Professional Practices for Business Continuity Practitioners

Professional Practice Introduction

Business Continuity Management (BCM) is a management process that identifies risk, threats and vulnerabilities that could impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response.

The objective of Business Continuity Management is to make the entity more resilient to potential threats and allow the entity to resume or continue operations under adverse or abnormal conditions. This is accomplished by the introduction of appropriate resilience strategies to reduce the likelihood and impact of a threat and the development of plans to respond and recover from threats that cannot be controlled or mitigated.

The Professional Practices are a body of knowledge designed to assist the entity in the development and implementation of a BCM program. Use of the Professional Practice framework can increase the likelihood that no significant gaps will be present in your program as well as increase the likelihood that the various parts of the program will work cohesively in an actual event.

These Professional Practices are intended to serve as both a guide for BCM Program development, implementation and maintenance and as a tool for conducting audits of an existing program. Using the Professional Practices to audit a program can identify program gaps or deficiencies so they may be corrected before an event occurs.

The Professional Practices have been developed and maintained by experienced Business Continuity professionals to provide a consistent framework for the industry, to assist others who wish to enter this field with the body of knowledge to develop the skills needed and to assist organizations in benchmarking their program against accepted and proven practices.

The sections within these practices are not presented in any particular order of importance, as it may be necessary to undertake or implement sections in parallel during the development of the BCM Program.

Professional Practice Subject Area Overview

1. Program Initiation and Management

Establish the need for a Business Continuity Management Program within the entity and identify the program components from understanding the entity's risks and vulnerabilities through development of resilience strategies and response, restoration and recovery plans. The objectives of this professional practice are to obtain the entity's support and funding and to build the organizational framework to develop the BCM program.

Professional Practices for Business Continuity Practitioners

2. Risk Evaluation and Control

The objective of this professional practice is to identify the risks/threats and vulnerabilities that are both inherent and acquired which can adversely affect the entity and its resources, or impact the entity's image. Once identified, threats and vulnerabilities will be assessed as to the likelihood that they would occur and the potential level of impact that would result. The entity can then focus on high probability and high impact events to identify where controls, mitigations or management processes are non-existent, weak or ineffective. This evaluation results in recommendations from the BCM Program for additional controls, mitigations or processes to be implemented to increase the entity's resiliency from the most commonly occurring and/or highest impact events.

3. Business Impact Analysis

During the activities of this professional practice, the entity identifies the likely and potential impacts from events on the entity or its processes and the criteria that will be used to quantify and qualify such impacts. The criteria to measure and assess the financial, customer, regulatory and/or reputational impacts must defined and accepted and then used consistently throughout the entity to define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each of the entity's processes. The result of this analysis is to identify time sensitive processes and the requirements to recover them in the timeframe that is acceptable to the entity.

4. Business Continuity Strategies

The data that was collected during the BIA and Risk Evaluation is used in this professional practice to identify available continuity and recovery strategies for the entity's operations and technology. Recommended strategies must be approved and funded and must meet both the recovery time and recovery point objectives identified in the BIA. A cost benefit analysis is performed on the recommended strategies to align the cost of implementing the strategy against the assets at risk.

5. Emergency Response and Operations

This professional practice defines the requirements to develop and implement the entity's plan for response to emergency situations that may impact safety of the entity's employees, visitors or other assets. The emergency response plan documents how the entity will respond to emergencies in a coordinated, timely and effective manner to address life safety and stabilization of emergency situations until the arrival of trained or external first responders.

6. Plan Implementation and Documentation

The Business Continuity Plan is a set of documented processes and procedures which will enable the entity to continue or recover time sensitive processes to the minimum acceptable level within the timeframe acceptable to the entity. In this phase of the Business Continuity Management Program, the relevant teams design, develop, and implement the continuity strategies approved by the entity and document the recovery plans to be used in response to an incident or event.

Professional Practices for Business Continuity Practitioners

7. Awareness and Training Programs

In this professional practice, a program is developed and implemented to establish and maintain corporate awareness about Business Continuity Management (BCM) and to train the entity's staff so that they are prepared to respond during an event.

8. Business Continuity Plan Exercise, Audit and Maintenance

The goal of this professional practice is to establish an exercise, testing, maintenance and audit program. To continue to be effective, a BCM Program must implement a regular exercise schedule to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization. As part of the change management program, the tracking and documentation of these activities provides an evaluation of the on-going state of readiness and allows for continuous improvement of recovery capabilities and ensures that plans remain current and relevant. Establishing an audit process will validate the plans are complete, accurate and in compliance with organizational goals and industry standards as appropriate.

9. Crisis Communications

This professional practice provides the framework to identify, develop, communicate, and exercise a crisis communications plan. A Crisis Communications plan addresses the need for effective and timely communication between the entity and all the stakeholders impacted or involved during the response and recovery efforts.

10. Coordination with External Agencies

This professional practice defines the need to establish policies and procedures to coordinate response, continuity and recovery activities with external agencies at the local, regional and national levels while ensuring compliance with applicable statutes and regulations.

DRII Professional Practices

Professional Practice One - Program Initiation and Management

Establish the need for a BCM Program within the entity and identify the program components from understanding the entity's risks and vulnerabilities through development of resilience strategies and response, restoration and recovery plans. The objectives of this professional practice are to obtain the entity's support and funding and to build the organizational framework to develop the BCM program.

The Professional's Role in Professional Practice One is as follows:

1. Establish why the entity needs a Business Continuity Management Program
2. Obtain leadership/management support for the BCM program
3. Coordinate and manage the implementation of the BCM program throughout the entity

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1. Establish the need for the business continuity program.
    a. Research and reference relevant business, legal, regulatory, statutory and contractual requirements and restrictions both from an internal and external perspective, providing recommendations on conformance and compliance for the organization.
    b. Reference relevant standards developed by national or international standards development bodies and/or trade or industry associations.
    c. Identify and resolve any conflicts between organizational policies and relevant external requirements.
    d. Review existing audit reports to ensure the proposed BCM program adequately addresses any gaps or opportunities previously identified (through either internal or external sources).
    e. Identify business practices (such as complex supply chain strategies implemented on a regional or global scale) that may adversely impact the entity's ability to recover following a disaster event.
    f. State the benefits of BCM and relate them to the entity's mission, objectives and operations.
    g. Explain executive management's/leadership's role, including their accountability and liability within the BCM Process.
    h. Develop formal reports and presentations focused on increasing the awareness and potential impact of risks to the organization from a Business Continuity Management (BCM) perspective.

2. Obtain leadership/management support for the BCM program.
    a. Develop a mission statement/charter for the BCM program.
    b. Develop objectives for the BCM program tied to support of the entity's mission.
    c. Develop Budget Requirements for BCM program.
    d. Define BCM program structure, its policies and critical success factors.
    e. Present and obtain management/leadership support and approval of BCM Program.
    f. Identify executive sponsors for BCM program development.
    g. Obtain executive approval for budget requirements.
    h. Gain agreement on the establishment of the Planning/Steering Committee along with tactical support functions needed, including primary and alternates for each role.
    i. Define the scope, responsibilities and overall accountability of each member of the Planning/Steering Committee and support functions.

3. Coordinate and manage the implementation of the BCM program throughout the entity.
    a. Lead the designated Planning/Steering Committee in defining objectives, program structure, policies and how critical success factors will be managed.
    b. Develop relevant policies, procedures and charters.
    c. Clearly define and obtain resource needed for BCM program.
    d. Identify teams for BCM program implementation including teams that will participate in the execution of the following activities:
        i. Risk assessment and resiliency strategies
        ii. Business impact analysis
        iii. Recovery strategy selection and implementation
        iv. Overall incident and emergency management
            1. Incident response and recovery
            2. Crisis management and communication
            3. Post incident gap analysis and implementation of lessons learned
        v. Developing Business continuity plan documentation
        vi. Plan testing, exercise and maintenance activities
        vii. Response, Recovery and restoration activities during an event
    e. Monitor status of ongoing budget impact per existing management process.

f. Develop project plans and identify tasks required to support the agreed upon. critical success factors such as:

i. Schedule

ii. Time estimates

iii. Milestones

iv. Personnel requirements, including training, succession planning and development

g. Oversee the ongoing effectiveness of the Program.

i. Develop the on-going management and documentation requirements for the BCM Program.

ii. Monitor, track and report to compliance to established BCM standards.

iii. Conduct internal and external benchmarking strategies.

h. Report to Senior Management/Leadership on Program status on a regular basis

i. Develop a schedule to report the progress of the BCM Program to the entity's leadership.

ii. Develop regular status reports for senior management/leadership that contain concise, pertinent, accurate, and timely information on key elements of the BCM Program

iii. Provide updates on the State of the BCM Program and make recommendations for Program enhancements on an on-going basis

iv. Monitor relevant industry and organizational standards to ensure BCM program is consistently delivering business value

DRII Professional Practices

Professional Practice Two - Risk Evaluation and Control

The objective of this professional practice is to identify the risks/threats and vulnerabilities that are both inherent and acquired which can adversely affect the entity and its resources, or impact the entity's image. Once identified, threats and vulnerabilities will be assessed as to the likelihood that they would occur and the potential level of impact that would result. The entity can then focus on high probability and high impact events to identify where controls, mitigations or management processes are non-existent, weak or ineffective. This evaluation results in recommendations from the BCM Program for additional controls, mitigations or processes to be implemented to increase the entity's resiliency from the most commonly occurring and/or highest impact events.

