Train.
Prepare.
Recover.

The Professional Practices for Business Continuity Management

About the Professional Practices

Mar 2017

Maintained by DRI International

For questions about this document, contact driinfo@**drii.org**. For more information, visit **www.drii.org**.

About the Professional Practices

Created and maintained by Disaster Recovery Institute International, *The Professional Practices for Business Continuity Management* is a body of knowledge designed to assist in the development, implementation, and maintenance of business continuity programs. It also is intended to serve as a tool for conducting assessments of existing programs.

Use of the Professional Practice framework to develop, implement, maintain a business continuity program can reduce the likelihood of significant gaps in a program and increase cohesiveness. Using the Professional Practices to assess a program can identify gaps or deficiencies so they may be corrected.

Business continuity management (BCM), as defined in this document, is a management process that identifies risk, threats, and vulnerabilities that could impact continued operations. Business continuity provides a framework for building organizational resilience and the capability for an effective response.

All other terms are defined in *The International Glossary for Resiliency* published and maintained by DRI International.

DRI makes both *The Professional Practices for Business Continuity Management* and *The International Glossary for Resiliency* available as free downloads via drii.org. *The Professional Practices for Business Continuity Management* is available in multiple languages.

Professional Practices 2017

As part of DRI International's ongoing efforts to maintain the relevance and utility of the Professional Practices, an extensive revision of substance, form, and function was undertaken starting in mid-2015 and finishing in the beginning of 2017. The goals were to provide information that would include:

- Advances in technology
- Cyber threat considerations
- Utilizing insurance as a risk transfer tool
- Strategies for manufacturing
- Supply chain processing
- Risk management concepts
- Legal and regulatory concerns

In addition, the titles of two of the Professional Practices were modified to be consistent with industry and profession standards, specifically:

- Professional Practice 2 was changed from "Risk Evaluation and Control" to "Risk Assessment"
- Professional Practice 5 was changed from "Emergency Response and Operations" to "Incident Response"

These new titles bring the Professional Practices in line with the terminology generally used by the majority of professionals and regulatory bodies.

As an adjunct to creating more generally accepted terminology, revisions in the abstracts and details of the Professional Practices were made to align them with *The International Glossary for Resiliency* published and maintained by DRI International. Linguistic analysis was used to reduce the number of English colloquialisms and idiosyncratic language. This facilitated the translation of the Professional Practices into the numerous languages to which they have been translated.

Finally, the numbering and pagination have been changed to allow for simpler referencing and ease of use.

Executive Summary

The Professional Practices for Business Continuity Management Objectives

1. **Program Initiation and Management**
   - Establish the need for a business continuity program.
   - Obtain support and funding for the business continuity program.
   - Build the organizational framework to support the business continuity program.
   - Introduce key concepts, such as program management, risk awareness, identification of critical functions/processes, recovery strategies, training and awareness, and exercising/testing.
2. **Risk Assessment**
   - Identify risks that can adversely affect an entity's resources or image.
   - Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective use of resources to reduce these potential impacts.
3. **Business Impact Analysis**
   - Identify and prioritize the entity's functions and processes in order to ascertain which ones will have the greatest impact should they not be available.
   - Assess the resources required to support the business impact analysis process.
   - Analyze the findings to ascertain any gaps between the entity's requirements and its ability to deliver those requirements.
4. **Business Continuity Strategies**
   - Select cost-effective strategies to reduce deficiencies as identified during the risk assessment and business impact analysis processes.
5. **Incident Response**
   - Develop and assist with the implementation of an incident management system that defines organizational roles, lines of authority and succession of authority.
   - Define requirements to develop and implement the entity's incident response plan.
   - Ensure that incident response is coordinated with outside organizations in a timely and effective manner when appropriate.
6. **Plan Development and Implementation**
   - Document plans to be used during an incident that will enable the entity to continue to function.
7. **Awareness and Training Programs**
   - Establish and maintain training and awareness programs that result in personnel being able to respond to incidents in a calm and efficient manner.
8. **Business Continuity Plan Exercise, Assessment, and Maintenance**
   - Establish an exercise, assessment and maintenance program to maintain a state of readiness.
9. **Crisis Communications**
   - Provide a framework for developing a crisis communications plan.
   - Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties.
10. **Coordination with External Agencies**
    - Establish policies and procedures to coordinate incident response activities with public entities.

Professional Practice One: Program Initiation and Management

Objectives

- Establish the need for a business continuity program.
- Obtain support and funding for the business continuity program.
- Build the organizational framework to support the business continuity program.
- Introduce key concepts, such as program management, risk awareness, identification of critical functions/processes, recovery strategies, training and awareness, and exercising/testing.

Professional's Role

1. Establish the need for a business continuity program.
2. Obtain support and funding for the business continuity program.
3. Coordinate and manage the implementation of the business continuity program throughout the entity.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Establish the need for a business continuity program.
   - 1.1. Research and reference relevant business, legal, regulatory, statutory, and contractual requirements and restrictions both from an internal and external perspective, providing recommendations on compliance and conformity for the entity.
   - 1.2. Reference relevant standards developed by national or international standards development bodies and/or trade or industry associations.
   - 1.3. Identify and resolve any conflicts between the entity's policies and relevant external requirements.
   - 1.4. Review existing audit reports to ensure the proposed business continuity program adequately addresses any gaps or opportunities.
   - 1.5. State the benefits of business continuity within the context of the entity's mission, objectives, and operations.
   - 1.6. Explain the role of leadership, including their accountability and liability related to business continuity.
   - 1.7. Develop formal reports and presentations focused on increasing awareness about the potential impact of risks to the entity.
2. Obtain support and funding for the business continuity program.
   - 2.1. Develop a mission statement and/or charter for the business continuity program within the context of the entity's mission.
   - 2.2. Develop objectives, assumptions, and scope for the business continuity program within the context of the entity's mission, objectives, and operations.
   - 2.3. Develop budget requirements for the business continuity program.

2.4. Define the business continuity program structure. Identify potential policy needs and critical success factors.
2.5. Present the proposed business continuity program structure to obtain leadership support and approval for the business continuity program.
2.6. Identify leadership sponsors for business continuity program development.
2.7. Obtain leadership approval for budget requirements.
2.8. Establish a committee or other oversight body such as a steering committee[1] to lead the business continuity program.
2.9. Define the scope, responsibilities, and overall accountability of each member of the steering committee and its support functions.

3. Coordinate and manage the implementation of the business continuity program throughout the entity.
3.1. Lead the steering committee in driving the implementation of objectives, program structure, and critical success factors. Address alignment with existing organizational policies and maintain consistent processes.
3.2. Develop or utilize existing policies, standards, and procedures for the business continuity program within the context of the entity's mission, objectives, and operations.
3.3. State the purpose of and obtain resources needed for the business continuity program.
3.4. Identify teams to support business continuity program implementation including those teams that will participate in the execution of the following activities[2]:
3.4.1. risk assessment and strategies,
3.4.2. business impact analysis,
3.4.3. recovery strategy selection and implementation,
3.4.4. overall incident management,
3.4.5. incident response and recovery,
3.4.6. crisis management and communication,
3.4.7. post-incident gap analysis and implementation of lessons learned,
3.4.8. business continuity plan documentation,
3.4.9. plan testing, exercise, maintenance, and audit activities, and
3.4.10. response, recovery, and restoration activities during an event.
3.5. Monitor the status of the ongoing budget impact of the business continuity program per the entity's existing budget management process.
3.6. Develop project plans for core components, such as the risk assessment and business impact analysis processes. Outline any tasks required to support the approved critical success factors, which may include, but are not limited to:
3.6.1. an implementation schedule,
3.6.2. time estimates,
3.6.3. program milestones, and
3.6.4. personnel requirements.
3.7. Oversee the ongoing effectiveness of the business continuity program.
3.7.1. Develop, monitor, track, and report on on-going management and documentation requirements for the business continuity program.
3.7.2. Monitor, track, and report compliance to relevant industry standards as defined in Section 1.2 above.

