Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Network Operations Subcommittee

SCTE OPERATIONAL PRACTICE

SCTE 227 2016

Cable Operator Location Risk Assessment Operational Practice

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) 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, 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.

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 documents.

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.

Table of Contents

Title   **Page Number**

List of Tables

Title   **Page Number**

1. Introduction

1.1. Executive Summary

A location risk assessment (LRA) is performed to identify threats that could negatively impact the ability to conduct business in a geographic location. The results of the LRA help to align strategic business decisions with effective risk reduction solutions at a geographic location. The LRA considers all threats whether they are financial, natural, political or human related. The LRA identifies and weighs the risks to business continuity based on a four-step process.

The four steps are:
1. Strategic risk assessment
2. Tactical risk assessment
3. Strategic and tactical risk assessment report
4. Project evaluation matrix

The purposes of performing the LRA are to:
- Determine if it is appropriate to do business in a specific geographic location,
- Identify probable threats to the business within the specific geographic location,
- Determine the financial exposure to the company *should* the probable threats occur, and
- Determine cost effective solutions to mitigate or minimize the risks.

The scope of the location risk assessment applies to all areas of the cable operator business that would impact operations based on locational considerations. Also, third party facilities such as co-location facilities, an LRA *should* be conducted.

These steps are guides for determining the overall risk assessment for a location. Depending on the particular cable operator project all steps *may* not be required.

The information learned from the strategic, tactical and location risk assessments will be summarized by category on the strategic and tactical risk assessments report. Based on the narrative issues an overall rank will be determined and assigned for an overall risk assessment. The overall risk assessment rank and reason for ranking will be transferred to the project evaluation matrix.

1.2. Benefits

LRA provides a basis for an informed business continuity plan. Cable operator's networks provide entertainment, communication and information services and therefore are a valuable asset to the community service it resides. Having a location risk assessment defined will enable cable operators make the best choices for planning how to mitigate threats that are location driven or dependent. Without a proper location risk assessment, recovery times during incidents could be prolonged and thus impact speeds at which the customer can resume use of services. Finally as an industry, cable operators will be more prepared in time of need based on location dependent concerns and ultimately aid in the improvement of customer satisfaction.

1.3. Intended Audience

Senior management of a business unit *should* initiate and sponsor the risk assessment and involve all key business units and stakeholders. Depending on the type of business risk assessment to be completed, the senior management of the business unit or location will assign project members to the risk assessment team. The strategic risk assessment team *should* be composed of representatives from the initiating business unit, and the finance and business development departments. Once the strategic risk assessment

is completed and the project is determined viable to pursue, other groups *may* be brought in to complete the tactical risk assessments.

The risk assessment team is responsible for completing the business risk assessment and making recommendations to the senior management of the business unit. The overall risk assessment becomes part of the decision matrix for approving the capital expense request.

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

Periodically the Federal Emergency Management Agency (FEMA) will redraw flood plain maps or insurance brokers and underwriters *may* update guidelines necessary for review under the LRA process. Crime statistics and zoning rules *should* also be reviewed. Development of a formal risk committee to address the comprehensive risk list as outlined in SCTE 206 2014 Cable Operator Business Continuity and Disaster Recovery Recommended Practices.

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.

- 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 206 2014 -- Cable Operator Business Continuity and Disaster Recovery Recommended Practices
  http://www.scte.org/documents/pdf/Standards/SCTE%20206%202014.pdf

3.2. Standards from Other Organizations

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

3.3. Published Materials

- No informative references are applicable.

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

ADA	Americans with Disabilities Act
BCI	Business Continuity Institute
FEMA	Federal Emergency Management Agency
ISO	International Organization for Standardization
IT	information technology
LRA	location risk assessment
N/A	not applicable
PCBs	polychlorinated biphenyl
ROI	return on investment
SCTE	Society of Cable Telecommunication Engineers

5.2. Definitions

narrative	Explains and justifies the ranking in a risk assessment
operating principles	Examines practices for alignment of activities to core strategic plans that define the foundation of how a company operates
recovery plan	Documented plan by an organization that will insure its recovery and continuity in the face of a disaster or other major outage
risk analysis	Progression from a risk assessment to quantify threats to an organization, the probability of them being realized and impacts to the organization

| risk assessment | Identification quantification, and prioritization of threats that could dramatically impact an operation, to include but not limited to technology, location, vendor, and process |

6. Four Steps to Location Risk Assessment

The following for steps are executed to perform a cable operator location risk assessment.

