Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Network Operations Subcommittee

SCTE 206 2014

Cable Operator Business Continuity and Disaster Recovery Recommended Practices

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Recommended Practices (hereafter called documents) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE 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 members, whether used domestically or internationally.

SCTE 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 Standards.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE 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 web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

Acknowledgments

The information in the following recommended practices was produced with the help and support of the corporations and organizations listed below.

Alpha
Colt Recycling
Comcast
Cox Communications, Inc.
Metrocast
Rogers
Time Warner Cable

SCTE wishes to particularly thank the following people for their participation as chapter leads, which included numerous conference calls, writing, and review.

Derek	DiGiacomo	Society of Cable Telecommunications Engineers
Greig	Fennell	Comcast
Jim	Shortal	Cox Communications, Inc.
Joe	**Viens**	**Time Warner Cable [WORKING GROUP CHAIR]**
John	Hewitt	Alpha
Marty	Davidson	Society of Cable Telecommunications Engineers
Peter	Muscanelli	Colt Recycling
Randy	Evans	Metrocast

TABLE OF CONTENTS

1.0 SCOPE

This document outlines the recommended practices for the management of a cable operator's business continuity and disaster recovery planning programs. This recommended practice outlines a study of best practices to prepare for and respond to natural and man-made disasters that may result in regional and potentially national service outages. Goals include minimization of mean-time-to-repair and rapid response based upon selected criteria. The scope and primary objectives are to:

1. Define a business continuity plan (BCP) – outline what the components are
    - Proactive planning: Identify the best practices to help mitigate customer impacting outages
    - 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

2.0 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, 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. 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. 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. 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.

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.

3.0 INFORMATIVE REFERENCES

The following documents may provide valuable information to the reader but are not required when complying with this recommended practice.

3.1 Business Continuity Institute
http://thebci.org

3.2 International Organization for Standardization (ISO) 22301
Societal security -- Business continuity management systems --- Requirements
http://www.iso.org/iso/catalogue_detail?csnumber=50038

3.3 DRII (Disaster Recovery Institute International) Ten Professional Practices
https://drii.org/certification/professionalprac.php?lang=EN

3.4 NFPA 1600
Standard on Disaster/Emergency Management and Business Continuity Programs
http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600

3.5 BSI 25999
Business continuity management. Code of practice
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030157563&rdt=wmt

3.6 ASIS SPC.1
Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard
https://www.asisonline.org/Standards-Guidelines/Standards/published/Pages/Organizational-Resilience-Security-Preparedness-and-Continuity-Management-Systems-Requirements-with-Guidance-for-Use.aspx?cart=360b6f5d6238490bae8c8209f3e597b5

3.7 National Infrastructure Protection Plan
http://www.dhs.gov/national-infrastructure-protection-plan

3.8 Strategic National Risk Assessment (SNRA)
http://www.dhs.gov/strategic-national-risk-assessment-snra

4.0 COMPLIANCE NOTATION

"SHOULD"	This word or the adjective "RECOMMENDED" means that there may be 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.

5.0 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 22301:2012 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.'

6.0 PROCESS FOR "BUSINESS AS USUAL": BUSINESS CONTINUITY INSTITUTE (BCI) GOOD PRACTICE GUIDELINES 2013

The "*BCI Good Practice Guideline*"[1] is a recognized recommended framework for a cable operator's establishment of a business continuity program. The BCI Guideline includes six subject areas of focus that will serve as a basis for establishment of a program as an operator. The first two are rooted in management practices while the other four are technical action oriented practices.

1. **Policy and Program Management**: Defines the organizational policy relating to business continuity and how the policy will be implemented, controlled and validated through the program.

2. **Embedding Business Continuity**: Continuous activity resulting from the policy and program management phase of the guiding principles. This subject area for cable is natural as the industry has grown out of an attitude/culture of getting things done when faced with adversity. Having this culture and individual attitude is almost a prerequisite for being in the cable industry. Always look to opportunity to formalize this embedded attitude approach.

3. **Analysis**: Business impact analysis largely rooted in information gathering, the analysis area will be a form of feedback loop to check in with the objectives and how a cable operator functions in terms of environmental landscape. Operators should identify what their critical activities are and at what levels should the critical activities continue in a best attempt to maintain business as usual in the eyes of the customer. The analysis is rooted in the business impact analysis that looks to quantify and qualify impacts in time of loss, interruption or disruptions. This area of focus would also consider the regulatory landscape as it relates to the Cable Act, FCC Rules and

[1] Access the latest BCI Good Practice Guide : http://www.thebci.org/

Best Practices, and state and local franchise agreements. It is also important to factor in the documented resiliency requirements to do business with government entities at the local, state and federal levels, and with highly regulated industries such as banking and finance. Look to identify the threats to the business (see section 7).

4. **Design**: The crafting of the actions used to address the continuity and recovery strategies, threat mitigation measures and incident response structure. The design is heavily influenced from analysis findings.

