies to repositories located in our self-managed, geographically dispersed backup data centers. This capability facilitates meeting our recovery time objectives, and mitigates risk of physical access and retrieval of backup information.

Information System Backup: Level 3 has implemented a hot standby solution in its alternate processing and storage site. Periodic testing is conducted on media reliability and information integrity.

Information System Recovery: System recovery is sequenced based on the criticality of the functions the information systems support and the recovery time objectives and recovery point objectives defined by the business. Each information system's failover capability utilizes recovery solutions designed to meet those recovery objectives.

Supply Chain/Critical Vendors

Level 3 critical vendors and suppliers are asked to demonstrate their business resiliency capabilities. This provides Level 3 the ability to manage any risk to their supply chain. Level 3 incorporates its partners in its exercise program.

Pandemic Preparedness

Level 3 recognizes its responsibility to our employees, customers and shareholders to minimize the potential for business disruption and recover operations as rapidly as possible should a disruption occur as a result of a pandemic outbreak. Through effective, ongoing preparation and planning, Level 3 employees are provided with public and private resources to enhance awareness and recommend precautions.

Level 3 maintains both Global and Business Unit Pandemic Influenza Plans, which are integrated into its Business Continuity Program. Pandemic preparedness focuses on:

- 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

Communications

Backup Communications: Level 3 has implemented redundant communications capabilities utilizing alternate carriers. Primary and backup conference bridges are supplied by separate vendors using diverse networks and routes. An automated paging system, utilized for notifying and communicating during an event, is also geographically redundant.

Remote Network Access: Level 3's network security architecture allows near-immediate and sustained remote access into our internal network to access critical applications and data through any ISP, regardless of provider.