SCTE · ISBE

STANDARDS

Network Operations Subcommittee

SCTE OPERATIONAL PRACTICE

SCTE 206 2021

Cable Operator Business Continuity and Disaster Recovery Operational Practices

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interoperability, interchangeability, best practices, and the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at https://scte.org.

140 Philips Road
Exton, PA 19341

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Executive Summary

This operational practice outlines a study of best practices to create and maintain a suitable disaster response plan which prepares for an effective response to natural and man-made disasters that may result in regional and potentially national service outages. The primary goals of an effective plan include minimization of mean-time-to-repair and rapid response based upon selected criteria.

1.2. Scope

The scope and primary objectives are to:

1. Define a business continuity plan (BCP) – outline what the components are
    a. Proactive planning: Identify the best practices to help mitigate customer impacting outages
    b. Reactive planning: restoration of service based on incident (disaster recovery (DR) plan)
2. Plan documentation, exercises, and maintenance
3. Improve understandings of cable operations for local offices of emergency management (OEM)
4. Outline threats to cable operations
5. Tools of BCP programs
6. Identify Incident Management Structure leveraging NIMS framework

1.3. Benefits

Cable operators play a vital role in every community and during times of need such as man-made or natural disruptions to day to day life, it is important for our industry to have proper plans to help minimize service disruption. Communication is vital to the restoration process for communities in need. Without proper continuity plans, times to restore can be delayed. Business continuity plans help cable operators review and optimize processes and procedures for dealing with incidents. The long-term advantage for having proper business continuity plans identified and exercised include brand confidence by subscribers, marketplace advantages and possibly regulatory avoidances. Through standards and best practices such as this publication, cable operators can optimize approaches for dealing with all-hazard risks.

1.4. Intended Audience

Cable operator business continuity employees and individuals involved with ensuring customer experience is optimized during time of incident.

1.5. Areas for Further Investigation or to be Added in Future Versions

None at time of publication.

2. Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to

investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1. SCTE References

- No normative references are applicable.

2.2. Standards from Other Organizations

- No normative references are applicable.

2.3. Published Materials

- No normative references are applicable.

3. Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

3.1. SCTE References

- SCTE 226 Cable Facility Classification Definitions and Requirements
  https://scte-cms-resource-storage.s3.amazonaws.com/Standards/ANSI_SCTE%20226%202015.pdf

3.2. Standards from Other Organizations

- International Organization for Standardization (ISO) 22301
  Societal security -- Business continuity management systems --- Requirements
  https://www.iso.org/standard/75106.html.
- Standard on Continuity, Emergency, and Crisis Management
  https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
- ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, And Continuity Management Systems - Requirements With Guidance For Use
  https://webstore.ansi.org/standards/asis/asisspc2009

3.3. Published Materials

- Business Continuity Institute
  http://thebci.org
- DRII (Disaster Recovery Institute International) Ten Professional Practices
  https://drii.org/resources/professionalpractices/EN
- Business continuity management. Code of practice
  http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030157563&rdt=wmt
- National Infrastructure Protection Plan
  http://www.dhs.gov/national-infrastructure-protection-plan
- Strategic National Risk Assessment (SNRA)
  http://www.dhs.gov/strategic-national-risk-assessment-snra

- FEMA National Incident Management System https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf

4. Compliance Notation

shall	This word or the adjective "***required***" means that the item is an absolute requirement of this document.
shall not	This phrase means that the item is an absolute prohibition of this document.
forbidden	This word means the value specified shall never be used.
should	This word or the adjective "*recommended*" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighted before choosing a different course.
should not	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
may	This word or the adjective "*optional*" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.
deprecated	Use is permissible for legacy purposes only. Deprecated features may be removed from future versions of this document. Implementations should avoid use of deprecated features.