6.1. STEP 1: Strategic Risk Assessments

Strategic Assessments: These assessments are made either when deciding to do business in a foreign country or when assessing the viability of doing work in a specific state within the United States. They assess the overall stability of doing business in that country or state and identify any strategic risk exposures to the company in pursuing the business venture. The strategic assessments are:

RISKS
- Country or political risks
- Financial risks
- Operational risks
- Technology risks
- Human capital

DEPARTMENTS
- Government affairs
- Finance
- Business unit management
- Engineering
- Human resources

The analysis tools used by the departments to perform the risk assessments are developed and maintained within the specific departments.

The strategic risk assessments are the first step in considering a new business venture and *should* be performed prior to any of the other risk assessments being completed. A ranking of 0 to 5 is assigned to each completed assessment along with any narrative issues uncovered by the department responsible for completion of the assessment. The ranking identifies the degree of risk or exposure to the company based on the following descriptions:

Table 1 - Strategic Risk Description

RANK	STRATEGIC RISK DESCRIPTION
0	No identified risk
1	Slight risk, but will not materially jeopardize the success of the venture or have significant strategic exposure to the company.
2	Slight risk to the success of the venture but without significant strategic exposure to the company.
3	Moderate degree of risk to the success of the venture with some strategic exposure to the company.
4	High degree of risk to the success of the venture with moderate strategic exposure to the company.
5	High degree of risk to the success of the venture with significant strategic exposure to the company.

The ranking for all the strategic risk assessments and narrative issues are summarized on the strategic and tactical risk assessment report (Step 4).

Once the strategic risk assessments have been performed and the issues identified and there is still a desire by the company to continue exploring the business venture, then the tactical risk assessments *should* be performed.

6.2. STEP 2: Tactical Risk Assessments

These risk assessments evaluate any potential environmental, security, technological, or other risks associated with doing business in a specific foreign or domestic location. The tactical risk assessments can include but is not limited to:

RISKS
- Environmental risks
- Loss control & property risk
- Security risks
- Technology risks

DEPARTMENTS
- Engineering
- Risk management/business units
- Corporate security

These identified departments *should* complete the tactical risk assessments prior to conducting any new business in the geographic location. Each of the risk assessments evaluates specific business concerns associated with conducting work at the location. Depending on the nature of the business venture or the work to be performed at the location, not all the risk assessments *may* need to be completed.

The analysis tools used by the departments to perform the risk assessments are developed and maintained within the specific departments with copies distributed to the appropriate corporate support group.

A ranking of 0 to 5 is assigned to each completed assessment along with any narrative issues uncovered by the department responsible for completion of the assessment. The ranking identifies the degree of risk or exposure to the company based on the following descriptions:

Table 2 - Tactical Risk Assessment Ranking

RANK	TACTICAL RISK DESCRIPTION
0	No identified risk
1	Slight risk, but will not materially jeopardize the success of the venture or have significant Tactical exposure to the company.
2	Slight risk to the success of the venture but without significant Tactical Risk exposure to the company.
3	Moderate degree of risk to the success of the venture with some Tactical Risk exposure to the company.
4	High degree of risk to the success of the venture with moderate Tactical Risk exposure to the company.
5	High degree of risk to the success of the venture with significant Tactical Risk exposure to the company.

The ranking for the tactical risk assessments and narrative issues are summarized on the strategic and tactical risk assessment report (Step 4).

6.2.1. Physical Risk Assessment Factors and Worksheets

The physical risk assessment factors tool is used to identify risks that could negatively impact a physical location. The physical risk assessment factor identifies and weighs the threats to a location. The risks are

classified in such key areas as environmental, health, safety, technology, economic, natural, political and human related risks.

- The physical risk assessment factors provides for a narrative explanation concerning the risk and ranks the risk from 0 to 5.

A ranking of 0 to 5 is assigned to each completed assessment along with any narrative issues uncovered by the department responsible for completion of the assessment. The ranking identifies the degree of risk or exposure to the company based on the following descriptions

Table 3 - Physical Risk Description

RANK	PHYSICAL RISK DESCRIPTION
0	No identified risk
1	Slight risk, but will not materially jeopardize the success of the venture or have significant physical risk exposure to the company.
2	Slight risk to the success of the venture but without significant physical risk exposure to the company.
3	Moderate degree of risk to the success of the venture with some physical risk exposure to the company.
4	High degree of risk to the success of the venture with moderate physical risk exposure to the company.
5	High degree of risk to the success of the venture with significant physical risk exposure to the company.

NOTE: The physical risk assessment factors tool is only meant to be a guide in helping facilitate discussion around potential risks faced at a location. You *may* determine that some risks, though ranking low on the physical risk assessment, merit mitigation and/or future planning to raise their ranking.

