BUSINESS CONTINUITY INSTITUTE

GOOD PRACTICE GUIDELINES

2007

A Management Guide to Implementing

Global Good Practice in

Business Continuity Management

CHAPTER 2

ABOUT THE GUIDE

Introduction

The BCI published its first Good Practice Guidelines in 2002. This played a significant part in the development of the British Standards Institution's (BSI) Publicly Available Specification for Business Continuity Management (PAS 56). GPG05 was issued followed by an extensive rewrite in to take into account the latest thinking in BCM internationally and to recognise increasing maturity in BCM practice across all sectors, public and private.

This new guide to implementation of Business Continuity Management (GPG07) has been prepared to support the launch of BS 25999-1 A Code of Practice for Business Continuity Management by the British Standards Institution. It can be viewed as implementation guide to BS25999 and as a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner.

However as a global institute, The BCI needs to reflect good practice across the world. BS25999 offers a comprehensive view of the subject but there are other standards in place with which many BCI professional members need to understand. As such the GPG07 is also designed to cover the main requirements of NFPA1600 (US and Canada) HB221 (Australia), APS 232 (Australia) and FSA (UK).

In no cases, however, must the GPG be seen as a replacement for those standards or as a guarantee of compliance with those standards.

Format of Guide

The Guide has been prepared in 6 chapters, which are in line with the earlier versions of the Guide and also with BS25999 nomenclature.

Chapter 1 consists of the introductory information plus **BCM Programme Management**.
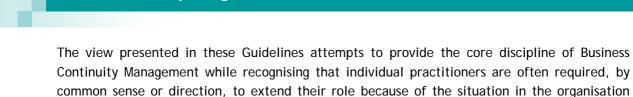
Chapter 2 is **UNDERSTANDING THE ORGANISATION**

Chapter 3 is **Determining BCM Strategy**

Chapter 4 is **Developing and Implementing BCM Response**

Chapter 5 is **Exercising, Maintaining & Reviewing BCM arrangements**

Chapter 6 is **Embedding BCM in the Organisation's Culture**

At the end of each chapter there is a summary of key learning outcomes that will support future use of the BCI Benchmarking tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide the core discipline of Business Continuity Management while recognising that individual practitioners are often required, by common sense or direction, to extend their role because of the situation in the organisation they work for.

Before referencing this Chapter of the Guide, you are advised to read Chapter 1, which explains in more detail how the guide works and how to use it most effectively.

About Chapter 2 - Understanding The Organisation

Business Continuity Management is an holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

Understanding the Organisation is a key element of good Business Continuity Management. It seeks to identify the key products and services of an organisation, and consequently define the time-criticality of activities that support them. This part of the BCM must be fully integrated into the organisation's objectives, obligations and statutory duties.

A thorough understanding of the business through Business Impact Analysis (BIA) and Risk Assessment (RA) in combination can often highlight business inefficiencies and focus on priorities that would not otherwise be apparent to senior management.

.

Chapter 2 - Understanding the Organisation

GUIDELINES STAGE 2

UNDERSTANDING THE ORGANISATION

COMPONENTS

1. GENERAL PRINCIPLES

2. BUSINESS IMPACT ANALYSIS

3. ESTIMATING RECOVERY REQUIREMENTS

4. ESTIMATING THREATS (RISK ASSESSMENT)

UNDERSTANDING THE ORGANISATION

Reference: BS 2999-1 Section 6

General Principles

As described in the section on BCM Policy step, the organisation must make a clear decision on whether the BCM will cover the whole organisation or just certain products or services. This sets the scope of the Business Impact Analysis (BIA) and Risk Assessment (RA) steps.

- The tools for understanding your business for business continuity purposes are:

- Business Impact Analysis (BIA) - a mandatory process for evaluating the impact over time of a disruption to an organisation's ability to operate

- Continuiity Recovery Requirements analysis - to estimate the resources and facilities and services that each activity will require at resumption

- Risk Assessment (RA) - to estimate the likelihood and impact on specific functions from known threats

The BIA identifies the urgency of each business activity undertaken by the organisation by assessing the impact over time of an interruption to this activity on the delivery of products and services. This information is used to identify the timescale of appropriate continuity and resumption strategies for each activity individually and in relation to one another.

