The Professional Practices for Business Continuity Management

This document is maintained by DRI International.
For questions about this document, contact driinfo@drii.org.
For more information, visit www.drii.org.

Version May 2023

DRI International

Table of Contents

Foreword

About the Professional Practices for Business Continuity Management

Created and maintained by Disaster Recovery Institute (DRI) 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, and 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) is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. Terms are defined in *The International Glossary for Resilience* published and maintained by DRI International.

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

Note on the Current Version

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 beginning on November 1, 2021, and finishing August 1, 2022. The goals were to provide information that would include:

- An enhanced version of Professional Practice Five: Incident Preparedness and Response to include more of the preparation activities related to incident management;
- More information on identifying various cyber threats and strategies for remediation by integrating cybersecurity activities into business continuity management;
- Enhancing the use of insurance as a risk transfer tool and providing more specific types of insurance policies that should be an integral part of business continuity management;
- Introducing more robust data backup techniques;
- More technology-specific strategies, and;
- More manufacturing strategies.

In addition, the titles of four of the Professional Practices were modified:

- Professional Practice One was changed from Program Initiation and Management to Program Management;
- Professional Practice Five was changed from Incident Response to Incident Preparedness and Response to emphasize the activities that are necessary to create an effective response plan;
- Professional Practice Eight was changed from Business Continuity Plan Exercise, Assessment, and Maintenance to Business Continuity Plan Exercise/Test, Assessment, and Maintenance for consistency; and
- Professional Practice Ten was changed from Coordination with External Agencies to Coordination with External Agencies and Resources.

Unless otherwise specified, lists are in no particular order. Needs may vary by entity.

Since the last revision of the Professional Practices, the resilience discipline has grown to be more holistic and inclusive as has the technical and business vocabulary. In the next stage of the update to the Professional Practices process, DRI will reconcile the terminology used in the Professional Practices and that used in *The International Glossary for Resilience.* The objective is to add and modify terms in the glossary to reflect the evolution of the language.

Acknowledgments

Thank you to our Professional Practice Committee Members for their contribution to the profession.

Revision Committee
Chair, Raymond Seid, MBCP, CBCLA, ARMP
DRI Coordinator, Al Berman, MBCP, CBCLA, CCRP
Michele Turner, MBCP
Andrea Abrams, CBCP
Mike Semel, CBCP

Review Committee
Don Schmidt, CBCP, CBCLA

Editors
Chloe Demrovsky, CBCV
Buffy Rojas Leach

Executive Summary

Objectives of the Professional Practices for Business Continuity Management

1. **Program Management**
   - 1.1. Establish the need for a business continuity program.
   - 1.2. Introduce key concepts, such as program management, risk awareness, impact to critical functions/processes, recovery strategies, training and awareness, and exercising/testing.
2. **Risk Assessment**
   - 2.1. Identify risks that could impact an entity's resources, processes, or reputation.
   - 2.2. Assess risks to determine the potential negative impacts to the entity, enabling the entity to determine the most effective means to reduce them.
3. **Business Impact Analysis**
   - 3.1. Identify and prioritize all of the entity's functions, processes, and dependencies in order to determine the greatest impact upon the entity should the functions not be available. This analysis should be retained and available to assist the entity in understanding incidents and/or the resulting consequences. Quantify the impact to the entity, its services, and the affected parties.
   - 3.2. Analyze, document, and communicate the findings to highlight all gaps between the entity's requirements and its current capabilities.
4. **Business Continuity Strategies**
   - 4.1. Select strategies to reduce gaps as identified during the risk assessment and business impact analysis.
   - 4.2. Identify the major functions of the entity, including potential third-party service providers, with the support of the responsible party for the business impact analysis.
5. **Incident Preparedness and Response**
   - 5.1. Understand the types of incidents that could threaten life, property, operations, or the environment and their potential impacts.
   - 5.2. Establish and maintain capabilities to protect life, property, operations, and the environment from potential incidents through the implementation of an incident management system to command, control, and coordinate response, continuity, and recovery activities with internal and external resources.
6. **Plan Development and Implementation**
   - 6.1. Document plans to be used during an incident that will enable the entity to continue to function.
   - 6.2. Define the exercise/testing criteria to validate that the plans will accomplish the desired goal.
7. **Awareness and Training Programs**
   - 7.1. Establish and maintain training and awareness programs that result in personnel being able to respond to disruptive incidents in a calm and efficient manner.
8. **Business Continuity Plan Exercise/Test, Assessment, and Maintenance**
   - 8.1. Establish a business continuity plan exercise/test, assessment, and maintenance program to improve the state of readiness of the entity.
9. **Crisis Communications**
   - 9.1. Create and maintain a crisis communications plan.
   - 9.2. Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties.
10. **Coordination with External Agencies and Resources**
    - 10.1. Establish policies and procedures to coordinate response activities with applicable public entities and private resources in accordance with Professional Practice Five: Incident Preparedness and Response.