The Professional's Role in Professional Practice Two is as follows:

1. Work with management and any risk management/enterprise risk management groups within the entity to gain agreement on a clear and standardized risk assessment methodology and to gain understanding of the entity's tolerance for risk.
2. Identify, develop and implement information gathering activities across the entity to identify threats/risks and the entity's vulnerabilities.
3. Identify probabilities and impact of the threats/risks identified.
4. Identify and evaluate the effectiveness of the current controls and safeguards in place.
5. Identify business resiliency strategies to control, mitigate, accept or take advantage of the potential impact of the risk/threat or reduce the entity's vulnerabilities.
6. Document and present risk/threat/vulnerability assessment and recommendations to the entity's leadership for approval.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1. Work with management and any risk management/enterprise risk management groups within the entity to gain agreement on a clear and standardized risk assessment methodology and to gain understanding of the entity's tolerance for risk.
   a. Identify risk analysis methodologies and tools. These may include:
      i. Qualitative and quantitative methodologies
      ii. Assessment of advantages and disadvantages
      iii. Data and content reliability/confidence factors
      iv. Use of mathematical formulas
   b. Select appropriate methodology and tool(s) for entity-wide implementation which parallel the entity's risk tolerance level.

- c. Work with the entity's leadership to gain an understanding of the entity's tolerance for risk.
- d. Work with management to select an appropriate cost benefit analysis model.
- e. Establish the measurement criteria necessary to quantify the risk identified and the effectiveness of existing controls.

2. Identify, develop and implement information gathering activities across the entity to identify threats/risks and the entity's vulnerabilities.
   - a. Determine methods of information gathering.
   - b. Collaborate with entity's legal counsel, physical security, information security, privacy and other pertinent areas to identify known risks and vulnerabilities.
   - c. Determine information sources to be used to collect data on risks.
   - d. Determine the credibility of the information sources.
   - e. Develop a strategy to gather information consistent with the entity's policies.
   - f. Develop a strategy to gather information that can be managed across all of the entity's divisions and locations.
   - g. Create entity-wide methods of information collection and distribution.
     - i. Forms and questionnaires
     - ii. Interviews
     - iii. Meetings
     - iv. Or combinations of above
3. Identify threats/risks and the entity's vulnerabilities.
   - a. Identify threats/risks and vulnerabilities to the entity taking into account frequency, probability, speed of development, severity and reputational impact to achieve a holistic view of risk across the entity.
   - b. Identify risk exposures from both internal and external sources. These sources include, but are not limited to:
     - i. Natural, technological or acts of man
     - ii. Industry/business model
     - iii. Accidental versus intentional
     - iv. Controllable exposures/risks versus those beyond the entity's control
     - v. Events with prior warnings versus those with no prior warnings
4. Identify probabilities and impact of the threats/risks identified.
   - a. Develop a method to evaluate exposures/risks in terms of risk frequency, probability, speed of development, pre incident warning (e.g. hurricane), severity and entity impact.
   - b. Identify the impact of identified risks. Risk impacts include, but are not limited to:
     - i. Facility
     - ii. Security (both physical and logical)

        iii. Reputational
        iv. Legal
        v. Customer
        vi. Procedural
        vii. Information Technology (including operational infrastructure)
        viii. People
        ix. Supply Chain (including outsourcing)
        x. Compliance
    c. Evaluate identified risk and classify them according to relevant criteria including, but not limited to:
        i. Risks under the entity's control
        ii. Risks beyond the entity's control
        iii. Risks with prior warnings (such as tornadoes and hurricanes)
        iv. Risks with no prior warnings (such as earthquakes)
    d. Evaluate impact of risks and vulnerabilities on those factors essential for conducting the entity's operations:
        i. Availability of personnel
        ii. Availability of information technology
        iii. Availability of communications technology
        iv. Status of infrastructure (including transportation), etc.

5. Identify and evaluate the effectiveness of the current controls and safeguards in place.
    a. Identify and evaluate the effectiveness of the inherent protection afforded key assets by virtue of their location relative to sources of risk.
    b. Identify and evaluate the effectiveness business continuity capabilities for groups within and external to the entity on which the entity is dependent to conduct its operations.
    c. Identify and evaluate the effectiveness of actions taken to reduce the probability of occurrence of incidents that could impair the ability to conduct business.
        i. Facility sighting
        ii. Safety policies and procedures
        iii. Training on proper use of equipment and tools
        iv. Preventive maintenance
    d. Identify and evaluate the effectiveness of controls to inhibit impact exposures: preventive controls (proactive controls that help to prevent a loss).
        i. Physical security practices (access control, cameras, security staff)
        ii. Information Security practices (firewalls, intrusion detection, passwords)
        iii. Employment practices (background investigations, hiring practices)
        iv. Privacy practices (clean desk policy, proprietary waste disposal)

e. Identify and evaluate the effectiveness of controls to compensate for impact of exposures: reactive controls (that typically work or are implemented in response to a loss).
   i. Sprinkler system
   ii. Fire brigade
   iii. Generator
   iv. UPS system

f. Evaluate security-related communications flow with other internal areas and external service providers.

6. Identify business resiliency strategies to control, mitigate, accept or take advantage of the potential impact of the risk/threat or reduce the entity's vulnerabilities.
   a. Discuss strategies and controls for managing the identified risks.
   b. Identify trigger points for key service and support areas to identify, escalate and execute strategies selected to take advantage of key risks.
   c. Establish interruption scenarios based on risks to which the entity is exposed. These scenarios should be based on situations severe in magnitude, occurring at the worst possible time, resulting in severe impairment to the entity's ability to conduct business.
   d. Understand options for risk management and selection of appropriate or cost-effective responses (examples include: risk avoidance, transfer, or acceptance of risk).
   e. Develop formal "risk acceptance" documentation and re-evaluation practices in conjunction with the entity accepted risk tolerance.
   f. Make recommendations on feasible, cost-effective security measures required to prevent/reduce security-related risks and exposures.
   g. Recommend changes, if necessary, to reduce impact due to risks and vulnerabilities.
      i. Physical protection
         1. Identify requirements necessary to restrict access at all pertinent levels (e.g. building, room, etc.).
         2. Investigate the need for barriers and strengthened structures to determine willful and accidental and/or unauthorized entry.
         3. Location: physical construction, geographic location, corporate neighbors', facilities infrastructure, community infrastructure.
         4. Identify the need for the use of specialist personnel to conduct checks at key entry points.
         5. Evaluate the need for manned and/or recorded surveillance .equipment to control access points and areas of exclusion;

including detection, notification, suppression (e.g., sensors, alarms, and sprinklers).

6. Changes to security and access controls, tenant insurance, leasehold agreements.

ii. Logical protection

1. Assess the need for system-provided protection of data stored, in process, or in translation; information backup and protection.
2. Evaluate information security: hardware, software, data, and network monitoring (e.g., detection, notification, etc.).
3. Location of assets.

iii. Changes to personnel procedures.

iv. Increased preventive maintenance and service as required.

v. Utilities: duplication of utilities, built in redundancies (Telco, power, water, etc.).

vi. Interface with outside agencies (vendors, suppliers, outsourcers, etc.).

7. Document and present risk assessment to the entity's leadership for approval.

a. Prepare a risk assessment report, standardizing the analysis across the entity

b. Present findings of risk assessment including, but not limited to:

i. Information on risks and exposures from risk analysis.

ii. An assessment of controls and/or strategies in place to manage known risks and a rating of the control effectiveness as fully effective, partially effective or ineffective.

iii. Recommend new controls to be implemented including cost/benefit.

iv. Recommend control improvements including cost/benefit.

v. Recommend appropriate areas to transfer risk.

vi. Recommend priorities for implementation of new control.

vii. Document areas where management accepts risk with a formal sign-off .

c. Receive approval of risk assessment recommendations.

DRII Professional Practices

Professional Practice Three - Business Impact Analysis

During the activities of this professional practice, the entity identifies the likely and potential impacts from events on the entity or its processes and the criteria that will be used to quantify and qualify such impacts. The criteria to measure and assess the financial, operational, customer, regulatory and/or reputational impacts must defined and accepted and then used consistently throughout the entity to define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each of the entity's processes. The result of this analysis is to identify time sensitive processes and the requirements to recover them in the timeframe that is acceptable to the entity.

The Professional's Role in Professional Practice Three is as follows:

1. Identify the criteria to be used to quantify and qualify the entity's impact from events.
2. Establish the Business Impact Analysis (BIA) process and methodology.
3. Plan and coordinate data gathering and analysis.
4. Gain leadership agreement on BIA methodology and the criteria to be used.
5. Analyze the data collected against the approved criteria to establish RTO and RPO for each operational area and the technology that supports them.
6. Document minimum resource requirements for resumption and recovery of core and support business functions and their escalation over time.
7. Prepare and present the BIA results to the entity's leadership and gain acceptance of the RTO and RPO for each process.