[1] While not universally applicable, steering committee is used throughout this document in lieu of committee for the purpose of clarity.
[2] These activities are defined and detailed in the Professional Practices Two through Ten.

3.7.3. Develop and execute internal and external benchmarking strategies.

3.8. Report to leadership on the status of the business continuity program on a regular basis.

3.8.1. Develop a schedule to report on the progress of the business continuity program to leadership.

3.8.2. Prepare regular status reports for leadership that contain concise, pertinent, accurate, and timely information on key elements of the business continuity program.

3.8.3. Provide updates on the state of the business continuity program and make recommendations for program enhancements on an on-going basis.

3.8.4. Monitor relevant industry standards as defined in Section 1.2 above to ensure that the business continuity program is delivering value consistent with current best practice.

Professional Practice Two: Risk Assessment

Objectives

- Identify risks[3] that can adversely affect an entity's resources or image.
- Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective use of resources to reduce these potential impacts.

Professional's Role

1. Work with leadership and any internal and/or external risk management or enterprise risk management groups to gain agreement on a standardized risk assessment methodology.
2. Identify, develop, and implement information-gathering activities across the entity to identify risks and threats.
3. Determine the probability and impact of the identified risks.
4. Identify and evaluate the effectiveness of controls and safeguards that are currently in place.
5. Identify resilience strategies to reduce the entity's risks and/or control or mitigate the potential impact of the risk.
6. Document and present the risk and vulnerability assessment and recommendations to leadership for approval.
7. Upon receiving approval from leadership, develop the entity's risk appetite and threshold to use as a basis for the ongoing management of a sustainable risk assessment process.

Activities

The professional would demonstrate knowledge by performing the following activities:

1. Work with leadership and any internal and/or external risk management or enterprise risk management groups (hereafter referred to as risk management groups) within the entity to gain agreement on a clear, standardized risk assessment methodology and to gain understanding of the entity's risk appetite and threshold.
   1.1. Identify risk analysis methodologies and tools, which may include, but are not limited to, quantitative methodologies (such as the use of mathematical formulas) and qualitative methodologies (such as the assessment of advantages and disadvantages). Review and incorporate the reliability and confidence factors of the data and content that is being used.
   1.2. Select the methodology and tools for entity-wide implementation that are appropriate to the entity's risk appetite and threshold.
   1.3. Establish measurement criteria necessary to quantify the probability and impact of identified risks and the effectiveness of any existing controls.
2. Identify, develop, and implement information-gathering activities across the entity to identify risks.

[3] 'Risk' is often used interchangeably with 'threat'. DRI has elected to use 'risk' for the purposes of this document.

2.1. Identify methodology to be used in the information-gathering process.
2.2. Collaborate with the entity's relevant groups including, but not limited, to risk management, legal counsel, physical security, and information security to identify known risks.
2.3. Determine and evaluate the credibility of any information sources that will be used to collect data on risks.
2.4. Develop a strategy to gather information consistent with the entity's policies.
2.5. Create entity-wide methods of information collection and distribution, including, but not limited to, forms, questionnaires, interviews, meetings, and/or combinations of these processes.
2.6. Identify the entity's risks.
2.6.1. Achieve a holistic view of entity-wide risk by identifying risks, accounting for the frequency, probability, speed of development, severity, and reputational impact.
2.6.2. Identify risk exposures from both internal and external sources, which may include, but are not limited to, natural phenomena, technological exposures, and human acts; industry or business model exposures; accidental and intentional acts; controllable exposures or risks as well as those which are beyond the entity's control; and events with and without prior warnings.

3. Determine the probability and impact of the identified risks.
3.1. Develop a method to evaluate any exposures and risks in terms of the risk frequency, probability, speed of development, severity, impact, and whether there are pre-incident warnings as in the case of hurricanes.
3.2. Identify the impacts of identified risks by category, which may include, but are not limited to, supply chain, cybersecurity, information technology including operational infrastructure, insurance, manufacturing, facility, physical security, reputational, legal, customer, and procedural.
3.3. Evaluate identified risks and classify them according to relevant criteria including, but not limited to, those risks that are under the entity's control and those risks that are beyond the entity's control.
3.4. Evaluate the impact of risks on those factors that are essential in order to conduct the entity's operations, including, but not limited to, the availability of personnel, information technology, and communications technology as well as the status of infrastructure, such as transportation.

4. Identify and evaluate the effectiveness of controls and safeguards that are currently in place.
4.1. Identify and evaluate the effectiveness of the protection afforded assets.
4.2. Identify and evaluate the effectiveness of any controls and safeguards that are currently in place for internal and external groups upon which the entity is dependent in order to conduct its operations.
4.3. Identify and evaluate the effectiveness of actions taken to reduce the probability of the occurrence of incidents that could impair the ability to conduct business, which may include, but are not limited to, facility location, safety policies and procedures, training on the proper use of equipment and tools, and preventive maintenance.
4.4. Identify and evaluate the effectiveness of existing controls to mitigate impact exposures such as preventative controls[4], which may include, but are not limited to, physical security practices (e.g. access control, cameras, and security staff); information security practices (e.g. firewalls, intrusion detection, and passwords); employment practices (e.g. background investigations and hiring practices); and privacy practices (e.g. a clean desk policy and proprietary waste disposal).

[4] Preventative controls are defined as proactive controls that help to prevent a loss.

4.5. Identify and evaluate the effectiveness of controls employed to reduce the impact of exposures, which may include, but are not limited to, sprinkler systems, fire brigades, generators, and uninterruptible power supply (UPS) systems.
4.6. Evaluate the distribution of security-related communications with internal areas of the entity as well as with external service providers.

5. Identify resilience strategies to control or mitigate the potential impact of the risk and/or reduce vulnerabilities.
   5.1. Identify trigger points for service and support areas to identify, escalate, and execute strategies selected to address risks.
   5.2. Recommend any changes needed to reduce the impact of identified risks, which may include, but are not limited to:
      5.2.1. Changes to physical protection:
         5.2.1.1. Identify requirements necessary to restrict access at all pertinent levels including, but not limited to, the building or any specific rooms.
         5.2.1.2. Investigate the need for barriers and strengthened structures to determine willful, accidental, and/or unauthorized entry.
         5.2.1.3. Address vulnerabilities of the location that may result from physical construction, geographic location, corporate neighbors, facilities infrastructure, and community infrastructure.
         5.2.1.4. Identify the need for the use of specialist personnel to conduct checks at points of entry.
         5.2.1.5. Evaluate the need for surveillance equipment at control access points.
         5.2.1.6. Changes to security and access controls, tenant insurance, and leasehold agreements.
      5.2.2. Identify changes to cybersecurity and information technology:
         5.2.2.1. Assess the need for system-provided protection of data that is being stored, in process, or in translation as well as information backup and protection.
         5.2.2.2. Evaluate information security including hardware, software, data, and network monitoring such as detection and notification.
         5.2.2.3. Evaluate the physical location of cybersecurity and information technology assets.
      5.2.3. Changes to personnel procedures.
      5.2.4. Changes including duplication and built-in redundancies to utilities.
   5.3. Interface with external resources, which may include, but are not limited to, vendors, suppliers, and outsourcers.