Professional Practice One: Program Management

Objectives

1. Establish the need for a business continuity program.
2. Introduce key concepts, such as program management, risk awareness, impact to 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. Create documentation to facilitate leadership program adoption and ongoing support.
3. Coordinate and/or lead the implementation of the business continuity program throughout the entity.

Activities

1. Establish the need for a business continuity program.
    - 1.1. Research, reference, and quantify relevant business, legal, regulatory, and contractual requirements and restrictions both from an internal and external perspective. Provide recommendations on compliance and conformity for the entity. Obtain subject matter experts to provide detailed information on specific operational and technical considerations as they apply to the entity. Reference relevant standards.
    - 1.2. Identify and resolve any conflicts between the entity's governance, policies, procedures, and external requirements. Ensure the proposed business continuity program adequately addresses any gaps that would reduce the effectiveness of the program. Review guidance, past incidents, and any existing audit reports.
    - 1.3. State the benefits of business continuity within the context of the entity's mission.
    - 1.4. Explain the role of leadership, including accountability and liability related to an ineffective business continuity program.
    - 1.5. 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. Create documentation to facilitate leadership program adoption and ongoing support.
    - 2.1. Develop a charter for the business continuity program within the context of the entity's mission. Include objectives, assumptions, and scope for the business continuity program.
    - 2.2. Develop a budget and acquire resources for the business continuity program.
    - 2.3. Define the business continuity program structure. Identify potential policy needs and critical success factors.
    - 2.4. Identify leadership for business continuity program development.
    - 2.5. Present the proposed business continuity program structure to obtain leadership support and approval for the business continuity program.
    - 2.6. Obtain leadership approval for the budget.
    - 2.7. Establish a steering committee/oversight body to have responsibility for the business continuity program.
    - 2.8. Define the scope of responsibilities and overall accountability of each member of the steering committee/oversight body and its support functions.

3. Coordinate and/or lead the implementation of the business continuity program throughout the entity.
   - 3.1. Advise the steering committee/oversight body to drive the implementation of objectives, program structure, and critical success factors. Address alignment with existing organizational policies.
   - 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:
     - 3.4.1. Risk assessment and strategies
     - 3.4.2. Business impact analysis
     - 3.4.3. Recovery strategy selection and implementation
     - 3.4.4. Incident management, response and recovery
     - 3.4.5. Crisis management and communication
     - 3.4.6. Post-incident gap analysis and implementation earned
     - 3.4.7. Business continuity plan documentation
     - 3.4.8. Plan exercising/testing, maintenance, and audit activities
     - 3.4.9. Response, recovery, and restoration activities during/after an incident
   - 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
     - 3.6.4. Personnel requirements
   - 3.7. Oversee the ongoing effectiveness of the business continuity program.
     - 3.7.1. Develop, monitor, track, and report ongoing management and documentation requirements for the business continuity program.
     - 3.7.2. Monitor, track, and report compliance/conformity to regulatory and industry standards.
     - 3.7.3. Develop and execute internal and external benchmarking strategies.
   - 3.8. Inform leadership as circumstances change.
     - 3.8.1. Develop a schedule to report on the status of the business continuity program to leadership.
     - 3.8.2. Prepare regular status reports for leadership that contain accurate and timely information on key elements of the business continuity program.

Professional Practice Two: Risk Assessment

Objectives

1. Identify risks that could impact an entity's resources, processes, or reputation.
2. Assess risks to determine the potential negative impacts to the entity, enabling the entity to determine the most effective means to reduce them.

Professional's Role

1. Work with leadership and any risk management groups to gain agreement on a risk assessment methodology.
2. Identify, develop, and implement information-gathering activities across the entity to identify risks.
3. Determine the probability and impact of the identified risks.
4. Evaluate the impact of risks on those factors that are essential to conducting the entity's operations.
5. Identify and evaluate the effectiveness of controls employed to reduce the impact of exposures.
6. Document and present the risk and vulnerability assessment and recommendations to leadership for approval.
7. Request approval from leadership to develop the entity's risk appetite to use as a basis for the management of an ongoing risk assessment process.