Note: While the Business Continuity Professional may be given the responsibility to manage a BIA, the 'ownership' of that BIA resides with the entity and its leadership, or the owners of the process or processes under consideration.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1) Identify the criteria to be used to quantify and qualify the impact to the entity.
   a) Define and obtain approval for criteria to be used to assess the impact on the entity's operations including but not limited to:
      (1) Customer impact
         (a) How quickly customers will know you have a problem
         (b) How worried they will be about it
         (c) What is the likelihood they will take their business elsewhere
         (d) What the impact to committed service levels will be
         (e) The impact to supply chain of customers

(f) Injury or death of customer (i.e. hospital patient)
(2) Financial impact
(a) Loss of revenue
(b) Additional costs to recover
(i) Declaration and daily usage fees
(ii) Overtime
(iii)Travel and expense
(iv)Insurance deductibles
(v) Replacing lost equipment, raw material and supplies
(c) Clean up and restoration cost
(d) Loss of financial control
(e) Impact to cash flow
(f) Impact to market share
(g) Impact on future sales
(h) Impact share price of stock
(i) Contractual fines or penalties
(j) Lawsuits
(3) Regulatory impact
(a) Fines
(b) Penalties
(c) Required to pull product off market due to loss of safety information
(4) Operational impact
(a) Reduced service levels
(b) Increased overtime costs
(c) Workflow disruptions
(d) Loss of control
(e) Inability to meet deadlines
(f) Supply chain disruption
(5) Reputational impact
(a) Media attention
(b) Social media
(c) Community
(d) Shareholder confidence
(e) Competitor taking advantage of negative attention
(6) Human impact
(a) Loss of life and injury
(b) Impact to the community
(c) Stress
(d) Long term emotional impact

2) Establish the BIA process and methodology.

DRII Professional Practices

- a) Identify and obtain a sponsor for the BIA activity.
- b) Define objectives and scope for the BIA process.
- c) Choose an appropriate BIA planning methodology/tool.
- d) Choose an appropriate BIA data collection methodology.
  - i) Data to be collected includes:
    - (1) Operational process.
    - (2) Impacts to the process and how those impacts change over time
      - (a) Impact to the process from loss of site
        - (i) Document current recovery capabilities
      - (b) Impact from loss of technology needed to perform the process
        - (i) Document current recovery capabilities
      - (c) Interdependencies
        - (i) Internal
        - (ii) External
        - (iii)Technology
      - (d) Minimum service levels
      - (e) Minimum resource requirements to perform function at the minimum acceptable level
        - (i) Technology
          - 1. Desktop hardware
          - 2. Network connectivity
          - 3. Printers
            - a. Standalone
            - b. Network
            - c. Mainframe
            - d. Color/black and white
          - 4. Fax machine
          - 5. Telephones
          - 6. Inbound/outbound trunk lines
          - 7. Print/file servers
          - 8. Applications
          - 9. Vendor software
          - 10. Internet connectivity
          - 11. Call recording
          - 12. Scanners
        - (ii) Physical space
          - 1. Physical desks
          - 2. Footprint needed for equipment
          - 3. Storage space for raw materials and finished product
          - 4. Shipping space

5. Print/mail space
6. Sorting space
7. Power requirements
8. HVAC requirements

(iii) Equipment

1. Manufacturing equipment
2. Print mail equipment
3. Photocopy machines
4. Tools

(iv) Vital records

1. Legal records
2. Contracts
3. Procedure manuals
4. Forms
5. Letterhead
6. Maintenance records
7. Insurance records
8. Product information

(v) Personnel

1. How many
2. What skills
3. What shifts
4. When

(vi) Supplies

1. Paper, pens, pencils, staplers, ink, toner, etc.
2. Raw materials

3) Plan and coordinate data gathering and analysis.

i) Data collection via questionnaires.

(1) Develop questionnaire and instructions as required.

(a) Understand the need for appropriate design and distribution of questionnaires, including explanation of purpose, to participating departmental managers and staff.

(2) Manage project kick-off meetings to distribute and explain the questionnaire.

(3) Support respondents during completion of questionnaires.

(4) Review completed questionnaires and identify those requiring follow-up interviews.

(5) Conduct follow-up discussions when clarification and/or additional data is required.

ii) Data collection via interviews.

(1) Provide consistency with the structure of each interview being predefined and following a common format.

(2) Ensure the base information to be collected at each interview is predefined.

(3) Enable each interviewee to review and verify all data gathered.

(4) Schedule follow-up interviews, if initial analysis shows a need to clarify and/or add to the data already provided.

iii) Data collection via workshop.

(1) Set a clear agenda and set of objectives.

(2) Identify the appropriate level of workshop participants and obtain agreement from management.

(3) Choose appropriate venue by evaluating location, facilities, and participant availability.

(4) Facilitate and lead the workshop or identify an appropriate resource to do so.

(5) Ensure workshop objectives are met.

(6) Ensure all outstanding issues at the end of the workshop are identified and the appropriate follow up is conducted.

4) Gain the leadership agreement on BIA methodology and the criteria to be used.

a) Identify and obtain agreement as to how potential financial and non-financial impact can be quantified and evaluated in each impact area.

b) Identify and obtain agreement on requirements for non-quantifiable impact information in each impact area.

c) Establish definition of the impact scale (e.g., high, medium, low) to be used during the data collection.

d) Obtain agreement from management on final time schedule.

e) Identify team members to participate in the BIA process.

i) Work with the BIA sponsor to identify the major areas of the entity including potential third party service providers.

ii) Working with the BIA sponsor to identify specific individuals to represent the major areas of the entity.

(1) Collect and review existing organizational charts.

(2) Identify functional management team members and appropriate third party provider representatives to participate in the data collection process.

iii) Inform the selected individuals of the BIA process and its purpose.

iv) Identify training requirements and establish a training schedule.

v) Train knowledgeable functional management representatives.

f) Conduct data collection.

5) Analyze the data collected against the approved criteria to establish RTO and RPO for each operational area and the technology that supports them.

a) Based on the data collected, determine the prioritization of processes/services.

b) Document interdependencies between each business process and the supporting infrastructure (data systems and related technology, supply chain management, third party partners and other resources).

i) Intradepartmental

ii) Interdepartmental

iii) External relationships

c) Determine the order of recovery for core and support business functions and technology.

6) Document minimum resource requirements for resumption and recovery of core and support business functions and their escalation over time.

a) Resource requirements to include:

i) Internal and external resources

ii) Owned versus non-owned resources

iii) Short versus long term resource needs

iv) Existing resources and additional resources required

(1) Key personnel

(2) Equipment

(3) Data

(4) Raw materials

(5) Other

b) Vital Records Management.

i) Document vital records in the entity, including paper and electronic, and establish when records will be needed during recovery.

ii) Evaluate existing backup and restoration procedures to identify any gaps between record recovery requirements and existing backup and restoration procedures.

c) Identify gaps between current recovery capabilities and requirements defined by the results of the BIA.

7) Prepare and present the BIA results to the entity's leadership and gain acceptance of the RTO and RPO for each process as defined by the results of the BIA.

a) Prepare draft BIA report using initial impact findings and identified gaps.

i) Provide a statement of entity mission, goals and objectives.

ii) Summarize the impact to the mission, goals and objectives that may result from a disruption.

iii) Provide a prioritized list of the processes and services of the entity and the RTO and RPO that resulted from the BIA.

(1) Include a summary of resource requirements over time to recover and resume operations.

(2) Include a gap analysis between current capabilities to meet the defined RTO and RPO and the needed capabilities.

iv) Issue draft report to participating functional representatives and request feedback.

    v) Review functional representative feedback and, where appropriate, revise findings accordingly, or add to outstanding issues.
    vi) Schedule a workshop or meeting with participating functional representatives and third party provider representatives to discuss initial findings, when necessary.
    vii) Ensure that initial findings are updated, as necessary, to reflect changes arising from these meetings.

b) Prepare final BIA report.

c) Prepare and submit formal presentation of BIA findings to entity's leadership.

d) Gain acceptance of the RTO and RPO for each process as defined by the results of the BIA.

DRII Professional Practices

Professional Practice Four - Business Continuity Strategies

The data that was collected during the BIA and Risk Evaluation is used in this professional practice to identify available continuity and recovery strategies for the entity's operations and technology. Recommended strategies must be approved and funded and must meet both the recovery time (RTO) and recovery point objectives (RPO) identified in the BIA. A cost benefit analysis is performed on the recommended strategies to align the cost of implementing the strategy against the assets at risk.