5. Abbreviations and Definitions

5.1. Abbreviations

ASIS	American Society for Industrial Security
BCI	Business Continuity Institute
BCM	business continuity management
BCMS	business continuity management system
BCP	business continuity plan
BSI	British Standards Institute
DR	disaster recovery
EOC	emergency operations center
DRII	Disaster Recovery Institute International
FCC	Federal Communication Commissions
FEMA	Federal Emergency Management Agency
HFC	hybrid fiber coax
ISO	International Organization for Standardization
MSO	multiple system operator (cable company)
NFPA	National Fire Protection Association
OEM	office of emergency management
SNRA	Strategic National Risk Assessment

5.2. Definitions

data center	A critical facility for housing computers, data storage, network transport and associated components to support service delivery, customer facing applications and back office automation.
headend	A critical cable facility that is primarily used for receiving video signals for processing and distribution to an operator's core network.

6. Why BCP/DR For Cable Operators

The way society accesses information has changed dramatically since the late 1940s when the cable TV industry was born. No longer are people and businesses waiting for information to arrive via radio, TV, or printed media such as newspaper, magazines and other pre-digital media. Today, with the explosion of the Internet, video-on-demand, and mobility via various devices, cable's reach is very dynamic, encompassing millions of homes in all 50 states and around the world.

The expansion of the cable service network beyond its roots in video service places a new paradigm on the value of the network. No longer an entertainment subscription service to achieve better TV reception and avoid having to put antennas on rooftops or rabbit ears on TV sets, businesses and individuals alike have come to expect an always-on service, opening the gateway to high-speed Internet access (often referred to as broadband), telephony AND television service. This expanded model for cable enables critical needs of our customers such as 911 and/or e911, home medical monitoring and home security, up-to-the-minute news alerts, banking, and cell tower backhaul service for our wireless infrastructure. The criticality of our service is fully realized during times of crisis, such as severe weather or other natural disasters. Both responders and those impacted by these events need to be able to seek aid or critical information when and where they need it in a timely manner.

With the combination of cable's reach to a broad customer base, and the new business risk profile changing, it is important to take a moment and understand the absolute fundamentals of how the technology comes together to make modern services possible. The cable industry's infrastructure is geographically diverse. Physical buildings, from data centers, to master headends, headends, hub sites, nodes, and the customer premise are all linked via a hybrid fiber coax (HFC) cable system and/or fiber optic cable. These buildings require planning and management regarding power/electricity, service provisions and proper environmental management to ensure each facility stop along the way is uninterrupted. A cable operator's facilities can span hundreds if not thousands of miles from the point of service origin to the end user – be it Internet access, TV programming or telephone service. When service is interrupted, where in the geography the interruption occurs determines how many customers will not have access to their subscribed services.

How does the service travel from point-to-point through the cable operator's facilities and ultimately to the customer's premise? Hundreds or even thousands of miles of distributed cabling called "outside plant" and its connected equipment – amplifiers, power supplies, taps, drops, and Wi-Fi access points – require electricity along the way. This electricity is typically provided by an electrical utility partner in the geographic region. Similar in nature to the electrical distribution lines, cable service will typically run facility-to-pole, pole-to-pole, pole-to-underground, underground-to-pole, and pole-to-customer. In overhead plant, the cable service is usually located between the telephone (the lowest cables on the poles) and the electrical utility's lines at the top of the poles. Amplifiers in the cable service are in-line with the coaxial cable along the path to the customer premise. Power supplies are often mounted in cabinets attached to utility poles or on the ground in appropriate weather-resistant cabinets. When power is

disrupted, battery-equipped standby power supplies provide electricity to the network for up to a few hours. It is also worthy to note that some of these cabinets may have the presence of natural or liquid propane gases. For lengthy outages, backup generators may be taken to the affected location, secured, fueled and operated to provide the necessary voltage to the amplifiers. The customer drop is the location of service entry to the building. Using this technology, multiple services can be delivered over a single cable. When natural disasters such as winter storms, hurricanes, and other events occur, the outside plant requires employees to be ready for service restoration.

A wide array of customer services travel through a cable system's core facilities, including hubs, headends, and data centers. Commercial customers such as financial institutions, healthcare providers, and educational institutions such as colleges, universities, and high schools all depend on cable's voice, data and video products somehow touching each of these facilities. During power grid challenges due to whatever cause, cable's facilities will require essential fuel for backup generators to keep these services available to both commercial and residential customers trying to access information, communicate, or maintain normalcy.