The Continuity Requirements Analysis provides the information that will allow the scale (size and numbers) of the appropriate continuity measures to be determined.

Risk Assessment (RA) activity helps in identifying potential causes of interruption to an organisation, the probability of occurrence and impact of the threat being realised. Measures can then be identified that attempt to reduce the probability of occurrence or reduce the impact of an incident arising from these specific threats. Within the BCM programme, a RA should focus on the specific technologies and inherent risks of the business activities identified as most urgent in the BIA results rather than on all risks to the organisation.

BUSINESS IMPACT ANALYSIS

Reference: BS 2999-1 Section 6.2—3

1. Introduction

The Business Impact Analysis is the foundation work from which the whole BCM process is built. It identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organisation and provides the data from which appropriate continuity strategies can be determined.

A Business Impact Analysis (BIA) can be used to identify the timescale and extent of the impact of a disruption at several levels in an organisation. For example to examine the effect of:

- The loss of the ability to deliver each product or service - to educate decisions on the scope of the BCM programme

- An interruption to the internal and external activities that that would disrupt the delivery of products and services - to provide the information for selection of continuity options and their resource requirements

- A disruption of a business area's activity - to assist the preparation of a detailed plan for the department

Once the scope is determined the BIA focuses on the activities (which support those products and services) identifying those whose failure would most quickly threaten delivery. These tend to be the 'operational' activities, which interact directly with customers or other outside organisations. However these activities may depend for their delivery on the 'support' of other internal and external process, which must also be analysed.

- Examples of operational functions include:

  - Customer service
  - Sales
  - Production

- Examples of support functions include:

  - IT
  - Human resources
  - External support services such as utilities

- Examples of strategic activities include:

  - Management
  - Projects
  - Planning

2. Precursors

It is necessary to obtain the full support of the Executive or most Senior Management Group before a Business Impact Analysis is attempted. It is unlikely that managers will be prepared to dedicate time to this exercise unless this top tier support is demonstrated.

A decision about which products and services are within the scope of the BCM programme may have been made before a BIA is undertaken which will be documented within the Business Continuity Management (BCM) Policy. Alternatively the BIA method can be used to understand the impact of the failure to deliver the product or service. This can then be used to educate this decision.

The BCM Policy is the key document, which sets out the scope and governance of the BCM programme. The Policy provides the context in which the BCM team implement the required capabilities. To be able to develop an appropriate Business Continuity Management programme you must ensure that it reflects organisational objectives and culture (See Chapter 1)

3. Purpose

The purpose of a Business Impact Analysis is - for each activity or product and service:

- To document the impacts over time that would result from its loss or disruption.

- Inform a management decision on Maximum Tolerable Period of Disruption

- Identify the dependencies (both internally and externally) that are required to enable the activity to operate effectively

It is possible, and desirable, that a BIA is used to determine the impact of interruption in advance of major business change such as:

- Introduction of a new product, process or technology

- Office relocation or a change in the geographical spread of the business

- Significant change in business operations, structure or staffing levels

- A significant new supplier or outsourcing contract

4. Concepts and Assumptions

Concepts

- Maximum Tolerable Period of Disruption (MTPD) - this is the duration after which an organization's viability (either financially or through loss of reputation) will be irrevocably threatened if delivery of a particular product and service cannot be resumed.

- Seasonality may affect the MTPD. As examples, a financial year-end may reduce the tolerable outage for the finance activity and a one-off contract with significant time penalties may reduce the tolerable outage for a range of functions within the

Version 2007.2 15th March 2007 © The Business Continuity Institute 2007

organisation.

- Recovery Point Objective (RPO) - is the point to which information must be restored to enable an activity to operate once it is resumed.

Terminology 'Critical' activities

- Having ascertained the MTPD for each activity it is often convenient to link activities with similar recovery requirements. Sometimes organisations call these groups according to the recovery timescale (e.g. 1 day, 2 day, 1 week etc); others use the term 'critical' (or 'mission critical' activities) for those activities required within the first few days. Unfortunately for those unfamiliar with BCM terminology, 'critical' is often interpreted as 'important' leading to misunderstandings when collecting data for the BIA and the, incorrect, assumption that recovery tactics and plans are not required for 'non-critical' activities. Terms with less ambiguous, time related meanings in general use include 'time-critical', time sensitive and 'urgent'.