The Professional's Role in Professional Practice Four is as follows:

1. Utilize the data collected during the BIA and Risk evaluation to identify the available continuity and recovery strategies for the entity's operations that will meet the RTO and RPO identified during the BIA process.
2. Utilize the data collected during the BIA and Risk evaluation to identify the available continuity and recovery strategies for the entity's technology that will meet the RTO and RPO identified during the BIA process.
3. Consolidate strategies where appropriate to reduce costs and/or complexity.
4. Assess the cost of implementing identified strategies through a cost/benefit analysis.
5. Recommended strategies and obtain approval to implement.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1. Utilize the data collected during the BIA and Risk evaluation to identify the available continuity and recovery strategies for the entity's operations that will meet the RTO and RPO identified during the BIA process.
    a. Review recovery requirements identified for each of the entity's operations.
    b. Identify alternative business continuity strategies. Potential options include but are not limited to:
        i. Do nothing and repair or rebuild at time of disaster
        ii. Develop manual workaround procedures
        iii. Develop reciprocal agreements (more common in small business operations, public sector mutual aid agreements and manufacturing environments)
        iv. Identify internal dual usage space that could be equipped to support recovery (conference rooms, training rooms, cafeterias, etc.)
        v. Identify an external alternate site
        vi. Contract with third party service providers / outsourcers

vii. Transfer workload to a surviving site

viii. Transfer staff and workload to a surviving site

ix. Suspend operations that are not time sensitive in a surviving site and transfer people/workload from the impacted site (displacement)

x. Build dedicated alternate site

xi. Have staff work from home

xii. Recovery strategies for manufacturing environments

1. Repair/Rebuild at time of disaster
2. Reciprocal agreements with other manufacturer
3. SKU prioritization
4. Customer prioritization
5. Utilize excess capacity in other plants

xiii. Strategies for the recovery of vital hard copy records and work in process to meet the RPO for these records and to ensure they are accessible following a disaster.

1. Photocopy
2. Scan
3. Fiche
4. Film

c. Review alternate site alternatives

i. Location

ii. Available space

iii. Suitability of space to need

iv. Communications capabilities (voice/data)

v. Equipment available

vi. Availability of raw materials

vii. Hardness of the site (redundant power, water, etc.)

d. Assess viability of alternative strategies against the results of business impact analysis/recovery time objectives

i. Compare solutions

ii. Advantages

iii. Disadvantages

iv. Costs (startup, maintenance & execution)

v. Mitigation capability and control options

vi. Ability to meet defined RTO and RPO

e. Develop preliminary cost/benefit analysis

2. Utilize the data collected during the BIA and Risk evaluation to identify the available continuity and recovery strategies for the entity’s technology that will meet the RTO and RPO identified during the BIA process.

a. Review recovery requirements identified for the technology that supports each of the entity's operations.

b. Identify alternative technology recovery strategies. Potential options include but are not limited to:

   i. Do nothing and repair or rebuild at time of disaster.

   ii. Have business operations develop manual workaround procedures.

   iii. Implement active/active technology environment through a dual data center eliminating the need for recovery.

   iv. Implement active/passive technology environment for high availability of time sensitive technology providing for quick restart of the required technology.

   v. Contract with third party service providers / outsourcers to provide technology recovery environment. This includes:

      1. A traditional "Hot Site" contract with a vendor where the vendor provides the equipment to recover from their inventory

      2. The entity puts their own equipment for recovery on the floor of the vendor's data center

   vi. Outsource the entire technology environment (cloud computing, etc.).

   vii. Identify site where recovery would occur but build-out only HVAC and electrical capabilities and populate with technology at time of disaster (warm site).

   viii. Identify site where recovery would occur but build-out only at time of disaster (cold site).

   ix. Identify strategies for recovery of data in electronic form that meets the RPO established for these records and ensures they are available following a disaster.

      1. Physical and Virtual Tape backup

         a. Incremental

         b. Full backup

         c. Differential

      2. Asynchronous replication

      3. Synchronous replication

c. Review alternate site alternatives

   i. Location

   ii. Available space

   iii. Suitability of space to need

   iv. Communications capabilities (voice/data)

   v. Equipment available

   vi. Hardness of the site (redundant power, water, etc.)

- d. Assess viability of alternative strategies against the results of BIA recovery objectives.
    - i. Compare solutions
    - ii. Advantages
    - iii. Disadvantages
    - iv. Costs (startup, maintenance & execution)
    - v. Mitigation capability and control options
    - vi. Ability to meet defined RTO and RPO
- e. Develop preliminary cost/benefit analysis

3. Consolidate strategies where appropriate to reduce costs and/or complexity.
    - a. Identify where the same recovery strategy could be used to meet the requirements for multiple areas of operations (i.e. A single alternate site used for recovery of business operations from different buildings that are not expected to be impacted by the same event)
4. Assess the cost of implementing identified strategies through a cost/benefit analysis.
    - a. Estimate the cost of implementing and maintaining recovery for the identified recovery strategies
    - b. Validate that the recovery strategy being implemented is in line with the amount of business at risk (Example: you would not implement a million dollar recovery strategy to protect $100,000 of business)
5. Recommended strategies and obtain approval to implement.

DRII Professional Practices

Professional Practice Five – Emergency Preparedness and Response

This professional practice defines the requirements to develop and implement the entity's plan for response to emergency situations that may impact safety of the entity's employees, visitors or other assets. The emergency response plan documents how the entity will respond to emergencies in a coordinated, timely and effective manner to address life safety and stabilization of emergency situations until the arrival of trained or external first responders.

The Professional's Role in Professional Practice Five is as follows:

1) Identify applicable emergency preparedness and response regulations.
2) Identify potential types of emergencies, scenarios that may occur and impacts that may result.
3) Identify the response capabilities needed.
4) Review existing emergency response procedures and assess capabilities to protect life, property, and the environment.
5) Recommend the development/improvement of emergency procedures.
6) Recommend the development and implementation of an incident management system for command, control, and coordination of personnel and resources during emergencies.
7) Review and coordinate emergency preparedness and response plans and procedures with trained, professional first responders

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1) Identify applicable emergency preparedness and response regulations.
    a) Health and safety
    b) Fire prevention
    c) Life safety
    d) Homeland security
    e) Environmental protection
    f) Regulations promulgated by federal, state, provincial, county, parish, tribal or local levels of government
    g) Regulations applicable because of:
        i) Hazards on-site
        ii) Size, height, or arrangement of a building
        iii) Location (e.g., proximity to waterways)

2) Identify potential types of emergencies, scenarios that may occur and the impacts that may result
    a) Natural, human-caused (accidental and intentional), and technological. For each type of emergency, identify potential scenarios that may result.
        i) Origin or location (internal or external)
        ii) Size or magnitude
        iii) Area if impact

b) For each type of emergency, identify potential impacts including:
  i) Casualties
  ii) Property damage
  iii) Operational interruption or disruption
  iv) Environmental contamination

3) Identify the response capabilities needed.
  a) Capabilities needed to protect life safety including:
    i) Evacuation
    ii) Sheltering
    iii) Shelter-in-Place (i.e. exterior airborne hazard)
    iv) Lockdown
    v) Accounting for all persons affiliated with the organization and affected by the emergency
    vi) Triage, treatment (first aid, CPR/automated external defibrillator), and transport of injured or ill
    vii) Rescue including search and rescue
  b) Capabilities needed to protect property including:
    i) Supervision and manipulation of building systems and equipment including utilities, ventilation and air conditioning, fire detection and suppression, and communications and warning.
    ii) Property conservation to prepare a facility for a forecasted event (e.g., orderly shutdown in advance of a hurricane) and to minimize damage with salvage and cleanup following an event.
    iii) Firefighting (e.g., incipient fire brigade, coordinated planning with public fire department, fire extinguisher training, etc.)
  c) Capabilities needed to prevent environmental contamination.
    i) Documentation, supervision, and manipulation of process systems, containment systems, and other systems designed to contain hazardous materials on-site

4) Review existing emergency response procedures and assess capabilities to protect life and property.
  a) Information Gathering
    i) Identify the response capabilities required to protect life, property, and the environment for the types of emergencies, scenarios, and impacts identified.
    ii) Identify and establish relationships with the internal departments and personnel and external agencies, contractors, and others with responsibility for emergency preparedness and response.
    iii) Gather emergency response procedures from internal departments and those assigned responsibility for emergency response including environmental, health, safety, security, human resources, facilities management, and operations.
    iv) Gather emergency response procedures and a description of emergency response capabilities from external sources including any building manager.
    v) Contact public agencies (e.g., emergency medical services, fire department, law enforcement, rescue, hazardous materials team, emergency management agency, etc.) to identify requirements, practices, and resources, and to open lines of communication. (Also see Professional Practice Ten).
  b) Resource Needs Assessment

i) Identify the resources needed to protect life, property, and the environment from the types of emergencies, scenarios, and impacts identified.
ii) Identify the internal and external personnel including public agencies, building managers, contractors, and others that are trained to respond to the emergencies identified.
iii) Identify the systems and equipment including detection, alarm, warning, communications, means of egress (i.e., exits), suppression, and containment systems available for emergency response.

c) Identify materials and supplies needed for emergency response.
d) Verify that mutual aid or partnership agreements are documented.
e) Assess the availability and capabilities of identified resources to determine whether the resources can be provided in a timely manner and are adequate to protect life, property, and the environment from the types of emergencies, scenarios, and impacts identified.
f) Review emergency response plans to determine whether the types of emergencies, scenarios, and impacts identified have been adequately addressed to protect life, property, and the environment.
g) Review emergency response plans to determine whether procedures adequately address hazard or threat monitoring, incident detection; prompt reporting to responsible person, department, and or agency; plan activation; alerting of first responders (internal and or external), warning of persons impacted or potentially impacted; and escalation as required to stabilize the incident.
h) Consult with public agencies (e.g., emergency medical services, fire department, law enforcement, rescue, hazardous materials, emergency management, etc.) to coordinate emergency preparedness and response as required by Professional Practice 10.
i) Document discrepancies and/or gaps between needs and capabilities.

