

SCTE | **STANDARDS**

Network Operations Subcommittee

SCTE STANDARD

SCTE 227 2022

**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, 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 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.

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 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 <https://scte.org>.

All Rights Reserved
©2022 Society of Cable Telecommunications Engineers, Inc.
140 Philips Road
Exton, PA 19341

Document Types and Tags

Document Type: Operational Practice

Document Tags:

- Test or Measurement
- Checklist
- Facility
- Architecture or Framework
- Metric
- Access Network
- Procedure, Process or Method
- Cloud
- Customer Premises

Document Release History

Release	Date
SCTE 227 2016	01/18/2016

Note: Standards that are released multiple times in the same year use: a, b, c, etc. to indicate normative balloted updates and/or r1, r2, r3, etc. to indicate editorial changes to a released document after the year.

Table of Contents

Title	Page Number
NOTICE.....	2
Document Types and Tags.....	3
Document Release History.....	3
Table of Contents.....	4
1. Introduction.....	5
1.1. Executive Summary.....	5
1.2. Scope.....	5
1.3. Benefits.....	5
1.4. Intended Audience.....	5
1.5. Areas for Further Investigation or to be Added in Future Versions.....	5
2. Normative References.....	6
2.1. SCTE References.....	6
2.2. Standards from Other Organizations.....	6
2.3. Other Published Materials.....	6
3. Informative References.....	6
3.1. SCTE Standards.....	6
3.2. Standards from Other Organizations.....	6
3.3. Other Published Materials.....	6
4. Compliance Notation.....	7
5. Abbreviations and Definitions.....	7
5.1. Abbreviations.....	7
5.2. Definitions.....	8
6. Four Steps to Location Risk Assessment.....	8
6.1. STEP 1: Strategic Risk Assessments.....	8
6.2. STEP 2: Tactical Risk Assessments.....	9
6.2.1. Physical Risk Assessment Factors and Worksheets.....	10
6.3. STEP 3: Strategic and Tactical Risk Assessment Report.....	18
6.4. STEP 4: Project Evaluation Matrix.....	20
6.5. Next Steps.....	22

List of Tables

Title	Page Number
Table 1 - Strategic Risk Description.....	9
Table 2 - Tactical Risk Assessment Ranking.....	10
Table 3 - Physical Risk Description.....	10

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 were the probable threats to occur, and
- Determine cost effective solutions to mitigate or minimize the risks.

The location risk assessment applies to all assets of the cable operator business that would impact operations based on locational considerations as well as third party facilities operators are dependent on.

Risks will be minimized by strategic, tactical and location risk assessments.

1.2. Scope

The scope of this document is to describe the steps necessary to perform a location risk assessment.

1.3. Benefits

Cable operators' networks provide entertainment, critical communication and information services, which are an integral part of the community they serve. By completing a location risk assessment, cable operators will be able make informed choices for potential location of a business unit and for planning how to mitigate threats that are dependent on location. LRA provides a basis for an informed business continuity plan. 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 their services.

1.4. Intended Audience

Senior management, engineering teams, or others responsible for uptime planning will benefit from reading this document.

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

Periodically local or national authorities (e.g., the U.S. Federal Emergency Management Agency), insurance providers or other subject matter experts, will update and identify natural and anthropogenic threats impacting location based risks. In addition to these updates there is a growing body of information

on risks due to global climate change; several sources are provided below under Other Published Materials. This information could result in the need to refresh the LRA or to perform mitigation activities to minimize potential impacts to the location. With better evolving data sources and models a more comprehensive location risk list could be defined leveraging SCTE 206 2021, “*Cable Operator Business Continuity and Disaster Recovery Operational Practices*”.

2. Normative References

The following documents contain provisions which, through reference in this text, constitute provisions of this document. The editions indicated were valid at the time of subcommittee approval. 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. Other 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 Standards

[SCTE 206] SCTE 206 2021, Cable Operator Business Continuity and Disaster Recovery Recommended Practices

3.2. Standards from Other Organizations

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

[BSI] Business Continuity Institute (BCI), <http://www.thebci.org/>

3.3 Other Published Materials

Climate Change A Risk Assessment David King, Daniel Schrag, Zhu Dada, Qi Ye and Arunabha Ghosh <https://www.csap.cam.ac.uk/media/uploads/files/1/climate-change—a-risk-assessment-v11.pdf>

Climate Impacts and Risk Assessment Climate Analytics <https://climateanalytics.org/what-we-do/climate-impacts-and-risk-assessment/>

Surging Seas Risk Finder Climate Central <https://riskfinder.climatecentral.org/>

Urban Adaptation Assessment Notre Dame Global Adaptation Initiative Notre Dame University <https://gain-uaa.nd.edu/>

US Climate Resilience Toolkit Unites States Global Change Research Program <https://toolkit.climate.gov/>

4. Compliance Notation

<i>shall</i>	This word or the adjective “ <i>required</i> ” means that the item is an absolute requirement of this document.
<i>shall not</i>	This phrase means that the item is an absolute prohibition of this document.
<i>forbidden</i>	This word means the value specified <i>shall</i> never be used.
<i>should</i>	This word or the adjective “ <i>recommended</i> ” means that there <i>may</i> exist valid reasons in particular circumstances to ignore this item, but the full implications <i>should</i> be understood and the case carefully weighed before choosing a different course.
<i>should not</i>	This phrase means that there <i>may</i> exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications <i>should</i> be understood and the case carefully weighed before implementing any behavior described with this label.
<i>may</i>	This word or the adjective “ <i>optional</i> ” indicate a course of action permissible within the limits of the document.
deprecated	Use is permissible for legacy purposes only. Deprecated features <i>may</i> be removed from future versions of this document. Implementations <i>should</i> 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 four steps *should* be 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 and shared with concerned stakeholders.

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 shared with concerned stakeholders.

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 FRE Q	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 _____

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
<i>Strategic</i>		
Country & Political Risk Assessment		
Financial Risk Assessment		
Human Capital Risk Assessment		
Operational Risk Assessment		
<i>Tactical</i>		
Environmental Risk Assessment		
IT Risk Assessment		
Security Risk Assessment		
Loss Control & Property Risk Assessment		
<i>Overall Risk Assessment</i>		

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. Next Steps

By performing a LRA, threats that could negatively impact the ability to conduct business in a geographic location can be identified. 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 the four-step process.

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 develop a business continuity plan that includes incident management, operational continuity, and recovery strategies.