Assumptions

- It is assumed that the organisation can be understood by analysis of separate business activities

- The MTPD may be difficult to determine for seasonal or periodic functions such as year-end processing and projects. In such instances impact analysis should focus on an interruption to the activity during one of these peaks

- Where resilience measures are already in place these should be assumed to be in operation (though they may prove not to be adequate)

Sensitivity of information

- It is possible that some information will be market / industry sensitive and so in some organisations it will not visible to the BCM professional. Not having this information should not stop the BIA activity being undertaken but may prejudice the accuracy of the end results.

5. Process

Scope and Scale

- If the organisation is part of a group – identify the relationship between the various parts of the organisation since this may affect the MTPD

- If the organisation has multiple locations identify the geographical scope of the BIA from the Policy.

- Sign off the terms of reference with the project sponsor drawn from Executive or Senior Management Group

Business Impact Analysis

- Identify discrete business activities across the organisation (which may cut across several departments) and management owners of these processes

- Identify suitable staff from whom information can be sought about the business processes – subject matter experts

- Identify the impacts which may result in damage to the organisation's reputation, assets or financial position

- Quantify the timescale within which the interruption of each business activity becomes unacceptable to the organisation

- Where an organisation has multiple sites it may be necessary to decide on the maximum geographic extent of a disruption or extent of resource loss that the organisation wants to, or needs to, plan to survive to quantify impact. This could be determined by:

    - Geographical extent (or market/customer area)
    - Regulatory or statutory requirements
    - Products, market sectors or specific customer requirements

Reporting

- Obtain sign-off by the process owner to confirm accuracy of information

- Obtain support of the BCM sponsor for the conclusions.

6. Methods and Techniques

Data collection

Methods, tools and techniques to carry out Business Impact Analyses include:

- Workshops

- Questionnaire (s) - paper and / or automated software

- Interviews (structured and unstructured)

As a general guideline:

- Workshops can provide rapid results and an opportunity for hands-on engagement with the programme provided there is consistent buy-in from all departments and participants

- Questionnaires provide large amounts of data but information quality can be very questionable if not completed with consistency

- Interviews can provide very good information but are time consuming and output can vary in format and detail

- Combinations of the above methods can provide excellent results providing an appropriate level of detail and a standard reporting format that will assist in consistency of recording and analysing information across multiple functions.

Data Collection Questionnaires

There is no 'one size fits all' methodology for business impact analysis data collection. Methods vary from one industry sector to another and from one practitioner to another. Each industry has its own specific needs in result content, information types, depth and coverage. However a few basic principles that should be considered are:
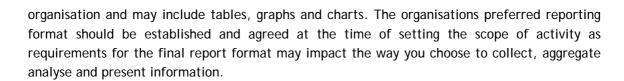
- The objective of the BIA is to collect information to educate the choice of appropriate continuity strategies which is determined by the urgency with which each activity needs to be resumed

- How will the information collected be used?

- What is the best format of data collection to report results effectively?

- What basic information is needed to establish the urgency of the performance of the activity being analysed in isolation and as part of the organisation as a whole:

  - Timeframes within which the activity must be resumed
  - Locations from which activity is undertaken
  - Influences on the activity, e.g. peak periods, regulatory reporting
  - What is the impact of not continuing the activity
  - How long can the organisation last without it
  - Are there any alternatives?
- Factors to consider include:

  - Volumes, e.g. calls per hour, output on production line
  - Contractual, regulatory or legal requirements
  - Key tools to achieving continuity of the activity (how many, where and when):
    - People – skill set
    - Equipment – IT, telecommunications, manufacturing / industrial plant
    - Data – paper and electronic
    - Dependencies – internal and external to organisation

Software

There are a variety of proprietary software products available to conduct Business Impact Analyses that may be useful but are not essential. The key benefits of utilising a software tool include ease of analysing results, storage of information and potentially reporting of the results their use does not however remove the need for interviews with or involvement of individuals knowledgeable in the activity being analysed.

Reporting

Every organisation has its own preferred style of reporting and in some instances the reporting style may need to be adjusted to accommodate multiple audience groups within the one

organisation and may include tables, graphs and charts. The organisations preferred reporting format should be established and agreed at the time of setting the scope of activity as requirements for the final report format may impact the way you choose to collect, aggregate analyse and present information.