When utility poles are knocked down, iced over, or otherwise damaged, resulting in the cable company's equipment also being damaged, it is up to the cable professional to safely restore service once the poles have been replaced, most commonly by the power or telephone company. A critical piece of this operation is the coordination with the local municipalities in charge of clearing debris. Without coordination efforts or close partnership, there is the risk of additional damage to cable plant resulting in longer than necessary restoration times, or disruption of services to critical facilities, such as hospitals or other first responder entities. Another important partnership in the communication channel is the electrical utility; as mentioned earlier, the cable plant depends on electricity. If there is no power either from the utility, standby power supply, or local backup generator, all of the cable services will be unavailable. From the cable operator's perspective, the restoration process typically should not require days or even hours of research looking for where the damage lies, as the advancement in networking technology provides the operator remote insight to where the customer-impacting damage is. Advanced network communications provide 24x7 status monitoring of network operations. During "blue sky days" cable, utility, and municipalities can define scenarios for both communication and restoration procedures for various scenarios. Further, it is strongly recommended that cable providers and electrical providers ensure they have a correct and accurate understanding of their interdependencies. An example may be the circuit number from the power provider and an in dept analysis of which power supply it controls from the cable provider.

In the new hyper-connected, data-driven, instantaneous access-to-information world, the importance of the cable network has exploded. Cable is both a huge enabler to AND provider of information to millions of customers. The partnerships and understanding formed by cable operator, utility provider and local municipality will ensure that when the services are needed the most or even disrupted because of unforeseen events; will help to expedite return to societal normalcy.

The BCP can serve as the roadmap to efficiently and cost-effectively restore the network, and overall business operations. This plan can protect a company's reputation, minimize exposure to regulatory risks, ensure continued revenue streams from residential and business customers, and avoid service level agreement or other contractual penalties.

In summary, cable providers should have business continuity plans to guide service restoration efforts, and these typically include access to the resources necessary to restore services. In large-scale service restoration, cable operators will sometimes need to look to local and state emergency management agencies for assistance in gaining access to damaged areas, for providing security to operate safely, and

for access to fuel. Cable companies stand ready to partner with local, state, and federal emergency management agencies.

7. Guiding Principles For Business Continuity and Disaster Recovery in Cable Networks

The overall guiding business continuity and disaster recovery principle for cable operators is to be proactive and plan to ensure products and services are operating as expected. In the face of an incident, a cable operator should be prepared with documentation and plans in place to execute the restoration of services as rapidly as possible. Well documented plans allow for companies to efficiently deal with stressful situations which include the potential of unavailability of critical personnel.

Business Continuity Management is defined in ISO 22301:2019 as 'the process of identifying potential threats to an organization's business operations', and as a process 'which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.' Cable operators ***should*** utilize ISO 22301 2019 as the baseline for creating a business continuity tool.

8. Incident Management Framework

8.1. Single Incident Commander

The NIMS ICS (Incident Command Structure) is a standardized approach to actively engage in the coordination, response, and recovery of planned or unplanned incidents. The ICS operates across multiple disciplines and enables incident managers from different functional groups to work together seamlessly. This structure includes five major functional areas, staffed as needed, for a given incident: Command, Operations, Planning, Logistics, and Finance/Administration. *Please note these section names can be modified to better align with an organizations Operational model.*