Activities

1. Work with leadership and any risk management groups to gain agreement on a risk assessment methodology.
    - 1.1. Work with leadership and any risk management groups to identify internal and external requirements.
    - 1.2. Gain agreement on a clear, standardized risk assessment methodology.
    - 1.3. Gain an understanding of the entity's risk appetite and threshold.
    - 1.4. Identify risk analysis methodologies and tools, which may include, but are not limited to, quantitative and qualitative analytics.
    - 1.5. Review and incorporate the reliability and confidence factors of the data that is being used.
    - 1.6. Select the appropriate methodology and tools for entity-wide implementation.
    - 1.7. Establish measurement criteria necessary to quantify the probability and impact of identified risks as well as the effectiveness of any existing controls.
2. Identify, develop, and implement information-gathering activities across the entity to identify risks.
    - 2.1. Identify the 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, insurance, legal counsel, physical security, supply chain management, information security, and relevant stakeholders to identify risks.
    - 2.3. Determine information sources that will be used to collect data on risks and reference the sources in the report. Develop a strategy to gather information consistent with the entity's policies.
    - 2.4. Create entity-wide methods of information collection and distribution, including, but not limited to, forms, questionnaires, interviews, meetings, and/or combinations of these processes.
    - 2.5. Identify the entity's risks.
        - 2.5.1. Achieve a holistic view of entity-wide risk by identifying risks, accounting for the frequency, probability, speed of development, severity, and financial and/or reputational impact.
        - 2.5.2. 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 incidents with or 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, rate of development, severity, impact, and whether there are pre-incident warnings, as in the case of hurricanes /typhoons/cyclones.
    3.2. Identify the impacts of identified risks by category, which may include, but are not limited to, workforce availability, supply chain, cybersecurity, information technology, product or service delivery, facility, reputational, legal, and regulatory.
    3.3. Evaluate identified risks in terms of those risks that are under the entity's control and those risks that are beyond the entity's control.
4. Evaluate the impact of risks on those factors that are essential to conduct the entity's operations.
    4.1. Provide personnel, information technology, communications technology, and logistics, such as transportation. Identify and evaluate the effectiveness of controls and safeguards that are currently in place.
    4.2. Identify and evaluate the effectiveness of asset protection. Identify and evaluate the effectiveness of controls and safeguards that are currently in place for internal and external groups upon which the entity is dependent 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, which may include, but are not limited to, workforce health and safety, physical security practices, information security, employment practices, and privacy practices.
5. Identify and evaluate the effectiveness of controls employed to reduce the impact of exposures.
    5.1. Evaluate equipment which may include, but is not limited to, sprinkler systems, fire brigades, generators, multiple internet connections, data backups, and uninterruptible power supply (UPS).
    5.2. Evaluate security-related communications within the entity and with external service providers.
    5.3. Identify trigger points for service and support areas to identify, escalate, and execute strategies selected to address risks.
    5.4. Recommend changes needed to reduce the impact of identified risks, which may include, but are not limited to:
        5.4.1. Identify changes to physical protection, including, but not limited to, the following actions:
            5.4.1.1. Identify requirements necessary to restrict access to all controlled areas.
            5.4.1.2. Investigate the need for barriers, strengthened structures, and alarms to deter unsafe and/or unauthorized entry. Address vulnerabilities of the location that may result from health, physical construction, geographic location, corporate neighbors, facilities infrastructure, and community infrastructure. Identify the need for the use of trained personnel and/or equipment to conduct checks at points of entry. Evaluate the need for surveillance equipment at access control points.
            5.4.1.3. Identify changes to security and access controls, tenant insurance, and leasehold agreements.
        5.4.2. Identify changes to cybersecurity and information technology, including, but not limited to, the following actions:
            5.4.2.1. Assess the need for protection of data that is being stored, whether the data is used for processing or for a backup in process. Investigate such techniques as air gapping and isolation to protect backup data.
            5.4.2.2. Evaluate information security including hardware, software, data, and network monitoring, such as detection and notification.
            5.4.2.3. Evaluate the protection of the physical location of cybersecurity and information technology assets.
        5.4.3. Identify changes to policies, procedures, communication, and personnel training procedures.
        5.4.4. Utilize a checklist and have work reviewed prior to implementation.
        5.4.5. Identify changes including duplication and built-in redundancies to utilities.

5.5. 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. Document and present the findings of the risk assessment, which may include, but are not limited to, the following components:
      6.2.1. Information on risks and exposures based on the risk and vulnerability analysis
      6.2.2. An assessment of any existing controls and/or strategies to manage known risks
      6.2.3. Recommendations for new controls to be implemented; provide a cost/benefit analysis to justify recommendations
      6.2.4. Prioritized recommendations for the implementation of any new controls
      6.2.5. Recommendations for appropriate means to transfer risk
7. Request approval from leadership to develop the entity's risk appetite to use as a basis for the management of an ongoing risk assessment process.
   7.1. Document the deferral decisions of leadership and/or non-acceptance of risks as applicable.