5. **Implementation**: Rooted in the identification and documentation of priorities, procedures, responsibilities and resources needed to assist the operator in managing disruption. Implementation can be accomplished in parts to support the greater goal of total business continuity planning.

6. **Validation**: Ensure capability reflects the nature, scale and complexity of the operator it has been designed to support. Validation is achieved via table top exercises, maintenance cycles and review of plans.

7.0 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
	Employee Impacting
	• Assassination
	• Basic services
	  • Health
	  • Security
	  • Safety
	  • Transportation
	• Biological
	• Bomb
	  • Bomb threat
	  • Explosion
	• Chemical
	• Food

• Heat wave
• Ice storm
• Lightning
• Pandemic or other disease
• Rain
• Snow
• Tornado
• Tropical storm (hurricane)
• Weather front
• Water spout
• Wind
	• Hijacking an individual, VIP or group
	• Individual behavior
	• Labor strikes
	• Mass behavior
	• Nuclear
	• Poisoning
	• Protests
	• 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

8.0 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 Section 6, an operator should now turn to the ISO 22301 Plan, Do, Check, Act model for success (see Figure 1). This model will help ensure the plan acknowledged by the cable operator is effective and reliable in returning the business back to normal.

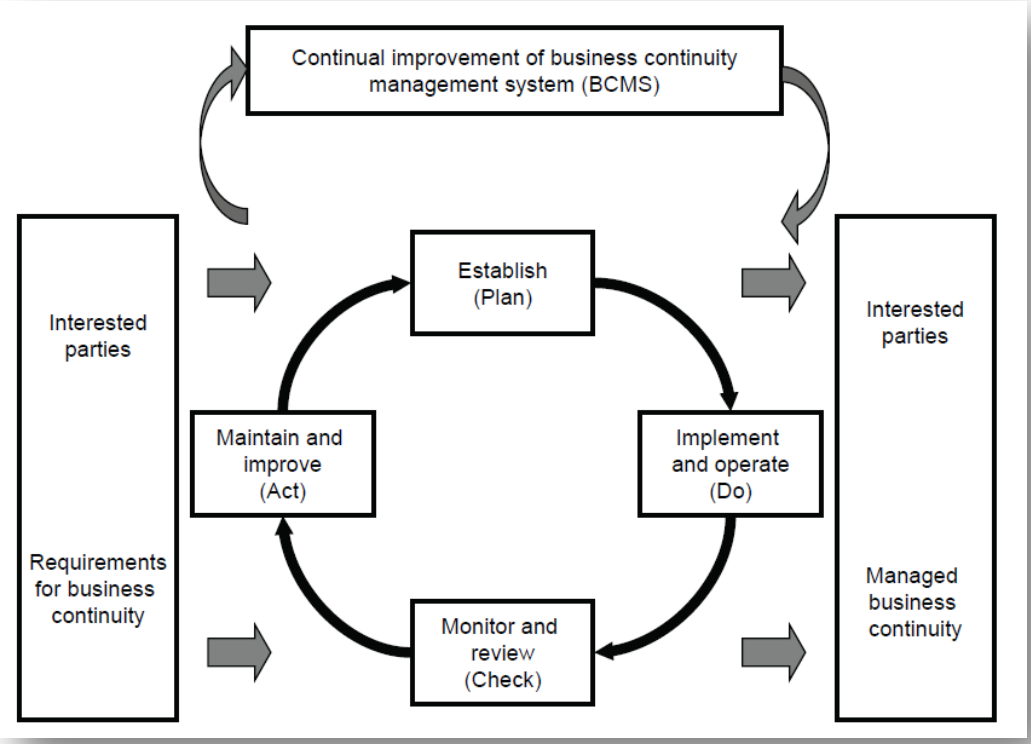

FIGURE 1 – ISO 22301 PLAN, DO, CHECK, ACT LIFECYCLE

The critical phases in the lifecycle defined in ISO 22301 include:

- **Plan**: Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organizations overall policies and objectives.

- **Do**: Implement and operate the business continuity policy, controls, processes and procedures.

- **Check**: Monitor and review performance against business continuity policy, and objects to report the results to management for review, and determine and authorize actions for remediation and improvement.

- **Act**: Maintain and improve the business continuity management system (BCMS) by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Maintaining the Plan

Applying the Plan Do Check Act model to the cable industry, and in order to serve as an effective tool, the business continuity plan must be continually maintained. This 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.

9.0 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 Plan Do Check Act model promotes not only the development of effective plans, but a continuous improvement methodology that fosters maturity of planning capabilities.

10.0 APPENDIX A: ABBREVIATIONS AND ACRONYMS LIST

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
DRII	Disaster Recovery Institute International
FCC	Federal Communication Commissions
ISO	International Organization for Standardization
MSO	multiple system operator (cable company)
NFPA	National Fire Protection Association
NIPP	National Infrastructure Protection Plan
OEM	office of emergency management
SNRA	Strategic National Risk Assessment