5) Recommend the development/improvement of emergency procedures.

a) Report significant discrepancies between the procedures, resources, and capabilities required for emergency preparedness and the procedures, resources, and capabilities currently available to management.
b) Provide prioritized recommendations to address the discrepancies or fill the gaps.
c) Solicit management support and commitment for required resources. The goal of the program in order of priority should be to protect life, property, and the environment from the types of emergencies, scenarios, and impacts identified.

i) Protection of Life Safety

(1) Warning - Establish a capability to promptly warn persons at risk or potentially at risk from a threat or hazard. Warning systems should be compliant with applicable regulations and capable of being heard and understood.
(2) Protective Actions - Organize team(s) to evacuate, shelter, or shelter-in-place (from an exterior airborne hazard). Establish procedures for and a capability to warn persons at risk from security threats that may require lockdown.
(3) Rescue - Arrange for a competent rescue capability to provide rescue services if required by regulation based on the hazards on-site (e.g., permit-required confined space). Establish a search and rescue capability if required by the types of emergencies, scenarios, and impacts identified and the availability or capability of external resources is inadequate.

(4) Accountability - Establish a capability to account for the safety and well-being of all persons affiliated with the organization engaged in an incident or who may be affected by an incident.

(5) Medical - Ensure there is an internal and or external capability compliant with regulations to promptly administer first aid or medical treatment and transport the sick or injured to a medical facility with the capability of treating injuries or illnesses that may occur at the facility.

(6) Counseling - Identify or provide access to mental health professionals who can provide counseling and related services following a traumatic incident.

(7) Security - Maintain or provide site, building, and or area security for protection of personnel, physical assets, and information during and following an incident.

ii) Property Protection

(1) Establish capabilities, document plans, and provide required resources to prepare facilities for forecast events identified. These events may include but are not limited to natural hazards (flood, tropical cyclone, etc.) and warning for human-caused events (e.g., civil disturbances, etc.).

(2) Establish capabilities to supervise building systems, utilities, and equipment to stabilize an incident in conjunction with building management, public agencies, or others who may be involved with the incident. This includes documenting systems, utilities, and equipment, and ensuring competent persons area available to manipulate systems as required by the incident or as directed by the incident commander.

(3) Establish capabilities, document plans, and provide required resources to stabilize incidents identified that have the potential to damage property or interrupt or disrupt business operations. The goal is to safely protect facilities, equipment, and contents and minimize damage while or after actions are taken to protect life safety.

(4) Establish capabilities, document plans, and provide (internal or external) resources for salvage, cleanup, and loss mitigation following a property damage incident.

(5) Coordinate with or establish links to the operators of critical infrastructure (e.g., roads, bridges, utilities, etc.) to provide information regarding the capabilities, availability, and restoration of infrastructure required to operate the facility.

iii) Environmental Protection

(1) Compile an inventory of hazardous materials that includes location and quantity. Ensure that Material Safety Data Sheets (MSDS) have been compiled as required by “Right to Know” or Hazard Communication regulations and the sheets are immediately accessible to emergency responders.

(2) Establish capabilities as required by regulations and provide required resources to minimize the potential environmental impacts of the hazards identified. These events may result in spills of hazardous materials, ruptures of piping or tanks, failure of process systems that release hazardous materials, or loss of containment.

(3) Document process systems, tanks, piping, and or containment of hazardous materials; establish procedures for preventing spills or releases; develop plans to stabilize an incident; and ensure competent persons area available to work in

conjunction with building management, public agencies (e.g., hazardous materials response teams), contractors, or others who may be involved with the incident.

iv) Crisis Communications
(1) Coordinate crisis communications planning between the emergency preparedness and response plan and emergency organization with the Crisis Communications Program and crisis communications team described in Professional Practice 9 "Crisis Communications."
(2) Identify a spokesperson authorized by management and capable of speaking on behalf of the organization to local audiences as part of the "public information" position of the incident management system and as part of any joint information center with public agencies.
v) Damage Assessment
(1) Emergency preparedness and response plans should include procedures for situation analysis and damage assessment in accordance with the entity's incident management system.
(2) Identify qualified persons with knowledge of the organization and its facilities and operations to assess interruption/disruption of operations and property damage.
(3) Organize a damage assessment team and develop a method to facilitate prompt identification of damage and to assess interruption/disruption and protocols for communication of situation reports to management and others (e.g., business continuity organization, crisis management team, etc.).

6) Recommend the development and assist with the implementation of an incident management system for command, control, and coordination of personnel and resources during emergencies.
a) Incident Management System
i) Develop and assist with the implementation of an incident management system that defines organizational titles, roles, lines of authority, succession of authority, and responsibilities for internal and external resources (e.g., corporate/business unit, departments, managers, supervisors, public agencies, contractors, etc.).
ii) Protocols and procedures for escalation; the engagement of additional internal and external services; and procurement of additional resources should be addressed within the incident management system.
iii) The system should include policies and procedures for activation of the incident management system, opening of the emergency operations center, communications and coordination with on-scene incident command, and coordination of emergency preparedness and response activities with continuity and recovery activities.
iv) Incident management should include initial and periodic situation analysis and should be guided by an incident action plan to achieve the goals of protective actions for life safety, property protection, business continuity, and recovery.
b) Emergency Operations Center
i) A physical or virtual emergency operations center (EOC) should be established and equipped to facilitate coordination of response, continuity, and recovery activities.
ii) Communications capabilities (e.g., two-way radio, email, text messaging, pagers, landline and wireless voice and data communications, etc.) necessary to support

incident management should be provided within the EOC. Communications capabilities should include the ability to gather information from internal and external sources, coordinate activities, and dissemination instructions and information.

iii) Communications during an incident should be documented.

iv) The EOC should be sized to house the anticipated number of persons; arranged to facilitate information gathering, processing, communications, and decision-making; and equipped to support occupancy for the duration of the types of emergencies and scenarios identified.

v) Security for the EOC should be implemented.

vi) Operating procedures should include identification, assignment, and scheduling of persons to fulfill emergency operations center functions and activities in accordance with the entity's incident management system.

vii) Operating procedures should include management and operations of the EOC; communications protocols, procedures, and information flow; and closure of the EOC.

7) Review and coordinate whether emergency preparedness and response plans and procedures have been reviewed by, and coordinated with, first responders

a) Identify the documents (e.g., fire prevention, hazardous materials management plan, integrated contingency plan, spill prevention and countermeasures, EPA risk management plan, etc.) that must be submitted to public agencies to comply with regulations.

b) Determine whether emergency preparedness and response plans have been submitted to external public agencies (e.g., emergency services such as fire departments, emergency medical services, rescue service, hazardous materials response team or contractor, law enforcement, environmental authorities, and other regulatory bodies) identified in Table 1 to comply with regulatory requirements and others (e.g., building manager, tenants, etc.) for the purpose of coordination.

c) Assist with the coordination of response protocols, plans, and procedures with public agencies and external resources. Coordination should include response to, coordination during, and recovery from, an incident. Authorization to, and credentials for, facility access following an incident should be determined.

Table 1. Coordination of Plans with Public Agencies

Agency		Plan to be Reviewed
Fire Dept.	Local or county	Evacuation, fire, hazmat, rescue, bomb threat, suspicious package, special events
Local Emergency Planning Committee	Local or regional	Hazard materials response plan
Law Enforcement	Local, county, or state	Bomb threat, suspicious package, labor strife, civil disturbance, special events
Emergency Medical Services	Ambulance, paramedics, fire dept., private service	Medical emergencies, hazmat
Emergency Management	Local or county	Hurricane, tornado, earthquake, flood, regional disasters

DRII Professional Practices

Professional Practice Six - Business Continuity Plan Development and Implementation

The Business Continuity Plan is a set of documented processes and procedures which will enable the entity to continue or recover time sensitive processes to the minimum acceptable level within the timeframe acceptable to the entity. In this phase of the Business Continuity Management Program, the relevant teams design, develop, and implement the continuity strategies approved by the entity and document the recovery plans to be used in response to an incident or event.