7. Outcomes and Deliverables

The outcomes from a Business Impact Analysis are:

1) The Maximum Tolerable Period of Disruption and its justification (nature of impacts) for each activity

2) Recovery Point Objective (RPO) to which information must be restored to enable an activity to operate once it is resumed.

8. Review

Good practice indicates that a Business Impact Analysis should be reviewed as a minimum annually but more frequently in the event of:

- A particularly aggressive pace of business change

- Significant change in the internal business processes, location or technology

- Significant change in the external business environment - such as market or regulatory change

This does not necessarily require the BIA to be completely redone. Careful design of the BIA report can facilitate this process by providing a benchmark against which changes in the above areas can be measured and their changed impact assessed.

ESTIMATING CONTINUITY REQUIREMENTS

Reference: BS 2999-1 Section 6.4

1. Introduction

The Continuity Requirements Analysis collects information on the numbers of resources required to resume and continue the business activities at a level required to satisfy the organisations obligations

2. Precursors

This step is usually undertaken at the same time as the BIA information is being gathered.

3. Purpose

Its purpose is to:

- Provide the resource information from which an appropriate recovery strategy can be determined / recommended

- Identify resource requirements resulting from activity dependencies that exist both internally and externally

4. Concepts and Assumptions

Continuity Requirements

It is often assumed that the required resources after a disruption will be a fraction of the numbers used during normal operations - at least for a period of time. However in some cases the resources in the early stages of recovery may need to be higher than normally used to cope with backlogs. For example in a call-centre additional staff may be needed to cope with the extra calls following an interruption and supporting IT systems may need to have a higher capacity to cope with this additional number of users.

5. Process

Continuity Requirements

- Quantify the resources (e.g. people, technology, telephony,) required over time to maintain the business functions at an acceptable level and within the maximum tolerable period of disruption For a period after the interruption this may be less or more than the usual resource requirement. It should take into account any extra activity that will be generated by the interruption and the need to clear backlogs.

Reporting

- Obtain sign-off by the process owner to confirm accuracy of information

- Obtain support of the BCM sponsor for the conclusions.

- Present to the Senior Management Group or Executive to determine whether results will be impacted by any proposed business change and for approval to move to strategy design stages.

- Proceed to development of BCM strategy.

6. Methods and Techniques

Data collection

Methods, tools and techniques to carry out Continuity Requirements Analyses include:

- Workshops

- Questionnaire (s) - paper and / or automated software

- Interviews (structured and unstructured)

The information is usually collected at the same time as the BIA information.

7. Outcomes and Deliverables

The outcomes from a Continuity Requirements Analysis are:

- The resources required during the time after a resumption to provide agreed service levels

- Interdependancies between internal activities and on external suppliers

This information feeds directly into the Business Continuity Strategy stage. The resource requirements will provide the data to evaluate alternative recovery solutions for adequacy of size and performance.

8. Review

The Continuity Requirements Analysis should be reviewed along with the BIA.

EVALUATING THREATS (RISK ASSESSMENT)

Reference: BS 2999-1 Section 6.5

1. Introduction

In the context of BCM, a Risk Assessment looks at the probability and impact of a variety of specific threats that could cause a business interruption. By prioritisation it may be possible to implement measures to reduce the likelihood or mitigate the impact of these threats.

When evaluating threats to business activities, the BIA provides an extra dimension (time) into the usual Threat Impact * Likelihood equation. It suggests that effort on implementing risk treatment measures should be targeted on those activities that will most quickly disrupt the business.

It is difficult to scope a Risk Analysis across an entire organisation however, by focussing on the resources required to operate the organisation's most urgent activities (i.e. following a BIA), the focus of the Risk Assessment can be reduced to a more manageable scope.

It should be recognised that Risk Assessment has serious shortcoming in evaluating catastrophic operational risks because:

- It is impossible to identify all threats

- Estimates of probability are guesswork or based on historic and sometimes inaccurate information.

- Impacts are not fixed ('high, medium and low') but increase over time at different rates

- The numeric scales used often over-emphasise the impact of minor events

The Risk Assessment may identify unacceptable concentrations of risk and what are known as 'single points of failure'. These should be highlighted to the business continuity sponsor at Executive or Senior Management level at the earliest possible opportunity along with options for addressing the issue. The strategic decision to mitigate, transfer or accept the risk should be formally documented and signed off.