6. Document and present the risk and vulnerability assessment and recommendations to leadership for approval.
   6.1. Prepare a risk assessment report standardizing the analysis across the entity.
   6.2. Present the findings of the risk assessment, which may include, but is not limited to, the following components:
   6.3. Information on risks and exposures based on the risk and vulnerability analysis.
   6.4. An assessment of any existing controls and/or strategies to manage known risks. Assessment should include a rating of the control and/or strategy effectiveness as fully effective, partially effective, or ineffective.
   6.5. Recommendations for new controls to be implemented including a cost/benefit analysis.
   6.6. Prioritized recommendations for the implementation of any new controls.
   6.7. Recommendations for appropriate areas to transfer risk.

7. Upon receiving approval from leadership, develop the entity's risk appetite and threshold to use as a basis for the ongoing management of a sustainable risk assessment process.

Professional Practice Three: Business Impact Analysis

Objectives

— Identify and prioritize the entity's functions and processes in order to ascertain which ones will have the greatest impact should they not be available.
— Assess the resources required to support the business impact analysis process.
— Analyze the findings to ascertain any gaps between the entity's requirements and its ability to deliver those requirements.

Professional's Role[5]

1. Identify the qualitative and quantitative criteria to be used to assess the impact to the entity as the result of an event.
2. Gain leadership agreement on business impact analysis methodology and the criteria to be used to establish the business impact analysis process and methodology.
3. Plan and coordinate data gathering and analysis.
4. Establish the criteria and methodology to be used in conducting the business impact analysis process.
5. Analyze the collected data against the approved criteria to establish a recovery time objective (RTO) and recovery point objective (RPO) for each operational area and the technology that supports those areas.
6. Prepare and present the business impact analysis results to leadership. Gain acceptance of the recovery time objectives and recovery point objectives as detailed in the business impact analysis.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Identify the qualitative and quantitative criteria to be used to assess the impact to the entity as the result of an event.
   1.1. Define and obtain approval for criteria to be used to assess the impact on the entity's operations, which may include, but is not limited, to the following activities:
      — Assess the impact on customers, including, but not limited to, how quickly customers will learn that a problem exists; the likelihood that they will take their business elsewhere; how concerned they will be based on existing agreements and impacts to committed service levels; the impact to the customer's supply chain; and whether there were any injuries or deaths as a result of the event.
      — Assess the financial impacts, including, but not limited to, the loss of revenue, loss of profits, impact to cash flow, impact to market share, impact to the share price of stock if applicable,

[5] Note: While the business continuity professional may be given the responsibility to manage a business impact analysis, the ownership of that business impact analysis resides with the entity and its leadership or the owners of the process or processes under consideration.

contractual fines or penalties, losses resulting from required payments for fixed costs, and increased overtime costs.

- Assess the regulatory impact, including, but not limited to, fines, penalties, requirements to recall products, and the revocation of any license or permit.
- Assess the operational impact, including, but not limited to, discontinued or reduced service levels, workflow disruptions, and supply chain disruptions.
- Assess the reputational impact, including, but not limited to, negative media attention, negative social media commentary, negative community perception, and impact to shareholder confidence.
- Assess the human impact, including, but not limited to, the loss of life, injury, impact to the community as well as both short and long-term emotional impact.

2. Gain leadership agreement on business impact analysis methodology and the criteria to be used to establish the business impact analysis process and methodology.
   - 2.1. Identify and obtain leadership support and/or identify the responsible party for the business impact analysis activity.
   - 2.2. Define objectives and scope for the business impact analysis process.
   - 2.3. Choose an appropriate business impact analysis planning methodology or tool.
   - 2.4. Choose an appropriate business impact analysis data collection methodology.
     - 2.4.1. Data to be collected should include operational processes and incremental resource requirements based on recovery duration.
     - 2.4.2. Data to be collected should include the impact from the loss of any technology needed to perform the process.
     - 2.4.3. Data to be collected should include internal and external dependencies.
     - 2.4.4. Identify additional requirements that are specific to the needs of the entity.
3. Plan and coordinate data gathering and analysis.[6]
   - 3.1. Data collection may be conducted using questionnaires.
     - 3.1.1. Develop questionnaires with instructions as required.
     - 3.1.2. Manage project kick-off meetings to distribute and explain the questionnaires.
     - 3.1.3. Support respondents as they complete the questionnaires.
     - 3.1.4. Conduct follow-up interviews when clarification and/or additional data are required.
   - 3.2. Data collection may be conducted using interviews.
     - 3.2.1. Maintain consistency by using a predefined structure for each interview, following a common format and using the same questions.
     - 3.2.2. Schedule follow-up interviews as necessary if the initial analysis indicates a need to clarify or add to the collected data.
   - 3.3. Data collection may be conducted using workshops.
     - 3.3.1. Define a clear agenda and set of objectives.
     - 3.3.2. Identify the appropriate level of workshop participants and obtain agreement from leadership and/or identify the responsible party.
     - 3.3.3. Choose appropriate venue by evaluating location, facilities, and participant availability.
     - 3.3.4. Facilitate and lead the workshop or identify an appropriate resource to do so.
     - 3.3.5. Ensure workshop objectives are met.
     - 3.3.6. Ensure outstanding issues at the end of the workshop are identified and the appropriate follow up is conducted.

[6] The collection methods listed in Section Three from 3.1 to 3.4 and are listed in no particular order. The needs of specific entities may vary.

3.4. Identify the major areas of the entity, including potential third-party service providers, with the support of the responsible party for the business impact analysis.
3.4.1. Collect and review existing organizational charts.
3.4.2. Identify specific individuals to represent each area of the entity.
3.4.3. Identify third-party provider representatives to participate in the data collection process.
3.4.4. Inform the selected individuals about the business impact analysis process and its purpose.
3.4.5. Identify training requirements and establish a training schedule.
3.4.6. Execute the training for the identified functional management representatives and appropriate third-party provider representatives.
3.5. Using the selected methodology, conduct the data collection necessary to support the business impact analysis process.

4. Establish the criteria and methodology to be used in conducting the business impact analysis process.
4.1. Identify and obtain agreement on the quantitative evaluation methods for potential financial and non-financial impacts in each impact area.
4.2. Identify and obtain agreement on the requirements for the qualitative evaluation methods in each impact area.
4.3. Create a schedule for the business impact analysis process.

5. Analyze the collected data against the approved criteria to establish a recovery time objective (RTO) and recovery point objective (RPO) for each operational area and the technology that supports the operational area.
5.1. Analyze the collected data to determine the prioritization of processes and services.
5.2. Document any interdependencies that exist between each business process and the supporting infrastructure, including, but not limited to, data systems and related technology, supply chain management, third-party providers, and other resources. These interdependencies may be intradepartmental, interdepartmental, or involve external relationships.
5.3. Determine the order of recovery for business functions and technology using the collected data.

6. Prepare and present the business impact analysis results to leadership. Gain acceptance of the recovery time objective and recovery point objectives as detailed in the business impact analysis.
6.1. Prepare draft business impact analysis report using initial impact findings and highlighting identified gaps in a gap analysis.
6.1.1. Provide a statement of the entity's mission, objectives, and operations.
6.1.2. Summarize the impact to the entity's mission, objectives, and operations that may result from an event.
6.1.3. Provide a prioritized list of the entity's processes and services including the recovery time objectives and recovery point objectives, a summary of resource requirements needed over time to recover and resume operations, and a gap analysis between the current capabilities and the needed capabilities to meet the defined recovery time objectives and recovery point objectives.
6.1.4. Issue the draft report to the participating functional management representatives and third-party provider representatives to obtain their feedback.
6.1.5. Review the feedback obtained from the functional management representatives and third-party provider representatives. Adjust the findings as needed.
6.1.6. Schedule workshops or meetings with the functional management representatives and third-party provider representatives to discuss the initial findings as necessary.
6.1.7. Update the findings as necessary to reflect any changes arising from the workshops or meetings.