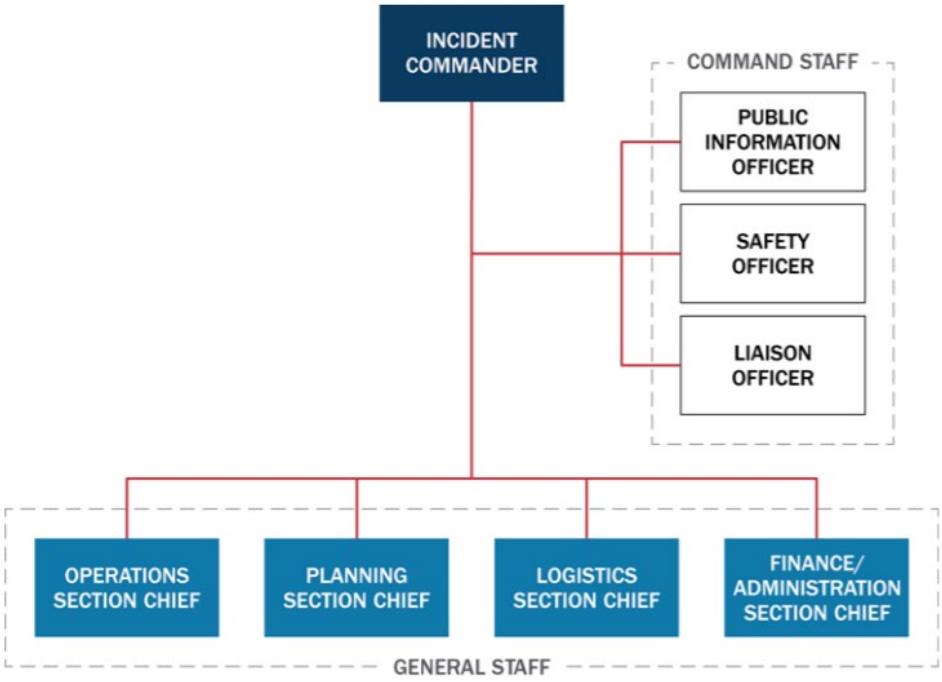

Figure 1- Example of an ICS Organization with a Single Incident Commander

8.2. Unified Command

The Unified Command uses a collaborative approach where individuals designated as an Incident Commander by authorities of their jurisdiction, organization or department, jointly determine priorities and objectives, allocate resources, and work together to execute integrated incident response efforts. Each member is expected to understand and communicate the priorities, capabilities and limitations of their particular department/area.

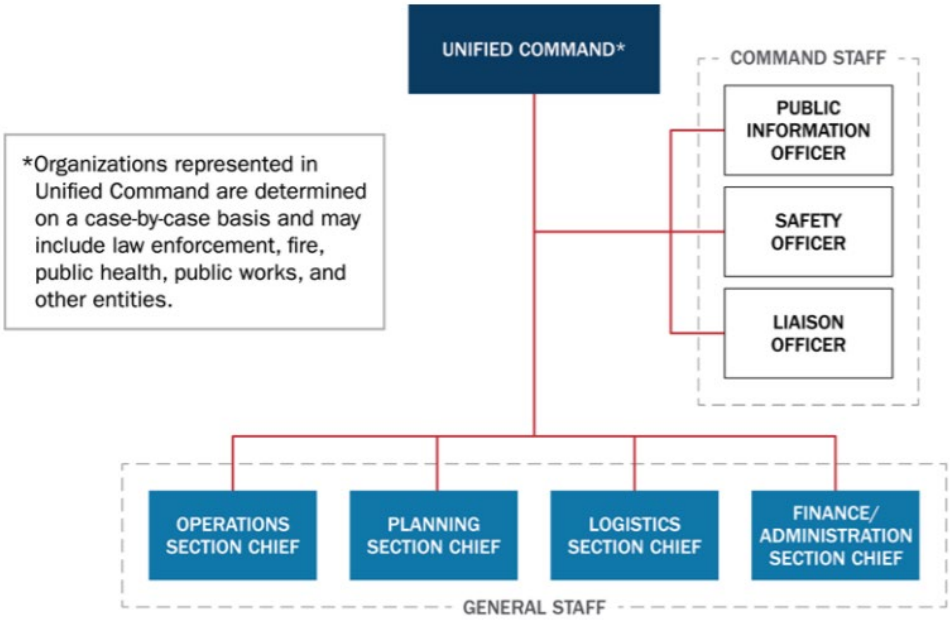

Figure 2- Example of an ICS Organization with Unified Command

9. Business Continuity Management System (BCMS) Life Cycle

Emergency preparedness, crisis management, business resumption and technology are core components of the business continuity management system. The BCMS life cycle is a powerful tool to help strengthen the overall readiness of the cable organization. The following found at https://bcmmetrics.com/ffiec-business-continuity-program/ is an excellent example of the various phases of the life cycle and is illustrated in Figure 3.