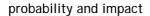In some countries and sectors the use of Risk Assessment is mandated.

2. Precursors

A Business Impact Analysis should be completed in advance of a Risk Assessment to identify the urgent functions upon which the risk assessment should be focused.

3. Purpose

The Purpose of a Risk Assessment is to:

- Identify the internal and external threats that could cause a disruption and assess their

probability and impact

- To prioritise the threats according to an agreed formula

- To inform a risk management control programme and action plan.

4. Concepts and Assumptions

Concepts:

Whatever the complexity of the actual formula adopted the following relationship is assumed:

- Risk = Threat impact * Probability

Some risk models then order risks by: Priority = Risk * Ability to control that risk.   This prioritises the threats that are easiest to control with, presumably, the argument that this will give the best return on investment of time and money but ignoring many external impacts.

In other risk models the risks assessed are examined with no controls in place and then again with current and desired controls in place.   This second step serves to emphasise that assumptions when managing the risk control environment should not be made and that the effectiveness of controls should always be examined and as applicable, challenged and improved.   If an organisation decides after taking this second step that they do not wish to improve controls - perhaps due to prohibitive cost - then the Risk and BCM managers need to be aware of this and factor this decision into their approach.

The organisation's 'risk appetite' or 'risk tolerance' is the amount of risk that an organisation is prepared to accept and drives the level of action it will take to control identified threats.

Assumptions

- All realistic threats can be identified

- Accurate and applicable statistics are available to estimate the probability of occurrence

- Threats which are easier to control (staff or own building issues) are to be prioritised at the expense of those which are less susceptible to influence – such as bad weather

- The use of a numerical scale to assign a value to impacts can adequately reflect the relative importance of less-quantifiable assets such as reputation

- The use of a numerical scale (1,2,3.) represents a realistic relationship between the different impact and probability bands (where in reality a logarithmic scale may be more realistic (e.g. 1, 10, 100, 1000…))

5. Process

The key stages in a Risk Assessment are:

- Tabulate a scoring system for impacts and probabilities and agree with project sponsor

- List threats to the urgent business processes determined in the BIA.

- Estimate the impact on the organisation of the threat using a numerical scoring system

- Determine the likelihood (probability or frequency) of each threat occurring and weight according to a numerical scoring system

- Calculate a risk by combining the scores for impact and probability of each threat according to an agreed formula

- Optionally prioritise the risks according to a formula which includes a measure of the ability to control that threat

- Obtain organisation sponsor's approval and sign-off of these risk priorities.

- Review existing risk management control strategies noting where the assessed risk level is out of step with the current risk management strategies for that threat.

- Consider appropriate measures to:

  - Transfer the risk e.g. through insurance
  - Accept the risk e.g. where impact / probability are low
  - Reduce the risk e.g. through the introduction of further controls
  - Avoid the risk e.g. by removing the cause or source of the threat

- Ensure that planned risk measures do not increase other risks. For example, outsourcing an activity may decrease some types of risk by increase others.

- Obtain the organisation sponsor's approval, a budget and sign-off for the proposed risk management control (s).

6. Methods and Techniques

The methods, tools and techniques to provide a Risk Assessment include:

Determining threats

- Event Tree Analysis

- Fault Tree Analysis

Assessing probabilities

- Insurance statistics

- Published disaster frequency statistics

Version 2007.2 15th March 2007 © The Business Continuity Institute 2007

Scoring systems

There are many scoring systems in published literature.

Tabulating Threats

- Threat Vulnerability Matrix

- Risk Quartile Matrix

Evaluating solutions

- Cost Benefit Analysis.

7. Outcomes and Deliverables

The outcomes from a Risk Assessment include the identification and documentation of:

- Single points of failure

- Prioritised list of threats to the organisation or to the specific business processes analysed

- Information for a risk control management strategy and action plan for risks to be addressed

- Documented acceptance of identified risks that are not to be addressed

8. Review

A Risk Assessment should be carried out as defined in the organisation's risk management strategy. This may be annually for the most time sensitive processes but more frequently if:

- The pace of business change is particularly aggressive.

- There is a significant change in the internal business processes, location or technology

- There is a significant change in the external business environment – such as market or regulatory change.