The Professional's Role in Professional Practice Six is as follows:

1) Design, develop and implement agreed upon recovery strategies.
2) Design framework and define document structure for the plan documentation.
3) Coordinate the effort to document recovery plans for the entity's operations and the technology that supports them.
4) Publish the plan documents.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1) Design, develop and implement agreed upon recovery strategies.
    - a) Work with the planning team to design, develop and implement recovery strategies for the entity's operations.
        - i) Work with business partners and vendors as appropriate.
        - ii) Manage the budget for strategy implementation.
        - iii) Report progress to Steering Committee.
        - iv) Ensure required tasks are completed for plan implementation that may include the following:
            - (1) Acquiring specified / planned recovery/business continuity resources, e.g. additional equipment, system, supplies, services, etc.
            - (2) Execution of response/recovery/restoration/business continuity required contractual arrangements.
            - (3) Appropriate documentation access for plan-in-place.
    - b) Work with the technology planning team to design, develop and implement strategies for recovery of the entity's technology.
        - i) Work with technology partners and vendor as appropriate.
        - ii) Manage budget for strategy implementation.
        - iii) Report progress to Steering Committee.
        - iv) Ensure required tasks are completed for plan implementation that may include the following:
            - (1) Acquiring specified / planned recovery/business continuity resources, e.g. additional equipment, system, supplies, services, etc.
            - (2) Execution of response/recovery/restoration/technology contractual arrangements.

        - (3) Appropriate documentation access for plan-in-place.
- 2) Design framework and define document structure for the plan documentation.
    - a) Determine how the plan will be organized and identify the teams needed to document the plans.
        - i) Organization – Decide how the plan will be organized.
            - (1) Enterprise-wide
            - (2) By site
            - (3) By business line
            - (4) By product line
            - (5) By service provided
            - (6) By technology
        - ii) Teams – individual experts needed to document recovery procedures. To include but not limited to:
            - (1) Business process experts from each process to be recovered
            - (2) Voice and data network
            - (3) Application support
            - (4) Storage management
            - (5) Equipment
            - (6) Human resource
            - (7) Finance
            - (8) Print and mail services
            - (9) Vendor management
            - (10) Records management
        - iii) Types of plans to be documented to include but not limited to:
            - (1) Strategic including succession planning
            - (2) Tactical
            - (3) Operational
            - (4) Emergency response
            - (5) Incident control and damage assessment
            - (6) Continuity and recovery
            - (7) Return-to-normal operations
        - iv) Planning Scenarios to be used during plan documentation may include but not limited to:
            - (1) Short-term (less than 1 month outage)
            - (2) Long-term (more than 3 month outage)
            - (3) Local (Site or campus specific)
            - (4) Regional impact
            - (5) Enterprise-wide impact
            - (6) Cascading impact potential
    - b) Define Roles and Responsibilities for Plan Development.
        - i) Identify tasks to be undertaken.
        - ii) Create action plans / checklists for plan development.

iii) Develop timeline for plan completion.

iv) Review, evaluate and recommend tools e.g. planning software, database(s), or specialized software, templates, etc.

v) Develop templates to be used to acquire information on processes, technology matrices and flowcharts.

vi) Identify other supporting documentation needed.

vii) Ensure built-in mechanisms to facilitate maintenance, e.g. version control.

c) Define table of contents for the plan documentation which may include but is not limited to:

i) Introduction

ii) Policy Statements

(1) Business Continuity policies

(2) Confidentiality Statement

iii) Scope / Objectives

(1) Tied to organizational mission, goals and objectives and business continuity policies

(2) Identification of time sensitive operations and the technology that supports them covered in this plan document

iv) Assumptions/exclusions made during the planning process

v) Recovery team description, organizational structure, and the responsibilities of each team

vi) Plan activation procedures

(1) Event notification

(2) Event assessment process

(3) Declaration procedures

(4) Escalation and mobilization procedures

vii) Restoration and recovery procedures

3) Coordinate the effort to document recovery plans for the entity's operations and the technology that supports them.

a) Emergency Plan / Incident Management Plan (see Professional Practice 5)

(1) Life safety procedures

(2) Incident command and control Procedures

(3) Roles and responsibilities

(4) Emergency Operations Center (EOC) location and activation

b) Damage assessment

(1) Initial damage assessment report to assist in decision process

(2) Full damage assessment

(a) Protecting site from further loss

(b) Economics of repair versus replacement

(c) Time to repair/replace versus plan activation

(d) Agreed upon restoration methods for business assets (e.g., equipment, electronics, documents, data, furnishings, premises, plant, computers, etc.).

- (e) Approval process for restoration and the implications of warranties.
- (f) Salvage process.

c) Crisis Management and Communication Plan (see also Professional Practice 5 and 9)

- (1) Identify crisis management team.
- (2) Procedures to transition from emergency response to crisis management and business continuity.
- (3) Documented procedures for communication to stakeholders throughout event.
    - (a) Notification procedures
    - (b) Status updates
    - (c) Media Releases
    - (d) Targeted Communications (Stakeholder)
        - (i) Media
        - (ii) Employees and their families
        - (iii) Regulatory bodies, emergency first-responders, agencies, special hazmat services
        - (iv) Investor relations
        - (v) Labor relations
        - (vi) Relations with other involved groups (example(s) include customers, vendors, suppliers, etc.).

d) Recovery site activation.

- (1) Declaration procedures
- (2) Recovery infrastructure provided that may include:
    - (a) Administration/logistics
    - (b) New equipment or just-in-time drops
    - (c) Technical services and procedures, such as
        - (i) Communication networks (voice, data, wireless, etc.)
        - (ii) Data preparation
        - (iii) Application support
        - (iv) End user liaison
    - (d) Business operations
    - (e) Inter-site logistics and communications
    - (f) Production recovery process and procedure

e) Operational / Recovery Plans

- (1) Recovery Teams
    - (a) Primary and alternates
- (2) Logistics
    - (a) Travel and housing recovery staff
    - (b) Transporting data needed for recovery
    - (c) Procurement of additional resources
- (3) Required Resources
    - (a) Desktop requirements
    - (b) Vital records

- (c) Voice and data communications
- (d) Key contacts / suppliers
- (e) Equipment requirements

f) Business Continuity Plan
- (a) Alternative ways to conduct business when normal resources are unavailable
- (b) Business continuity processes, procedures and communication
- (c) Mobilizing alternate resources
- (d) Managing alternate resources

g) Technology Recovery Plans
- (1) Recovery teams
  - (a) Primary and alternates
- (2) Mobilizing resources
  - (a) Logistics
    - (i) Travel and housing recovery staff
    - (ii) Transporting data needed for recovery
    - (iii)Procurement of additional resources
- (3) Required Resources
  - (a) Data and storage requirements
    - (i) SAN
    - (ii) NAS
    - (iii)Tape
  - (b) Voice and data communications hardware
    - (i) Network bandwidth
    - (ii) Phone switch
    - (iii)Call recording
    - (iv)Routers
  - (c) Hardware and software requirements
    - (i) Server
    - (ii) Mainframe
    - (iii)Tape drives/tape silo/virtual tape library
    - (iv)Application software
    - (v) Operating systems
    - (vi)Scheduling system
    - (vii) Source code
    - (viii)
  - (d) Infrastructure requirements
    - (i) Power/PDU
    - (ii) Generator/UPS
    - (iii)Cooling
    - (iv)Cabling
    - (v) Footprint
    - (vi)Security

- (e) Information security requirements
  - (i) Firewalls
  - (ii) Authentication
  - (iii)Virus protection
  - (iv)Encryption
- (f) Key contacts / suppliers
- (g) Equipment requirements

(4) Technology recovery plan (supporting processes)

- (a) Detailed step by step procedures for recovery of technology environment
- (b) Application interdependencies
- (c) Change management
- (d) Problem management
- (e) Testing/Exercise / Maintenance
  - (i) Exercise requirements
  - (ii) Scope, objectives and schedule
  - (iii)Plan maintenance program

4) Publish plan documents.

- a) Provide final draft to plan development teams / business process owners.
- b) Obtain executive management sign-off.
  - i) Publish and distribute plans or portions of the plans to everyone who has a documented role. (The information necessary for each participant to execute their role).
- c) Establish procedures for distribution and control of plans, e.g. distribution list.
- d) Establish procedures for distribution and control of plan changes and updates.

DRII Professional Practices

Profession Practice Seven - Awareness and Training Programs

In this professional practice, a program is developed and implemented to establish and maintain awareness about the Business Continuity Management (BCM) Program and to train the entity's staff so that they are prepared to respond during an event.

The Professional's Role in Professional Practice Seven is as follows:

1) Establish objectives of BCM awareness and training program.
2) Identify functional awareness and training requirements.
3) Identify appropriate internal and external audiences.
4) Develop awareness and training methodology.
5) Identify, acquire or develop awareness and training tools.
6) Identify external awareness and training opportunities.
7) Oversee the delivery training and awareness activities.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1) Establish objectives and components of BCM awareness and training program.
    a) Obtain support of senior management.
    b) Secure adequate budget.
    c) Define program management approach and implementation timeframes.
    d) Obtain commitment from managers and operational staff.
    e) Align BCM training to recovery priorities.
2) Identify functional awareness and training requirements.
    a) Identify and document the BCM roles and responsibilities requiring training.
    b) Define the desired level of awareness based on responsibilities.
    c) Identify desired level of expertise to be achieved through training.
3) Identify appropriate internal and external audiences.
    a) Identify and prioritize internal groups and their awareness and training needs.
        i) Management.
            (1) Incident management training.
            (2) Understanding BCM Program components.
        ii) Team members (including all employees to be engaged at a basic level).
            (1) How they will be notified of an event.
            (2) Responding to specific threats or events.
            (3) Knowing what to do when evacuated from the work site.
            (4) Having knowledge of recovery plans and their role.
            (5) New employee orientation.