6.2. Prepare the final business impact analysis report.
6.3. Prepare and submit a formal presentation of the findings in the final business impact analysis report to the leadership.
6.4. Gain acceptance from leadership for the recovery time objectives and recovery point objectives for each operational area as defined by the findings in the final business impact analysis report.

Professional Practice Four: Business Continuity Strategies

Objectives

— Select cost-effective strategies to reduce deficiencies as identified during the risk assessment and business impact analysis processes.

Professional's Role

1. Utilize the data collected during the risk assessment and business impact analysis processes to identify the available continuity and recovery strategies for the entity's operations that will meet the recovery time objectives and recovery point objectives as defined in the business impact analysis.
2. Utilize the data collected during the risk assessment and business impact analysis to identify the available continuity and recovery strategies for the entity's technology that will meet the recovery time objectives and recovery point objectives as defined in the business impact analysis.
3. Identify supply chain issues, for both suppliers and customers, from the business impact analysis that may affect the selection of a recovery strategy.
4. Consolidate strategies where appropriate to reduce costs and/or complexity.
5. Assess the cost of implementing identified strategies through a cost/benefit analysis.
6. Recommend strategies and obtain approval to implement.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Utilize the data collected during the risk assessment and business impact analysis processes to identify the available continuity and recovery strategies for the entity's operations that will meet both the recovery time objective and recovery point objective requirements as defined in the business impact analysis.
   1.1. Review the recovery requirements identified for each of the entity's operational areas.
   1.2. Identify alternative business continuity strategies. Potential options include, but are not limited to, the following strategies[7]:
      1.2.1. Develop manual workaround procedures.
      1.2.2. Develop reciprocal agreements.[8] Reciprocal agreements must be tested to ensure viability as a recovery option; they may not be a viable strategy for an extended period and may require an additional longer-term recovery strategy.
      1.2.3. Identify internal dual-usage space that could be equipped to support recovery, such as conference rooms, training rooms, or cafeterias. Ensure the time necessary to prepare and equip the space is consistent with the recovery time objective and recovery point objective requirements.

[7] The strategies listed in Section One from 1.2.1 to 1.2.13 are listed in no particular order. The needs of specific entities may vary.
[8] Reciprocal agreements are most commonly used in small business operations, public sector mutual aid agreements, and manufacturing environments.

1.2.4. Identify an external alternate site.
1.2.5. Contract with third-party service providers or outsourcers.
1.2.6. Transfer workload to a surviving site.
1.2.7. Transfer staff and workload to a surviving site.
1.2.8. Suspend operations that are not time-sensitive in a surviving site and transfer personnel and/or workload from the impacted site to the surviving site. This is also known as displacement.
1.2.9. Build a dedicated alternate site.
1.2.10. Direct impacted personnel to work from home.
1.2.11. Manufacturing environments have specific needs and may use the following recovery strategies:
- Repair/rebuild at the time of the event.
- Shift production to another line or site.
- Utilize existing inventory.
- Utilize excess capacity in other plants.
- Buy back product from customer(s) and redistribute it as needed.
- Provide a substitute product in lieu of the unavailable products.
- Outsource production.

1.2.12. To meet the recovery point objectives for the recovery of vital hard-copy records and work-in-process and to ensure that they are accessible after an event, the following strategies may be used: photocopies, scans, or cloud storage.
1.2.13. Review alternate site options using the following criteria as applicable: location, the availability and suitability of the space, communications capabilities including voice and data, the availability of equipment and raw materials, and the hardness and sustainability of the site including the availability of resources such as redundant power and water.

1.3. Assess the viability of alternative strategies against the results of the business impact analysis using the following criteria as applicable: the ability to meet the defined recovery time objectives and recovery point objectives, a comparison of solutions, the advantages and disadvantages, costs incurred through preparation, maintenance and execution, and the mitigation capability and control options.
1.4. Review existing insurance coverage, which may include, but is not limited to, extra expense, business interruption, contingent business interruption, payroll, and flood, so that the selected business continuity strategies will complement the coverage that will be used during the recovery process.
1.5. Develop a preliminary cost/benefit analysis for the selected strategies for the entity's operations.

2. Utilize the data collected during the risk assessment and business impact analysis to identify the available continuity and recovery strategies for the entity's technology that will meet the recovery time objectives and recovery point objectives as defined in the business impact analysis.
2.1. Review the recovery requirements identified for the entity's technology in each operational area.
2.2. Identify alternative technology recovery strategies. Potential options include, but are not limited to, the following strategies[9]:
2.2.1. Develop manual workaround procedures for each operational area together with functional management representatives.

[9] The strategies listed in Section One from 2.2.1 to 2.2.9 are listed in no particular order. The needs of specific entities may vary.

2.2.2. Implement an active/active technology environment through a dual data center, thereby eliminating the need for recovery.
2.2.3. Implement active/passive technology environment for high availability of time-sensitive technology, thereby providing for a quick restart of the required technology.
2.2.4. Contract with third-party service providers or outsourcers to provide technology recovery environment, which may include a traditional hot site contract with a vendor in which the vendor provides the equipment to recover from their inventory or a contract by which the entity puts its own equipment for recovery on the floor of the vendor's facility.
2.2.5. Outsource the entire technology environment through a strategy such as cloud computing.
2.2.6. Identify a site where recovery would occur but build-out only heating, ventilating, and air conditioning (HVAC) and electrical capabilities; populate with technology at time of disaster (warm site).
2.2.7. Identify a site where recovery would occur but build-out only at time of disaster (cold site).
2.2.8. Identify strategies for recovery of data in electronic form that meets the recovery point objectives established for these records and ensures they are available following a disaster. Ensure time to restore the data is within the identified recovery time objective and recovery point objective guidelines set in the business impact analysis.
2.2.9. Review alternate site options using the following criteria as applicable: location, the availability and suitability of the space, communications capabilities (including voice and data), the availability of equipment and raw materials, and the hardness and sustainability of the site (including the availability of resources such as redundant power and water).

2.3. Assess the viability of alternative strategies against the results of the business impact analysis using the following criteria as applicable: the ability to meet the defined recovery time objectives and recovery point objectives, a comparison of solutions, the advantages and disadvantages, costs incurred through preparation, maintenance, and execution, and the mitigation capability and control options.
2.4. Develop a preliminary cost/benefit analysis for the selected strategies for the entity's technology.

3. Identify supply chain issues, for both suppliers and customers, from the business impact analysis that may affect the selection of a recovery strategy.
   3.1. Identify any delivery issues that may arise from the relocation to another site.
   3.2. Ensure that the effect on the entity's operation and processes is minimal in the case of a supplier event.
   3.3. Identify any issues that may occur with the delivery of product to a customer in the event of an interruption to its operation.
4. Consolidate strategies where appropriate to reduce costs and/or complexity. Identify areas in which the same recovery strategy could be used to meet the requirements for multiple areas of operations, such as using a single alternate site for the recovery of business operations from different sites that are not expected to be impacted by the same event.
5. Assess the cost of implementing identified strategies through a cost/benefit analysis.
   5.1. Estimate the cost of implementing and maintaining recovery for the identified recovery strategies.
   5.2. Validate that the recovery strategy being implemented is commensurate with the impacted operational area.
      5.2.1. Consider financial, regulatory, and additional factors that could affect recovery.
      5.2.2. Ensure the recovery solution is in line with recovery objectives.
      5.2.3. Ensure the cost of recovery is in line with the value of what is to be recovered.
6. Recommend strategies and obtain approval to implement.

Professional Practice Five: Incident Response

Objectives

— Develop and assist with the implementation of an incident management system that defines organizational roles, lines of authority and succession of authority.
— Define requirements to develop and implement the entity's incident response plan.
— Ensure that incident response is coordinated with outside organizations in a timely and effective manner when appropriate.