The purposes of performing the risk assessment factors are to:
- Identify threats for which situation response and business continuity plans can be prepared and tested;
- Evaluate the susceptibility of a location to the same "catastrophic" event for multiple critical facilities in the same area or region;
- Identify exposures and impacts from major human-made hazards, including vehicular/rail traffic (physical exposure and chemical release vapor clouds), air traffic flight paths, and or neighboring hazardous industrial processes. (inside or outside the premise);
- Select technical property where the first floor is at or above the 500 year level for flood exposure;
- Identify threats so improvements can be made to prevent or minimize the impact of the threat prior to the threat occurring. Changes to the current operating environment *may* be justified where probability and impact ratings are high

The results of the risk assessment factors are summarized in the strategic and tactical risk assessment report. (Step 4)

Provided on the next six pages are the worksheets for evaluating the risk assessment factors.

RISK ASSESSMENT FACTORS

Location_____

HUMAN & POLITICAL RISK ASSESSMENT	PROB*	PAST FREQ	BUS IMP*	NARRATIVE (Narrative description required if High or Medium Risks)	RANK (0-5)
Country Risks					
Brand image concerns					
Brand protection concerns					
Counterfeiting & trademark concerns					
Economic environment					
Environmental regulations					
Health & safety situation					
Human rights environment					
Labor pool & climate					
Legislative environment					
Political environment					
Regulatory environment (taxes, zoning, fines)					
Reporting					
Social environment					

Legend:
*PROBABILITY & *BUSINESS IMPACT

        H   **HIGH RISK - Contact risk management/security/business continuity**
        M   **MEDIUM RISK - Risk reduction strategy required**
        L   **LOW RISK**
        X   **N/A**

PAST FREQUENCY (list number of occurrences in last 10 years)

RISK ASSESSMENT FACTORS

Location_____

BUSINESS OPERATIONS	VALUE	YES	NO	NARRATIVE	RANK (0-5)
BUSINESS IMPACTS					
Building Asset Value					
Revenue Impact					
Business function only at this location					
Documented inventory list					
Documented recovery plan					
Geo-redundancy of applications					
Geo-redundancy of networks					
Loss of normal operations in excess of 30 days					
On-site storage of data					
Personnel skill set easily replaced with internal or external resources					
PROPERTY IMPACTS					
Building frame is steel or concrete					
Chiller/Cooling System					
Equipment near exterior walls					
Fire suppression system					
Fuel stored in building					
Hazardous materials stored in building					
Less than 20 feet from another building					
Many large glass windows					
Multi-story					
Multi-tenant					
Physical security at entrance					

RISK ASSESSMENT FACTORS

Location_____

LOSS CONTROL & PROPERTY RISK ASSESSMENT	PROB*	PAST FREQ	BUS IMP*	NARRATIVE (Narrative description required if High or Medium Risks)	RANK (0-5)
Natural Risks					
Fire/explosion or environmental release exposure from a neighboring site					
Drought					
Earthquake					
Flood > 500 year					
Hurricane					
Other wind damage					
Slide area					
Snow/ice storm or blizzard					
Tidal wave					
Tornado					
Volcano					
Collision Impact					
Air traffic flight patterns					
Train traffic					
Vehicle (intersecting highways)					
Building/Equipment Risks					
Fire					
ADA compliant					
Fire Protection/detection system					
Freezing/bursting of pipes					
Gas leaks					
Heating disruption					
Lighting non-compliance					
Power failure/fluctuation					
Roof Integrity					
Structural integrity					
Waste water treatment failure					

Legend:
*PROBABILITY & *BUSINESS IMPACT

    H   **HIGH RISK - Contact risk management/EPS/business continuity**
    M   **MEDIUM RISK – Risk reduction strategy required**
    L   **LOW RISK**
    X   **N/A**

PAST FREQUENCY (list number of occurrences in last 10 years)

RISK ASSESSMENT FACTORS

Location_____

ENVIRONMENTAL RISK ASSESSMENT	PROB*	PAST FREQ	BUS IMP*	NARRATIVE (Narrative description required if High or Medium Risks)	RANK (0-5)
Environmental Risks					
Asbestos/PCBs					
Community health risks					
Drinking water availability and source					
Endangered species/wetlands					
Ground/surface water contamination					
Hazardous material spill					
Indoor air quality					
Lead based paint exposure					
Municipal sewer system issues					
Offsite contamination					
Onsite contamination					
Proximity to former/existing landfills					
Proximity to hazardous manufacturing					
Underground tanks					

Legend:
*PROBABILITY & *BUSINESS IMPACT
      H   **HIGH RISK - Contact risk management/EPS/business continuity**
      M   **MEDIUM RISK – Risk reduction strategy required**
      L   **LOW RISK**
      X   **N/A**

PAST FREQUENCY (list number of occurrences in last 10 years)