(6) Training specific to their role.
b) Identify and prioritize external target groups.
i) Key stakeholders.
ii) Third parties.
4) Develop Awareness and Training Methodology.
a) Conduct awareness and training needs assessment.
i) Conduct awareness and training surveys or other means of assessing current state of awareness and readiness.
ii) Gain feedback through focus groups.
iii) Identify trends and new developments.
iv) Review previous tests/ exercise results and gap analyses.
b) Benchmark current levels of awareness and readiness against desired levels.
c) Initiate plan to address awareness and training gaps.
d) Design the training process.
i) Identify delivery methods.
(1) Awareness campaigns.
(2) Web based training.
(3) Internal web site.
(4) Instructor led training.
(5) Scenario based training.
(6) Instructional guides and templates.
(7) Briefing papers, newsletters, bulletins, articles.
(8) Train the trainer sessions.
(9) Continuity and incident management exercises.
ii) Define training roles and responsibilities.
iii) Prioritize teaching points defining the BCM message to be assimilated.
iv) Select order and delivery methods.
5) Identify, develop or acquire awareness and training tools and resources.
a) Identify internal training resources.
b) Contract with external vendors for training.
c) Purchase training software packages.
d) Develop and implement BCM website.
e) Utilize social media tools (LinkedIn, Facebook, Twitter, YouTube etc.).
f) Develop and distribute brochures of frequently asked questions.
g) Create awareness posters.
h) Purchase and distribute awareness promotional items (magnets, pens, flashlights, etc.).
i) Develop training courseware.
6) Identify external awareness and training opportunities.
a) Conferences
b) Seminars

   c) User groups and associations
   d) White papers/publications
   e) Regional networks and working groups
   f) Industry sector working groups
   g) Certification bodies
   h) Formal academic education programs
   i) Awareness special events

7) Oversee the delivery training and awareness activities.
   a) Schedule and deliver training activities.
   b) Schedule and conduct awareness activities.
   c) Monitor effectiveness of the awareness and training activities.
   d) Review results and provide report to leadership on activities.

DRII Professional Practices

Professional Practice Eight - Business Continuity Plan Exercise, Audit, and Maintenance

The goal of this professional practice is to establish an exercise, testing, maintenance and audit program. To continue to be effective, a Business Continuity Management (BCM) Program must implement a regular exercise schedule to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization. As part of the change management program, the tracking and documentation of these activities provides an evaluation of the on-going state of readiness and allows for continuous improvement to recovery capabilities and ensure that plans remain current and relevant. Establishing an audit process will validate the plans are complete and accurate and in compliance with organizational goals and industry standards as appropriate.

The Professional’s Role in Professional Practice Eight is as follows:

1. Establish an exercise/testing program.
2. Establish a plan maintenance program.
3. Identify or establish appropriate industry and/or organizational standards.
4. Establish a business continuity program audit process.
5. Communicate exercise/test/audit results and recommendations.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1. Establish an Exercise/Testing Program
    a. Develop an exercise program that meets the entity’s continuity objectives.
        i. Align with the entity’s strategy and tactical requirements.
        ii. Provide a high level of confidence for the continuity ad recovery of operations.
    b. Obtain executive sponsorship for exercise/testing program development.
    c. Develop a realistic, progressive and cost effective program.
        i. Document the exercise/testing standards and guidelines to be used.
        ii. Defined exercise/testing program assumptions and limitations.
        iii. Identify exercise types to be included that will create a comprehensive exercise program based on the recovery strategies implemented and the RTO and RPO defined by the entity for its operations. These may include operational, facility and technical exercises and testing such as:
            1. Life safety exercises
            2. Plan walk–through / tabletop review

3. Scenario based tabletop exercise
4. Call notification exercise
5. Alternate site exercise
6. Standalone platform, infrastructure or application recovery test
7. Full end to end functional exercise of an operation or technology
8. Comprehensive exercise of all recovery strategies required to recover the time sensitive operations and technology from a single site
9. Integrated technology exercise with internal and external interdependencies

iv. Identify participants, roles and responsibilities in the exercise/test program.

1. Recovery team(s)
2. Observers/reporters
3. Time keepers
4. Auditor/reviewers
5. Facilitator
6. Suppliers
7. Out-sourced services and providers

v. Define exercise program objectives and select appropriate scenarios.

1. Approximate the types of incidents the organization is likely to experience. Include suitable activities to exercise various facets of the recovery strategies, example(s):
   a. Technical - Does the equipment work?
   b. Procedural - Are the procedures correct?
   c. Logistical - Can people access the recovery facility and execute their recovery procedures?
   d. Timelines - Can the required RPO/RTOs be achieved?

vi. Determine exercise requirements for each exercise to be conducted.

1. Define and document exercise objectives
2. Define and document in-scope/out-of-scope requirements
3. Define exercise notification process.
   a. Announced/planned
   b. Unannounced/surprised

vii. Schedule exercises/tests to be conducted.

1. Develop a multi-year progressive schedule building on lessons learned and mastery of recovery processes.
2. Develop specific schedule for exercises and tests to be conducted on an annual basis or as frequently as necessary to ensure competency and to meet regulatory requirements.

DRII Professional Practices

viii. Define and document evaluation criteria aligned with exercise objectives and scope:
  1. Quantitative
  2. Qualitative

ix. Identify pre - exercise activities
  1. Identify resources required to conduct the exercise.
  2. Identify participants (example(s): business unit contacts, IT representatives, umpires, adjudicators, etc.).
  3. Ensure all understand the objectives of the exercise and their roles.
  4. Provide an inventory of hardware, software and physical assets required for the exercise (examples: PC/laptop, Security access, telephone, applications, printers, etc.).
  5. Document and communicate specifications for the exercise environment.
  6. Specify production vs. test environments.
  7. Time for test - business day vs. weekend.
  8. Provide a timetable of events and circulate to all participants, facilitators and adjudicators.
  9. Establish “back-out” or test/exercise cancellation plan.

x. Conduct exercise.
  1. Should an incident occur during an exercise you should have a predetermined mechanism for cancelling the exercise and invoking the actual continuity process.
  2. Record exercise process.
  3. Document exercise results via the activation and maintenance of the issues log.
  4. Declare end of exercise.
  5. Shut down procedures.
  6. Perform clean-up activities.

xi. Identify post exercise activities.
  1. Conduct debriefing sessions to review exercise results and identify actions for improvements.
  2. Post-exercise reporting.
  3. Provide a comprehensive summary with recommendations.
  4. Document action plan report.
  5. Identify open issues.
  6. Identify actionable items with responsibilities and timeframes for resolution.

      7. Monitor (and escalate where necessary) progress to completion of agreed actions.
      8. Communicate exercise results.
      9. Document lessons learned.
      10. Document expected versus actual results.
      11. Document unexpected results.

2. Establish plan maintenance program.
   a. Define plan maintenance method and schedule.
      i. Define ownership of plan data.
      ii. Prepare maintenance schedules and review procedures.
      iii. Select maintenance tools.
      iv. Monitor maintenance activities.
      v. Establish plan update process.
      vi. Ensure that scheduled plan maintenance addresses all documented recommendations.
   b. Define change control process
      i. Analyze business changes with planning implications.
      ii. Develop change control procedures to monitor changes (utilize existing change control process if already in place).
      iii. Create proper version control; develop plan re-issue, distribution, and circulation procedures.
      iv. Identify plan distribution lists for circulation.
      v. Develop a process to update plans based on response to audit findings.
      vi. Set guidelines for feedback of changes to planning function.
      vii. Implement change control process.
3. Identify or establish appropriate standards.
   a. Review appropriate industry (NFPA, ISO, ANSI, etc.) and national/international (US, British, Australian, etc.) standards.
   b. Review process owner expectations based on industry standards and organizational as well as "client" service expectations.
   c. Develop an organizational standard with a recurring review and enhancement/continuous improvement process.
   d. Based on industry and/or national/international standards as well as organizational and/ or client expectations.
   e. Frequency and scope appropriate for the organization.
   f. Approved by leadership.
4. Establish a business continuity program audit process.
   a. Define schedule for self-assessment audit.

   b. Prepare to support other audits which may occur.
      i. Internal audit
      ii. External audit
      iii. Second-party audit
   c. Document audit standards and guidelines.
      i. Select/develop any needed audit tools.
      ii. Establish audit schedule.
      iii. Conduct/monitor audit activities.
      iv. Audit the plan structures, contents, and action sections.
         1. Audit program requirements, documents and standards.
         2. Audit templates and plan.
         3. Audit test requirements and results.
         4. Audit repository for plan and test results.
         5. Audit the plan documentation control procedures.
         6. Audit version control process and documentation.
         7. Audit distribution lists and associated processes.
         8. Audit change control process.
      v. Review management response to audit findings.
      vi. Confirm responses have been submitted and action plans documented.
      vii. Verify completed actions have been captured in the plan and supporting documentation.