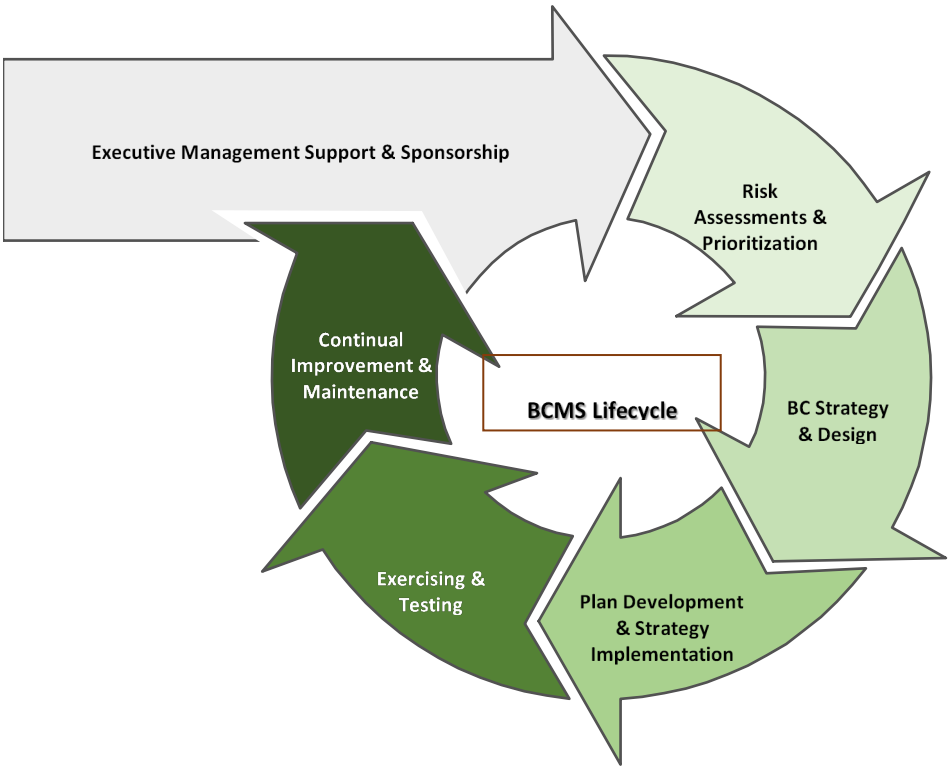

Figure 3- Business Continuity Management System Life Cycle

- **Phase 1 – Executive Management Support & Sponsorship**
  - Program maturity assessment and annual roadmap
  - Program budget and resource planning
- **Phase 2 – Risk Assessments & Prioritization**
  - Business impact analysis
  - Application impact and crown jewel analysis
  - Site and 3rd party risk assessment
  - Business dependency analysis
  - Technical dependency analysis
  - Business processes mapping to technical capabilities
  - Recovery gap analysis
- **Phase 3 – Business Continuity Strategy & Design**
  - Continuity and hosting strategy options
  - Business case and recommendation
  - Strategic roadmap development
- **Phase 4 – Plan Development & Strategy Implementation**
  - Recovery solution acquisition/build
  - Implement and enhance business and technical recovery capabilities
  - Resiliency plans
  - Incident response plan
- **Phase 5 – Exercise and Testing**
  - Pre-test
  - Conduct test
  - Post-test

- **Phase 6 – Continual Improvement & Maintenance**
  - Quality review and maintenance
  - Training and awareness
  - Communication plan
  - Metrics and compliance scorecard
  - Executive reporting
  - Change management

10. Threat Identification

A large portion of the planning work to ensure business as usual will be recognition of applicable threats to specific operations. This will vary from operator to operator based on size, location, public/private company etc., however there are some common threat scenarios that are shared across the cable community.