Professional's Role

1. Identify applicable emergency preparedness and incident response guidelines.
2. Identify potential types of incidents that may occur and the impacts that may result.
3. Identify the necessary response capabilities.
4. Review existing incident response procedures and assess the capabilities to protect life, property, and the environment.
5. Recommend the development and implementation of an incident management system for the command, control, and coordination of personnel and resources during incident response activities. Develop and assist with the implementation of a delegation of authority that defines organizational roles, lines of authority, and succession of authority.
6. Review and coordinate incident response plans and procedures with personnel and relevant organizations as appropriate.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Identify applicable emergency preparedness and incident response guidelines including, but not limited to, health and safety, fire prevention, and those required by regulations issued by the federal, state, provincial, county, parish, tribal, or local levels of government.
2. Identify potential types of incidents that may occur and the impacts that may result.
   2.1. For each type of incident, identify potential scenarios that may result and make note of the following information:
      2.1.1. The origin or location and whether the event was internal or external.
      2.1.2. The scope or magnitude.
      2.1.3. The area of impact.
   2.2. For each type of incident, identify potential impacts including, but not limited to, casualties, property damage, and environmental contamination.

3. Identify the necessary incident response capabilities.
   3.1. Capabilities needed to protect life safety may include, but are not limited to, evacuation, shelter-in-place to be used in case of an event such as an exterior airborne hazard, lockdown, and accounting for all persons affiliated with the organization and visitors affected by the incident.
   3.2. Capabilities needed to protect property including:
      3.2.1. Supervision and operation of building systems and equipment including utilities, ventilation and air conditioning, fire detection and suppression, and communications and warning.
      3.2.2. Property conservation to prepare a facility for a forecasted event, such as the orderly shutdown in advance of a hurricane, and to minimize damage with salvage and cleanup following an event.
      3.2.3. Firefighting, including activities such as the coordinated planning with public fire department and fire extinguisher training.
   3.3. Capabilities needed to prevent environmental contamination such as supervision and the operation of systems designed to contain hazardous materials on-site.
4. Review existing incident response procedures and assess the capabilities to protect life, property and the environment.
   4.1. Perform an information-gathering process.
      4.1.1. Identify the response capabilities required to protect life, property, and the environment for the identified types of incidents.
      4.1.2. Identify and establish relationships with internal departments and external agencies that have responsibilities for emergency preparedness and incident response.
      4.1.3. Gather incident response procedures from internal departments and those individuals with assigned responsibility for incident response including, but not limited to, environmental, health, safety, security, and management.
      4.1.4. Gather incident response procedures and a description of response capabilities from external sources with known response capabilities or obligations.
      4.1.5. Contact public agencies, including, but not limited to, medical services, fire department, law enforcement, and hazardous materials teams, to identify requirements, practices, and resources, and to establish liaison relationships.
   4.2. Conduct a resource needs assessment.
      4.2.1. Identify the resources needed to protect life, property, and the environment from the types of incidents identified.
      4.2.2. Identify the internal and external personnel, including those from public agencies, who are trained to respond to the identified incidents.
      4.2.3. Identify the systems and equipment, including, but not limited to, detection, alarm, communications, suppression, and containment systems available for incident response.
   4.3. Verify that mutual aid or partnership agreements are documented and current if applicable.
   4.4. Review incident response plans to determine whether the following procedures are addressed: hazard or threat monitoring and incident detection; prompt reporting to the responsible person, department, and/or agency; alert first responders and warn impacted or potentially impacted persons; and perform escalation as events unfold.
   4.5. Identify discrepancies and/or gaps between identified requirements and capabilities.

5. Recommend the development, and assist with the implementation, of an incident management system for command, control, and coordination of personnel and resources during incident response activities. Develop and assist with the implementation of a delegation of authority that defines organizational roles, lines of authority, and succession of authority.
   5.1. Document procedures for evaluation and escalation including the engagement of additional internal and external services and the process for obtaining additional resources as needed.
   5.2. Incident reporting should include initial and periodic situation analysis updates.
   5.3. A physical or virtual emergency operations center (EOC) should be established to facilitate coordination of response, continuity, and recovery activities.
   5.4. The EOC should be sized to house the anticipated number of persons and equipped to support occupancy for the duration of the types of incidents identified.
   5.5. The EOC should be equipped with full communications capabilities, such as two-way radio, email, text messaging, pagers, landline, and wireless voice and data communications necessary to support incident management.
   5.6. Communications during an incident should be documented to the extent possible and practical.
   5.7. Operating procedures should include the management and operations of the EOC including communications and information flow as well as the closure of the EOC when appropriate.
6. Review and coordinate incident response plans and procedures with personnel and relevant organizations as appropriate.
   6.1. Identify the documents, such as those used for fire prevention and hazardous materials management plans, that must be submitted to public agencies to maintain compliance with applicable regulations.
   6.2. Assist with the coordination of response plans and procedures with public agencies and external resources.

Professional Practice Six: Plan Development and Implementation

Objectives

— Document plans to be used during an incident that will enable the entity to continue to function.

Professional's Role

1. Use the approved strategies developed in Professional Practice Four as the basis for plan documentation.
2. Define the structure for the plan documentation.
3. Coordinate the effort to document recovery plans for the entity's operations and the supporting infrastructure.
4. Publish the plan documents.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Use the approved strategies developed in Professional Practice Four as the basis for plan documentation.
   - 1.1. Design, develop, and implement recovery strategies for the entity's operations.
     - 1.1.1. Identify requirements that will be used in creating the business continuity plan.
     - 1.1.2. Report on the progress of the plan development and implementation to leadership and/or steering committee[10].
     - 1.1.3. Complete all required tasks for plan implementation, which may include, but are not limited to:
       - 1.1.3.1. Acquiring recovery and business continuity plan resources ensuring that internal and external resource requirements are included.
       - 1.1.3.2. Establishing response, recovery, restoration, and business continuity contracts.
       - 1.1.3.3. Establishing access controls for the development and maintenance of documentation.
2. Define the structure for the plan documentation.
   - 2.1. Determine how the plan will be organized and identify the teams needed to document the plans[11].
     - 2.1.1. Ensure alignment with the scope of the planning process.
     - 2.1.2. The types of plans to be documented may include, but are not limited to, strategic (including succession planning), operational, incident response, recovery, restoration, and return-to-normal operations.

[10] See Professional Practice One for further detail on defining the reporting structure.
[11] This refers to the teams that are created to document plans and may differ from the teams that execute plans.

2.1.3. Strategy considerations may include, but are not limited to, whether the term will be short (such as a day and or a month) or long (such as more than a month); whether the impacts will be local (site or campus-specific), regional, or enterprise-wide; and whether there is cascading impact potential.

2.2. Define the roles and responsibilities for plan development, including:
- 2.2.1. Identifying the tasks to be undertaken.
- 2.2.2. Developing a timeline for plan completion.
- 2.2.3. Reviewing, evaluating, and recommending tools, which may include, but are not limited to, planning software, databases, specialized software, and templates.
- 2.2.4. Developing templates that can be used to capture information on processes, technology matrices, and flowcharts.
- 2.2.5. Identifying other supporting documentation as needed.
- 2.2.6. Ensuring that there are built-in mechanisms to facilitate maintenance such as version control.

2.3. Define the content requirements for the plan, which may include, but are not limited to:
- 2.3.1. Policy and governance, such as business continuity policies and procedures, authority levels, which may be found in corporate governance, and a confidentiality statement.
- 2.3.2. The scope and objectives, which should align with the entity's mission, goals and objectives, and business continuity policies, and include the identification of time-sensitive operations and the resources needed to support them.
- 2.3.3. Any assumptions found in the planning process.
- 2.3.4. The structure of the personnel involved in the process; including the description, organizational structure, and the roles and responsibilities of each team.
- 2.3.5. The plan activation procedures should include incident assessment, escalation, the reporting process, declaration procedures, and recovery and restoration procedures.