5. Communicate exercise/test/audit results and recommendations.
   a. Identify appropriate stakeholders.
      i. Process owners
      ii. Governance coordinators
      iii. Senior leadership/operations oversight
   b. Select appropriate communication methods and communicate in a timely manner.
      i. Reporting level of detail
      ii. Where appropriate, consider graphic representations or comparison reports targeted by audience
   c. Establish a feedback/validation loop to confirm appropriate actions have been taken as a result of reported findings.
      i. Issues tracking
      ii. Date item opened
      iii. Owner of issue
      iv. Date item closed

DRII Professional Practices

Professional Practice Nine - Crisis Communications

This professional practice provides the framework to identify, develop, communicate and exercise a crisis communications plan to address how communications will be handled by the entity before, during and after an event. The crisis communications plan is developed collaboratively with the entity's public information and internal information resources where they exist to ensure consistency of the entity's communications. The plan will address the need for effective and timely communication between the entity and all the stakeholders impacted by an event or involved during the response and recovery efforts.

The Professional's Role in Professional Practice Nine is as follows:

1) Design, develop and implement a crisis communications plan.
2) Communicate and train stakeholders on roles and responsibilities for the crisis communications plan.
3) Exercise the crisis communications plan.
4) Maintain the crisis communications plan as defined in Professional Practice 8.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1) Design, develop and implement a crisis communications plan.
    a) Identify existing public information and internal information resources within the entity.
    b) Collaborate with public information and internal information resources to design the plan.
        i) Define objectives, scope and plan structure.
        ii) Review the organization's existing crisis communications plan.
        iii) Identify and document gaps in the existing plan.
        iv) Using results of the Risk Assessment in Professional Practice 2, identify potential events for which communications should be planned.
        v) Establish roles and responsibilities for the crisis communication team.
            (1) Use EOC as a location to control what message goes out and when
            (2) Internal information
            (3) Public Information
            (4) Media spokesperson
        vi) Identify all stakeholders to be considered during the development of the crisis communication plan and the appropriate spokesperson for each stakeholder.
            (1) Employees and their families
            (2) Customers
            (3) Vendors and suppliers

        (4) Board of Directors
        (5) Investors
        (6) Media
        (7) Community leaders
        (8) Outsourced operations
        (9) Local responding authorities
        (10) Regulators
        (11) Labor organizations
        (12) Competitors
        (13) Industry bloggers

c) Determine how stakeholders will be quickly and effectively notified of an incident.

d) Provide guidance within the plan to determine frequency of communications needed to each stakeholder before an event, during the event itself and following an event.

e) Identify most effective methods for communicating with identified stakeholders before, during and after an event.

    i) Notification systems
    ii) Email and group distribution lists
    iii) Conference call
    iv) Intranet
    v) Press conference
    vi) Event information line
    vii) Media sources
        (1) Print
        (2) Radio
        (3) TV
        (4) Internet
        (5) Social media sites
            (a) Facebook
            (b) Twitter
            (c) Linked-in
            (d) Blogs

f) Establish guidelines for quickly identifying the context of an event, its potential impacts and its stakeholders.

g) Establish guidelines for initial communication to be taken following an event and the intended (an potential unintended) consequences.

h) Identify and assign members to the crisis communication teams identified in the plan.

i) Develop guidelines for communications with the entity’s emergency response operations.

j) Prepare pre-scripted messages based on possible events

k) Document the plan.

2) Communicate and train stakeholders on roles and responsibilities defined in the crisis communications plan.
   - a) Distribute the crisis communication plan to everyone who has a role within the plan.
   - b) Provide training to those who have a role within the plan.
     - i) Provide media training to anyone who is expected to communicate with the media.
   - c) Communicate to internal stakeholders on plan.
     - i) Available communication methods and how they will be used for notification.
     - ii) How to respond to notifications.
     - iii) How to respond to requests for information from external sources.
     - iv) Where to get information.
3) Exercise the Crisis Communications Plan.
   - a) Establish crisis communication plan exercise schedule consistent with the guidelines in Professional Practice 8.
     - i) Consider conducting an exercise during other BCM exercises.
   - b) Determine methods of testing the crisis communication plan.
   - c) Develop scenario, scope and objectives for each exercise.
   - d) Conduct a lessons learned session after the exercise and document the action items.
4) Update the crisis communication plan based results of exercises and in accordance with the plan maintenance schedule established in Professional Practice 8.

DRII Professional Practices

Professional Practice Ten - Coordinating with External Agencies

This professional practice defines the need to establish policies and procedures to coordinate response, continuity and recovery activities with external agencies at the local, regional and national levels while ensuring compliance with applicable statutes and regulations.

The Professional's Role in Professional Practice Ten is as follows:

1. Identify and establish emergency preparedness and response procedures in accordance with Professional Practice Five.
2. Identify applicable emergency preparedness and response regulations and the agencies having jurisdiction over the organization's facilities and operations.
3. Coordinate emergency preparedness and response procedures with external agencies.

The Business Continuity Professional would demonstrate knowledge of this professional practice area by performing the following:

1. Identify and establish emergency preparedness and response procedures in accordance with Professional Practice 5.
2. Identify applicable emergency preparedness and response regulations and the agencies having jurisdiction over the organization's facilities and operations.
    a. Identify applicable emergency preparedness and response regulations in accordance with Professional Practice 5.
    b. Identify regulatory agencies having jurisdiction over the organization's facilities and operations. Agencies may include building officials, fire marshals, law enforcement, environmental compliance, code enforcement, emergency management, homeland security, industry regulators or others.
    c. Identify the authority of regulatory agencies to order regional, site, or building evacuation, and obtain, if available, credentials for priority access to facilities following an incident.
    d. Identify requirements for submittal of information about the facility (i.e., "pre-incident plans") including a description of its occupancy, hazards, building construction, utility systems, protection systems, and emergency preparedness and response procedures.
    e. Identify requirements for periodic facility inspections; observation of tests of building systems and or equipment; conducting evacuation or shelter drills; and the required scope and frequency of training and exercises.
    f. Identify requirements, thresholds (i.e., quantity or duration), and timeframes for mandatory reporting of incidents including impairments to protection systems, fires, injuries, fatalities, hazardous materials spills or releases, and other conditions or incidents.
    g. Develop or update emergency preparedness and response procedures to comply with laws, regulations, ordinances, and the requirements of regulatory agencies.

h. Disseminate information to appropriate management and team members.

3. Coordinate emergency preparedness and response procedures with external agencies.
   a. Identify first responders to the organization's facilities. First responders may be called for fires, hazardous materials spills or releases, rescue, emergency medical services, law enforcement issues, utility outages, or situations affecting facility access or transportation services (e.g., roads, bridges, tunnels, or private rail sidings). Responders may be public, contracted, volunteer, or provided as part of mutual aid or partnership agreements.
   b. Assess the availability (i.e., response time) and capabilities of first responders in accordance with Professional Practice Five. "Needs Assessment."
   c. Develop and document emergency alerting procedures (e.g., automatic via fire alarm, telephone, etc.) and notification protocols or requirements (mandatory reporting of spills, injuries, etc.).
   d. Identify representatives from first responder agencies and establish an open dialogue.
   e. Invite first responders to tour the organization's facilities to develop a "pre-incident plan".
   f. Identify and document emergency preparedness and response roles and responsibilities for the types of emergencies, scenarios, and impacts identified in Professional Practice 5.
   g. Develop procedures for establishing an incident command post where responding agencies can meet the organization's incident commander to unify command under the incident management system used. Document the role and responsibilities of the organization's staff working within the incident management system used. (See Professional Practice 5).
   h. Coordinate, conduct, and or participate in training, drills, and exercises with first responders to comply with regulations, as needed to establish required capabilities, and or as requested by first responders.
   i. Conduct a debrief meeting immediately following training, drills and exercises and document actions to be taken to improve emergency preparedness and response capabilities.
   j. Document the exercise and improvement plan and provide copies to management and team members.
   k. Update emergency preparedness and response plans using the improvement plan and lessons learned from training, drills, and exercises

Coordination of Plans with Public Agencies

Agency		Plan to be Reviewed
Fire Dept.	Local or county	Evacuation, fire, hazmat, rescue, bomb threat, suspicious package, special events
Local Emergency Planning Committee	Local or regional	Hazard materials response plan
Law Enforcement	Local, county, or state	Bomb threat, suspicious package, labor strife, civil disturbance, special events
Emergency Medical Services	Ambulance, paramedics, fire dept., private service	Medical emergencies, hazmat
Emergency Management	Local or county	Hurricane, tornado, earthquake, flood, regional disasters