RISK ASSESSMENT FACTORS

Location_____

SECURITY RISK ASSESSMENT	PROB*	PAST FREQ	BUS IMP*	NARRATIVE (Narrative description required if High or Medium Risks)	RANK (0-5)
Human Risks					
Bomb threat					
Burglary/theft					
Embezzlement/fraud					
Kidnapping/extortion					
Labor dispute/strikes					
Robbery					
Sabotage					
Supplier/vendor strike					
Terrorism					
Transit/hijacking					
Unauthorized physical access					
Vandalism/malicious mischief					

Legend:
*PROBABILITY & *BUSINESS IMPACT

    H   **HIGH RISK - Contact risk management/corporate security/business continuity**

    M   **MEDIUM RISK – Risk reduction strategy required**

    L   **LOW RISK**

    X   **N/A**

PAST FREQUENCY (list number of occurrences in last 10 years)

RISK ASSESSMENT FACTORS

Location_____

INFORMATION TECHNOLOGY RISK ASSESSMENT	PROB*	PAST FREQ	BUS IMP*	NARRATIVE (Narrative description required if High or Medium Risk)	RANK (0-5)
Technical Risks					
Application concerns					
Critical application failures					
Current itemized listing of equipment at location					
Ease of equipment replacement					
Electromagnetic interference					
External telecommunications failures					
Internal telecommunications failure					
Legacy equipment concerns					
Malfunction or failure of technologies/networks					
Talent-expertise replacement					
Uniqueness of technologies					
Vendor support concerns					
Data Risks					
Computer virus concerns					
Data entry error					
Improper handling of data					
Malicious damage to data					
Malicious damage to equipment					
Malicious damage to network components					
On-site storage of data					
Unauthorized access to data					

Legend:
*PROBABILITY & *BUSINESS IMPACT
      H   **HIGH RISK** - Contact risk management/corporate security/business continuity
      M   **MEDIUM RISK** – Risk reduction strategy required
      L   **LOW RISK**
      X   **N/A**

PAST FREQUENCY (list number of occurrences in last 10 years)

6.3. STEP 3: Strategic and Tactical Risk Assessment Report

The strategic and tactical risk assessment report summarizes the findings of the various strategic and tactical risk assessments performed regarding the business venture or specific location. Based on the narrative issues and rankings assigned, an overall risk assessment is determined. The overall risk assessment ranking is used in completing the project evaluation matrix and becomes one of the six assessment factors for approving the capital expense request.

The following page provides a template to complete the strategic and tactical risk assessment report.

STRATEGIC AND TACTICAL RISK ASSESSMENT REPORT

RISK ASSESSMENT	RANK	NARRATIVE ISSUES
Strategic		
Country & Political Risk Assessment		
Financial Risk Assessment		
Human Capital Risk Assessment		
Operational Risk Assessment		
Tactical		
Environmental Risk Assessment		
IT Risk Assessment		
Security Risk Assessment		
Loss Control & Property Risk Assessment		
Overall Risk Assessment		

RANKING

0	No identified risk
1	Slight risk; no jeopardy to success of venture; no exposure
2	Slight risk to success of venture; minimal exposure
3	Moderate risk to success of venture; some exposure
4	High risk; moderate exposure
5	High risk; significant exposure

6.4. STEP 4: Project Evaluation Matrix

The project evaluation matrix is used to summarize information about the overall project. Here various criteria about the project are ranked and discussed. Part of the criteria is an assessment of the identified internal and external risks with doing business in a given geographic location. An overall risk ranking is assigned, and recommendations are given for continuing, or not continuing with the project. Recommendations *may* include what *should* be done to mitigate any probable risks from occurring, or if the risk does occur, what *should* be done to minimize the impacts of the risk to the business.

The following page provides a project evaluation matrix.

PROJECT EVALUATION MATRIX

CRITERIA	RANKING	WEIGHT	TOTAL	REASON FOR RANKING
Financial Return ROI %		**10**		
Strategic Match		**5**		
Operating Principle		**5**		
Strategic Architecture		**5**		
Essential Maintenance		**5**		
Risk Assessment		**-10**		
Score w/o ROI % **with ROI %**				

RANKING

0	No identified risk
1	Slight risk; no jeopardy to success of venture; no exposure
2	Slight risk to success of venture; minimal exposure
3	Moderate risk to success of venture; some exposure
4	High risk; moderate exposure
5	High risk; significant exposure

6.5. Summary and Conclusion

Having performed a LRA threats that could negatively impact the ability to conduct business in a geographic location have been identified. The results help to align strategic business decisions with effective risk reduction solutions at a geographic location. The LRA considered all threats whether they are financial, natural, political or human related. The LRA identifies and weighs the risks to business continuity based on the four-step process.

Finally, from well-rounded business continuity objective the next step would be to assess strategies, accept risks identified, or transfer of risk and/or mitigate some or all of the identified risks.

Upon successful completion of a location risk assessment, cable operators *should* perform a business impact analysis AND launch business continuity plan to include: incident management, operational continuity, and recovery strategies.