3. Coordinate the effort to document recovery plans for the entity's operations and the supporting infrastructure, which may include, but are not limited to, the following types of plans:

3.1. An incident management plan, which should include the following:
- 3.1.1. Life-safety procedures.
- 3.1.2. Incident command and control procedures.
- 3.1.3. Roles and responsibilities for the personnel involved in incident management.
- 3.1.4. The location for the emergency operations center (EOC) location and procedures for its activation.
- 3.1.5. The process for conducting an assessment, which should include protecting the site from further loss; a cost/benefit analysis of repair versus replacement of entity assets (such as equipment, technology, documents, data, furnishings, premises, or the plant); the estimated time needed to repair or replace entity assets; the agreed-upon restoration methods for entity assets; the approval process for restoration and insurance considerations; and the salvage process.

3.2. A crisis management and communication plan[12], which should include the following:
- 3.2.1. A list of the individuals who will be part of the crisis management team.
- 3.2.2. An outline of the procedures to transition from incident response to crisis management and business continuity.

[12] See also Professional Practices Five and Nine.

3.2.3. Notification procedures for communication to interested parties throughout event (such as status updates, media releases, and other targeted communications designed for interested parties), which may include, but are not limited to, the media, employees and their families, regulatory bodies, emergency first-responders, agencies, special hazmat services, investors, the governing board of directors or other relevant leadership authority, labor representatives, and other involved groups (such as customers, vendors, or suppliers).

3.3. A recovery site activation plan, which should include the following:

3.3.1. Alert procedures

3.3.2. Declaration procedures

3.3.3. Recovery infrastructure provided, which may include:

3.3.3.1. Administration and logistics

3.3.3.2. New equipment or just-in-time drops

3.3.3.3. Technical services and procedures, such as communication networks (including voice, data, and wireless); data preparation; and application support.

3.3.3.4. End-user liaison

3.3.3.5. Business operations

3.3.3.6. Inter-site logistics and communications

3.3.3.7. Production recovery process and procedure

3.4. An operational or recovery plan or plans, which should include the following:

3.4.1. Recovery teams, including both primary and alternate teams.

3.4.2. The logistics involved in arranging for the travel and housing of recovery staff, transporting the data needed for recovery, and assuring the procurement of additional resources, as necessary.

3.4.3. Resource documentation, including, but not limited to, technology requirements, vital records, voice and data communications, critical external contacts and suppliers, and equipment requirements.

3.5. A business continuity plan, which should include the following:

3.5.1. Recovery teams, including primary and alternate members

3.5.2. Alternative ways to conduct business when normal resources are unavailable

3.5.3. Business continuity processes, procedures, and communication

3.5.4. Mobilizing alternate resources

3.5.5. Managing alternate resources

3.6. A technology recovery plan or plans, which should include the following:

3.6.1. Recovery teams: Primary and alternate members

3.6.2.Mobilizing resources

3.6.2.1. The logistics involved in arranging for the travel and housing of recovery staff, acquiring the data needed for recovery, and the procurement of additional resources.

3.6.2.2. The required resources

3.6.2.2.1. Storage requirements, which may include, but are not limited to, network storage devices and data storage devices.

3.6.2.2.2. Voice and data communications hardware, which may include, but are not limited to, network switches and interface equipment.

3.6.2.2.3. Hardware and software requirements, which may include, but are not limited to, processors, tape drives/tape silo/virtual tape library, application software, operating systems, source code, and security software and devices.

3.6.2.2.4. Infrastructure requirements, which may include, but are not limited to, power sources and controllers; heating, ventilating, and air conditioning (HVAC); cabling; and access security.

3.6.2.2.5. Information security requirements, which may include, but are not limited to, firewalls, authentication, virus or spyware protection, encryption, key contacts and suppliers, and equipment requirements.

3.6.3. The technology recovery plan should outline a detailed procedure for the recovery of the technology environment, including the following steps:

3.6.3.1. Identify application dependencies.

3.6.3.2. Create a process for change management.

3.6.3.3. Create a process for problem management.

3.6.3.4. A plan for testing, exercising, and maintenance (including exercise requirements); scope, objectives and schedule; and a plan maintenance program.

4. Publish the plan documents.
   4.1. Provide a final draft to the plan development teams and business process owners.
   4.2. Obtain authorized signatures.
   4.3. Publish and distribute the plans or portions of the plans to anyone with a documented role including the information necessary for the participants to execute their roles.
   4.4. Establish procedures for the distribution and control of plans (such as a distribution list), including plan changes and updates.

Professional Practice Seven: Awareness and Training Programs

Objectives

— Establish and maintain training and awareness programs that result in personnel being able to respond to incidents in a calm and efficient manner.

Professional's Role

1. Establish the objectives and components of the business continuity awareness and training program.
2. Identify the awareness and training requirements across the functions of the entity.
3. Prioritize the awareness and training requirements for the entity's internal personnel.
4. Develop the methodology for the awareness and training program for the entity.
5. Identify, develop, or acquire awareness and training tools and resources needed to meet the objectives of the program.
6. Oversee the delivery of the activities conducted to accomplish the objectives of the awareness and training program.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Establish the objectives and components of the business continuity awareness and training program.
   - 1.1. Define the program management approach.
   - 1.2. Set implementation timeframes.
   - 1.3. Obtain leadership's support for the program.
   - 1.4. Obtain commitment from the relevant personnel.
2. Identify the awareness and training requirements across the functions of the entity.
   - 2.1. Define and document the desired level of business continuity awareness across the entity.
   - 2.2. Define and document training resource requirements.
3. Prioritize the awareness and training requirements for the entity's internal personnel.
   - 3.1. When designing an awareness program, it is important to consider which internal personnel must be made aware of the relevant components of the business continuity program. Required topics of which all employees should be made aware may include, but are not limited to:
     - — Business continuity program objectives,
     - — Event notification and expectations, and
     - — Incident response procedures.
   - 3.2. When designing a training program, it is important to consider which internal personnel must be trained in the relevant components of the business continuity program.
     - 3.2.1. Required topics in which all employees should be trained, may include, but are not limited to:
       - — Evacuation drills, and
       - — Scenario-based walkthroughs.

3.2.2. Required topics in which management should be trained, may include, but are not limited to:
- Evacuation drills, and
- Scenario-based walkthroughs.

3.2.3. Required topics in which business continuity team members should be trained, may include, but are not limited to:
- Evacuation drills,
- Scenario-based walkthroughs, and
- Technology exercises.

4. Develop the methodology for the awareness and training program for the entity.
   4.1. Conduct a needs assessment for the awareness and training program, which may include, but is not limited to, the following methods:
   - Conduct a survey of needs in order to assess the current state of awareness and readiness and to determine whether the current state is in alignment with the expectations of leadership and current best practice. Survey participants could be at various levels and may include diverse interested parties such as functional management, plan participants, and the broader business population.
   - Use the collected data to identify trends and new developments.
   - Review previous test and exercise results and conduct gap analyses based on those results.