Examples of these threats include:

Table 1 - Business Threat List

NATURAL	MAN-MADE

• Blizzard
• Drought
• Dust storm
• Flooding
• Fire - wild, rural or urban
• Geological activities
  • Earthquake
  • Volcanic eruption
  • Landslide
  • Avalanche
  • Mudslide
  • Weathering
  • Erosion
• Heat wave
• Ice storm
• Lightning
• Pandemic or other disease
• Rain
• Snow
• Tornado
• Tropical storm (hurricane)
• Weather front
• Waterspout
• Wind
	Employee Impacting
	• Assassination/Inauguration
	• Basic services
	  • Health
	  • Security
	  • Safety
	  • Transportation
	• Biological
	• Bomb
	  • Bomb threat
	  • Explosion
	• Chemical
	• Food
	• Hijacking an individual, VIP or group
	• Individual behavior
	• Labor strikes
	• Mass behavior
	• Nuclear
	• Poisoning
	• Protests/Civil Unrest
	• Terrorism (domestic and foreign)
	• Wounding
	• Transportation accidents
	Technology

	• Cyber
	• Hardware malfunction
	• Hazardous materials related events
	  • During production
	  • During transportation by road, air, rail, pipeline and sea
	  • During storage
	• Information technology related events
	• Software malfunction
	• Supply chain disruption
	• Theft/vandalism
	• Utilities
	  • Communications
	  • Electricity
	  • Gasoline
	  • Natural gas
	  • Oil
	  • Water

11. Continual Improvement and Review

As business continues to change with both current and targeted customer landscape changes, so should the BCP/DR plan. Leveraging the framework outlined in ISO 22301, an operator can embed a plan, do check, act approach to optimize responses. This will help ensure the plan acknowledged by the cable operator is effective and reliable in returning the business back to normal.

Maintaining the Plan

Applying a compressive approach based on ISO22301 will serve as an effective tool and ensuring continual audit or testing of the content of the plan will help minimize customer impact during incident. This approach serves to not only update changes in personnel, vendors, and business processes, etc., but also provides the opportunity to improve the plan. Typically, the business continuity coordinator facilitates the update cycle, but the BCP teams who are closest to the business perform the changes. A proven approach encompasses a combination of periodic maintenance intervals, with special updates required when there are significant business or personnel changes. Documents where changes take place most frequently (internal contact lists, vendor lists, customer lists, for example) should be updated as required, and reviewed in their entirety annually. Documents that are more static could be modified semi-annually. One option would be to use seasonal triggers for maintenance intervals, such as onset of the hurricane season, or the beginning of winter. Any activation of the BCP should trigger an after-action review, which offers a significant opportunity for lessons learned and substantive changes to the plan.

Testing and Exercising the Plan

Through a program of tests and exercises, one can validate to the highest degree possible that the plan will be effective when called into use. There are several types of tests and exercises that can be performed, and these include training staff on the plan. It is recommended that the exercise program begin in a limited fashion and grown in complexity and scope over time. This allows for skill building and increases confidence in the plan. Test types include:

- **Checklist tests** – Verifying that copies of the plan documents are current and properly distributed, that emergency forms and supplies are present, etc.
- **Structured walk-through tests** – (i.e., table-top exercise) Detailed walk-through of the various components of the plan on a team or departmental basis.
- **Recovery simulations and/or functional exercise** – Teams use the plan, equipment, facilities and supplies just as they would in a real situation.

12. Conclusion

Business continuity plans have been credited with saving countless businesses from significant operational impacts, financial losses, and damage to corporate reputations. For cable operators, minimizing network disruptions, and quickly restoring service after a significant interruption is what customers count on to provide life's most important connections. Managing these situations requires detailed planning, and effective coordination with multiple outside organizations. Recognition of ISO 22301 in the Cable Operator Business Continuity and Disaster Recovery Recommended Practice provides the path to achieve these goals. Its comprehensive and full lifecycle approach promotes development of an all-hazards continuity planning framework. The lifecycle approach promotes not only the development of effective plans, but a continuous improvement methodology that fosters maturity of planning capabilities.