Note: BS 2999-1 Section 6.6 (Determining choices) is addressed in Stage 1— Scope of the BCM Programme

KEY BCM INDICATORS

The following are key elements of what would be expected from a mature BCM organisation

CORPORATE GOVERNANCE

1. The BCM programme contains explicit formal mechanisms that ensure compliance with all applicable external legislation, regulation and industry codes of practice

2. The BCM programme contains explicit formal mechanisms that ensure objective compliance with all applicable internal policies, directives and adopted industry codes of practice.

3. The BCM programme contains explicit formal mechanisms that enable prompt identification and reflection of all changes in statute, policy or codes that affect BCM

BIA PRACTICE

4. The organisation carries out business impact analysis (BIA) for all areas of its operation

5. The BIA assesses and records over time stakeholders' tolerance to deprivation of the organisation's products, services and other interests

6. The BIA assesses and records over time the organisation's tolerance to each significant type of continuity-related impact it could sustain

7. The BIA assesses and records over time the types, severities and combinations of continuity-related impact that could reasonably occur.

8. The BIA assesses and records over time the overall impact on the organisation of non-restoration of each activity following any disruption

9. The BIA establishes, quantifies and justifies:

- A. The maximum tolerable period of disruption for each activity

- B. The levels to which all activities must be restored over time

- C. All the resources required by each activity over time to achieve the recovery time objectives

- D. The organisation's business activities or functions, resources and infrastructures

10. The BIA takes full account of and fully complies with BCM policy

11. The BIA fully complies with the organisation's specified approach

12. The BIA's findings and conclusions are fully documented

13. The BIA and all associated documentation is

- A. Up-to-date and reflective of the organisation's current condition

- B. Formally reviewed at least annually against BCM Policy and whenever a significant change in the organisation's impact profile occurs

- C. Signed off by senior management

14. The BIA takes account of the following types of tangible financial impact

- A. Opportunity cost

- B. Increased cost of working and expenses

- C. Revenue or equivalent throughput value reduction

- D. Inefficiency and profitability

- E. Uninsured asset replacement

- F. Capital value and financial viability

15. The BIA takes account of the following types of intangible non-financial impact

- A. Reputation, brand and presence

- B. Legal and contractual liabilities

- C. Quality of product and service

- D. Stakeholder confidence and support

- E. Staff morale and well being

- F. Operational and management control

- G. Environmental damage

RISK ASSESSMENT PRACTICE

16. The organisation systematically plans and carries out formal BCM-related risk assessment for all areas of its operation

17. The risk assessment identifies, evaluates and records the following:

- A. All relevant hazards and threats to the organisation's most urgent activities and resources

- B. All relevant vulnerabilities of each of the organisation's most time-sensitive activities and resources

- C. All relevant concentrations of risk that threaten business continuity (single points of failure)

- D. All relevant continuity risks due to suppliers and outsource providers

18. The risk assessment identifies, evaluates and records

- A. All the major disruption scenarios that could affect the organisation

- B. Continuity risks that are to be accepted, handled elsewhere or otherwise not addressed by the BCM programme

- C. Measures that reduce the likelihood, duration and impact of a disruption on the organisation's key products and services

- D. Continuity risks arising from key skills shortages or concentrations

19. The risk assessment uses the impact information contained in the BIA to provide a consistent estimate of exposure

20. The risk assessment re-states and takes into full account the organisation's tolerance or appetite for continuity risks

21. The risk assessment covers the following areas:

- A. Uses appropriate statistics to assess the likelihood of each realistic threat to continuity

- B. Refers to the organisation's insurance arrangements and quantifies resulting exposure

- C. Is an integral part of the organisation's risk management and control framework

- D. Provides the basis for prioritising the treatment of continuity risks

22. The organisation has formal strategies for mitigating all business continuity risks for all areas of its operations

23. The strategies mitigate the effects of, and ensure the organisation can tolerate and recover acceptably from

- A. All continuity-related scenarios identified in the risk assessment (s)

- B. Denial of access or loss of any worksite (s)

- C. Any technology failure

- D. Any supplier or utility failure

- E. Any outsource or other business unit failure

- F. Any civil emergencies that arise

Chapter 3 of the Good Practice Guidelines examines:

Determining BCM Strategy