   4.2. Benchmark the current levels of awareness and readiness within the entity against desired level and initiate plan to address awareness and training opportunities.
   4.3. Design the training process.
      4.3.1. Define objectives, identify and select delivery methods, including, but not limited to, awareness campaigns, exercises, scenario-based walkthroughs, and newsletters.
      4.3.2. Define the roles and responsibilities for the awareness and training program.
5. Identify, develop, or acquire awareness and training tools and resources needed to meet the objectives of the program.
   5.1. Identify internal and external resources necessary to support the program, which may include, but are not limited to, courseware, a dedicated business continuity website, relevant government-sponsored websites, entity-sanctioned social media tools, brochures, and awareness posters.
   5.2. Identify additional internal and external awareness and training opportunities, which may include, but are not limited to, conferences, webinars, user groups and associations, white papers and other publications, certification bodies, and relevant academic education programs.
6. Oversee the delivery of the activities conducted to accomplish the objectives of the awareness and training program.
   6.1. Schedule and conduct awareness activities.
   6.2. Schedule and deliver training activities.
   6.3. Monitor the effectiveness of the awareness and training activities through follow-up surveys or other methods.
   6.4. Review the results of the awareness and training program activities. Provide a report to leadership on the outcomes of the program.

Professional Practice Eight: Business Continuity Plan Exercise, Assessment, and Maintenance

Objectives

— Establish an exercise, assessment and maintenance program to maintain a state of readiness.

Professional's Role

1. Establish an exercise/test program.
2. Establish a plan maintenance program.
3. Identify appropriate governance.
4. Establish an audit process for the business continuity program.
5. Document and communicate the results and recommendations from the exercise/test and audit process.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities.

1. Establish an exercise/test program.
   - 1.1. Develop an exercise/test program that meets the entity's business continuity program's scope and objectives.
     - 1.1.1. Ensure that the documented recovery process is thorough and that there are no deficiencies.
     - 1.1.2. Identify any gaps in the process and opportunities for improvement.
   - 1.2. Obtain the necessary support for the development of the exercise/test program.
   - 1.3. Develop an effective program for exercising/testing.
     - 1.3.1. Document the exercise/test criteria.
     - 1.3.2. Define any exercise/test program assumptions.
     - 1.3.3. In order to create a comprehensive program, identify the types of exercise/test that will be included in the exercise/test program. These may include, but are not limited to, the following: life safety; plan walkthrough; scenario-based tabletop; notification; alternate site; standalone platform, infrastructure, or application; functional process; full end-to-end test of an operation or technology; comprehensive exercise/test of all internal resources required to recover the entity; and fully-integrated exercise/test with both internal and external dependencies.
     - 1.3.4. Identify the participants and their roles and responsibilities in the exercise/test program, which may include, but are not limited to, recovery team(s), observers and reporters, time keepers, auditors and reviewers, facilitators, suppliers, and outsourced service providers.

1.4. Define the exercise/test program objectives and scope to select appropriate scenarios.
- 1.4.1. Create realistic scenarios based on the risk assessment as described in Professional Practice Two. Include activities which may invoke various facets of the recovery strategies, including, but not limited to, technical scenarios defined as the operational capabilities; procedural scenarios defined as the accuracy of the procedures; logistical scenarios defined as the ability to access the recovery facility and execute their recovery procedures; and timeline scenarios defined as the ability to achieve objectives within established timeframes.
- 1.4.2. Determine the exercise/test requirements and draft a detailed plan for the activities.
  - 1.4.2.1. Define and document objectives for the exercise/test.
  - 1.4.2.2. Define and document the scope of the exercise/test. Ensure clear parameters that differentiate in-scope and out-of-scope activities.
  - 1.4.2.3. Define the exercise notification process, which may include either announced, planned exercises or unannounced, surprise exercises.
  - 1.4.2.4. Schedule a timeframe for the exercise. Develop a specific schedule for the exercise/test to be conducted on an annual basis or as often as necessary to ensure competency and to meet regulatory requirements. Develop a multi-year incremental exercise/test schedule that incorporates lessons learned from previous exercises.
  - 1.4.2.5. Define and document both quantitative and qualitative evaluation criteria aligned with the objectives and scope of the exercise/test.
  - 1.4.2.6. Identify activities that must occur prior to the exercise, which may include, but are not limited to, the following:
    - 1.4.2.6.1. Identify the resources required to conduct the exercise/test.
    - 1.4.2.6.2. Identify the participants necessary to conduct the exercise/test.
    - 1.4.2.6.3. Distribute communications that explain the objectives of the exercise and the roles of all participants.
    - 1.4.2.6.4. Provide a list of hardware, software, physical supplies, equipment, and other items required for the exercise/test.
    - 1.4.2.6.5. Document and communicate the specifications for the environment that are necessary to conduct the exercise.
    - 1.4.2.6.6. Specify whether the exercise/test will use a production or non-production environment.
    - 1.4.2.6.7. Specify the time and date of the exercise/test.
    - 1.4.2.6.8. Provide a timetable of events and circulate to all the participants.
    - 1.4.2.6.9. Establish a “back-out” cancellation plan for the exercise/test.
- 1.4.3. Conduct the exercise/test as planned.
  - 1.4.3.1. Should an actual incident occur during an exercise/test, there must be a pre-determined mechanism for cancelling the exercise/test and invoking the actual continuity process. This may differ from the “back-out” plan in 1.4.2.6.9.
  - 1.4.3.2. Record the exercise/test events.
  - 1.4.3.3. Document the exercise/test results.
  - 1.4.3.4. Declare an end to the exercise/test.
  - 1.4.3.5. Perform the shut-down procedures at the conclusion of the exercise/test.
  - 1.4.3.6. Perform any necessary cleanup activities.

1.4.4. Identify activities that must be completed following the exercise/test.
1.4.4.1. Conduct debriefing sessions to review the results of the exercise/test. Identify lessons learned and actions for improvements.
1.4.4.2. Report on the results of the exercise/test. Provide a comprehensive summary with recommendations.
1.4.4.3. Document an action plan for the recommendations that resulted from the exercise/test.
1.4.4.4. Identify any outstanding issues identified as a result of the exercise/test or that existed prior to the exercise/test.
1.4.4.5. Identify action items including responsibilities assigned to specific participants and timeframes for resolution.
1.4.4.6. Monitor the progress to completion of the identified action items. Escalate when necessary according to the entity's communication requirements.
1.4.4.7. Document the lessons learned from the exercise/test including expected versus actual results and unexpected results.
1.4.4.8. Communicate the results of the exercise/test to the relevant organizational parties.

2. Establish the plan maintenance program.
2.1. Define the method and schedule for the plan maintenance program.
2.1.1. Define the ownership of the plan data. Identify specific personnel.
2.1.2. Prepare maintenance schedules and review procedures.
2.1.3. Select maintenance tools.
2.1.4. Monitor the maintenance activities.
2.1.5. Establish an update process for the plan.
2.1.6. Ensure that scheduled plan maintenance addresses all documented recommendations that resulted from the exercise/test.
2.1.7. Report on maintenance activities to the relevant organizational parties.
2.2. Define a change management process for the plan maintenance program.
2.2.1. Analyze any entity changes that would result in changes to the business continuity program and the planning process.
2.2.2. Develop change control procedures to monitor changes. Integrate the procedures with any existing entity-wide change control process.
2.2.3. Create proper version control. Develop procedures for the re-issue, distribution, and circulation of the plan to the relevant parties.
2.2.4. Identify plan distribution lists for circulation.
2.2.5. Develop a process to update plans based on the response to audit findings.
2.2.6. Create procedures to facilitate maintenance of the plan.
2.2.7. Implement change control process.

3. Identify appropriate governance.
3.1. Review the expectations of the relevant organizational parties. Expectations may be motivated by industry requirements, the internal needs of the entity, and service level agreements.
3.2. Identify entity-wide processes including a recurring review, enhancement, and continuous improvement process.
3.3. Identify appropriate governance models based on industry, national, or international standards.
3.4. Define the frequency and scope of exercise/test that meets the needs of the entity.
3.5. Ensure approval by the relevant organizational parties.

4. Establish an audit process for the business continuity program.
   - 4.1. Determine a schedule for conducting a self-assessment audit.
   - 4.2. Prepare to support other audits that may occur, which may include, but are not limited to, internal audit, external or third-party audit, regulatory body audit, or a second-party audit.
   - 4.3. Document any audit requirements.
   - 4.4. Select or develop any tools that may be necessary to conduct the audit.
   - 4.5. Establish the audit schedule.
   - 4.6. Conduct audit activities and monitor the process.
     The audit of the plan structures, contents, and action sections, may include, but is not limited to, program requirements, documents and standards; templates and plans; exercise/test requirements and results; the repository for the plan and exercise/test results; the plan documentation control procedures; the version control process and documentation; and the distribution lists and associated processes.
   - 4.7. Audit the change control process for the plan documentation and business continuity program.
   - 4.8. Review response to the audit findings.
   - 4.9. Confirm that the responses are submitted and that the action plans are documented. Verify that all completed actions are captured in the plan and supporting documentation.
5. Document and communicate the results and recommendations from the exercise/test, and audit process.
   - 5.1. Identify relevant organizational parties, which may include, but are not limited to, process owners, governance coordinators, oversight committees, and organizational leadership.
   - 5.2. Select the appropriate communication methods including the appropriate reporting level of detail and utilize them in a timely manner. Where appropriate, consider graphic representations or comparison reports targeted to specific audiences.
   - 5.3. Establish a feedback process and validation loop to confirm that appropriate actions have been taken as a result of the reported audit findings. This process should include issues tracking, the date of opening for the item, the owner of the issue, and the date of closing for the item.

Professional Practice Nine: Crisis Communications

Objectives

- Provide a framework for developing a crisis communications plan.
- Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties.

Professional's Role

1. Design, develop, and implement a crisis communications plan.
2. Communicate and train members of the crisis communications team on their roles and responsibilities.
3. Exercise/test the crisis communications plan.
4. Update the crisis communications plan.

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Design, develop, and implement a crisis communications plan.
   - 1.1. Review existing crisis communications plan, identifying and documenting gaps, as necessary. If no plan exists, create the plan.
   - 1.2. Leverage the results of the risk assessment as outlined in Professional Practice Two in order to identify potential events for which communications should be planned.
   - 1.3. Define the objectives, scope, and plan structure.
   - 1.4. Establish the location, roles, and responsibilities for the crisis communication team, which is responsible for the plan.
     - 1.4.1. Identify and document the primary location for the crisis communication team's operations. It may be a physical or virtual location.
     - 1.4.2. Identify the governance structure for developing internal messaging.
     - 1.4.3. Identify the internal media function who will serve as the primary contact for outgoing media communications.
   - 1.5. Identify internal and external interested parties for the crisis communications. They may include, but are not limited to, employees and their families, investors, customers, vendors and suppliers, outsourced operations, insurers, community leaders, local responding authorities, governing bodies, regulators, labor organizations, competitors, the media, industry bloggers and trade publications, and other interested or involved parties. Ensure the alignment of the crisis communications spokesperson with the audience for the message.

1.6. Develop and document the interested party notification process.
    1.6.1. Determine the frequency of communications before, during, and after the event.
    1.6.2. Identify communication methods, which may include, but are not limited to, incident notification systems, email and group distribution lists, conference calls, intranet systems, press conferences event information lines and media sources (such as print, radio, television), the Internet, social media platforms, and blogs.
1.7. Establish guidelines to identify the event and its potential impacts.
1.8. Establish guidelines for the initial communication following an event.
1.9. Identify and assign members to the crisis communications team.
1.10. Develop guidelines for communications with the incident response operations.
1.11. Document sample communications that can be used as templates during an event.

2. Communicate and train members of the crisis communications team on their roles and responsibilities.
    2.1. Distribute the crisis communication plan to those who have been assigned roles and responsibilities.
    2.2. Provide training to those who have been assigned roles and responsibilities. Training may include, but is not limited to, the determination of triggers to initiate the crisis communication process, notification and response procedures, and the proper protocol for issuing communications.
3. Exercise/test the crisis communications plan.
    3.1. Establish an exercise/test schedule for the crisis communications plan that is consistent with the guidelines outlined in Professional Practice Eight.
    3.2. Determine the methodology for exercising/testing the crisis communications plan.
    3.3. Develop the scenario, scope, and objectives for each exercise/test.
    3.4. Conduct a session to determine lessons learned after the exercise/test. Document the corrective action items.
4. Update the crisis communication plan.
    4.1. Update the plan based on the results of the exercises/tests conducted and in accordance with the plan maintenance schedule established in Professional Practice Eight.

Professional Practice Ten: Coordinating with External Agencies

Objectives

— Establish policies and procedures to coordinate incident response activities with public entities.

Professional's Role

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

Activities

The business continuity professional would demonstrate knowledge by performing the following activities:

1. Identify and establish incident response procedures for the entity in accordance with Professional Practice Five.
2. Identify applicable emergency preparedness and incident response guidelines and the agencies having jurisdiction over the entity's facilities and operations.
   - 2.1. Identify regulatory agencies with jurisdiction over the entity's facilities and operations. Agencies may include, but are not limited to, facility officials, fire marshals, law enforcement, regulators, and other governmental organizations.
   - 2.2. Identify requirements for the submission of information about the facility (such as a description of its occupancy, hazards, protection systems, and response procedures) to appropriate organizations, including those identified in section 2.1.
   - 2.3. Identify requirements for periodic facility inspections, including the frequency of exercise/test and training activities.
   - 2.4. Identify the requirements and timeframes for mandatory reporting of incidents including, but not limited to, impairments to protection systems, fires, injuries, fatalities, hazardous material spills or releases, and other incidents.
   - 2.5. Develop or update emergency preparedness and incident response procedures to comply with laws, ordinances, regulations, and other mandated directives.
   - 2.6. Report information to regulatory agencies as appropriate.

3. Coordinate incident response procedures with external agencies.
   3.1. Identify the external agency that will act as the first responder to the entity's facilities in the event of an incident.
   3.2. Develop and document emergency alerting procedures (such as automatic alerts via fire alarm, or manual alerts via telephone and notification protocols) and requirements (such as mandatory reporting of spills, injuries, and other incidents).
   3.3. Identify representatives from the first responder agencies and establish liaison relationships with the relevant agency personnel.
   3.4. Invite personnel from first responder agencies to tour the entity's facilities and ask them to provide recommendations for improvements to the incident response plans.
   3.5. Identify and document incident response roles and responsibilities for the types of incidents and scenarios outlined in Professional Practice Five.
   3.6. Coordinate, conduct, and participate in training, drills, and exercises with external agencies and first responders to increase awareness and compliance with regulations.
   3.7. Conduct a debriefing meeting following any training, drills, and exercises. Document actions that must be taken in order to improve incident response capabilities.
   3.8 Document the exercise results and lessons learned. Provide copies to leadership and other relevant organizational parties. Update the incident response plans using the lessons learned and feedback from exercises/training in accordance with the schedule established in Professional Practice Eight.

Legal Disclaimer

Committee

Chair, Raymond Seid, MBCP, CBCLA, ARMP

DRI Coordinator, Al Berman, CBCP, CBCV, MBCP, CBCLA

Harley Lemons, MBCP

Michele Turner, MBCP

Review Committee

Mike Morganti, MBCP, CBCLA

Harvey Betan, CBCP, CBCV, MBCP, CBCLA

Don Schmidt, CBCP, CBCLA

Editors

Chloe Demrovsky, CBCV

Buffy Rojas Leach

Acknowledgments

Gary Villeneuve, MBCP, CBCLA, CPSCP, ARMP

Bobby Williams, CBCP, MBCP

All of our translation committees