Professional Practice Three: Business Impact Analysis

Objectives

1. Identify and prioritize all of the entity's functions, processes, and dependencies in order to determine the greatest impact upon the entity should the functions not be available. This analysis should be retained and available to assist the entity in understanding incidents and/or the resulting consequences. Quantify the impact to the entity, its services, and the affected parties.
2. Analyze, document, and communicate the findings to highlight all gaps between the entity's requirements and its current capabilities.

Professional's Role

1. Identify and document the qualitative and quantitative criteria to be used to assess the impact to the entity resulting from an incident.
2. Recommend objectives and scope for the business impact analysis process.
3. Establish the criteria and methodology to be used in conducting the business impact analysis process.
4. Analyze the collected data against the approved criteria to establish a recovery time objective (RTO), recovery point objective (RPO), and resources for each operational area and its supporting technology.
5. Prepare and present the business impact analysis results to leadership. Gain acceptance of the recovery time objectives, recovery point objectives, and resources as detailed in the business impact analysis.

Activities

1. Identify and document the qualitative and quantitative criteria to be used to assess the impact to the entity resulting from an incident.
    - 1.1. Identify critical deadlines (for example, wire transfers, payroll, or regulatory filings).
    - 1.2. Define and obtain approval for criteria to be used to assess the impact to the entity and affected parties, which may include, but is not limited, to the following items:
        - 1.2.1. Impact to customers, including, but not limited to, how quickly customers will learn that a problem exists; the likelihood that they will terminate their relationship with the entity; existing agreements requirements and impacts to service level agreements (SLAs); and the entity's impact to customers' supply chains.
        - 1.2.2. 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; impact to credit rating; contractual fines or penalties; losses resulting from required payments for fixed costs; or increased overtime expenses.
        - 1.2.3. Regulatory impact, including, but not limited to, fines, penalties, the involuntary recall of products, or the revocation of any license or permit.
        - 1.2.4. Operational impact, including, but not limited to, discontinued or reduced service levels and supply chain disruptions.
        - 1.2.5. Reputational impact, including, but not limited to, negative media attention, negative social media commentary, negative community perception, and impact to shareholder confidence.
        - 1.2.6. Workforce and interested party impact, including, but not limited to, the loss of life, injury, impact to community services, environment, and psychological impact.
    - 1.3. Financial elements that provide risk transfer through insurance, which may include, but are not limited, to business interruption, contingent business interruption, supply chain, cyber, and extra expense insurance.

2. Recommend objectives and scope for the business impact analysis process.
    2.1. Gain leadership agreement on business impact analysis methodology and the criteria to be used to establish the business impact analysis process and methodology.
    2.2. Identify and obtain leadership support and/or identify the responsible party for the business impact analysis.
    2.3. Choose a methodology or tool for the business impact analysis process and data collection. Data to be collected should include operational processes and incremental resource requirements based on recovery duration.
    2.4. Data to be collected should include the impact from the loss of any resource needed for the operational process.
    2.5. Data to be collected should include internal and external dependencies.
    2.6. Identify additional requirements that are specific to the entity.
    2.7. Plan and coordinate data gathering and analysis.
    2.8. Data collection may be conducted using questionnaires.
        2.8.1. Develop questionnaires with instructions.
        2.8.2. Conduct project kick-off meetings to distribute and explain the questionnaires.
        2.8.3. Support respondents as they complete the questionnaires.
    2.9. Schedule follow-up interviews or workshops if clarification of the data provided is warranted.
        2.9.1. Define a clear agenda and set of objectives.
        2.9.2. Data collection may be conducted using workshops.
        2.9.3. For each workshop, identify the appropriate level of workshop participants and obtain agreement from leadership and/or identify the responsible party.
        2.9.4. Choose an appropriate venue by evaluating location, facilities, and participant availability. Consider virtual interviews for participants who are unable to attend in person.
        2.9.5. Facilitate and lead the workshop.
        2.9.6. Ensure workshop objectives are met.
        2.9.7. Ensure outstanding issues at the end of the workshop are identified and the appropriate follow up is conducted.
    2.10. Identify the major functions of the entity, including potential third-party service providers, with the support of the responsible party for the business impact analysis.
        2.10.1. Collect and review existing organizational charts.
        2.10.2. Identify specific individuals to represent each functional area of the entity.
        2.10.3. Identify third-party provider representatives to participate in the data collection process.
        2.10.4. Inform the selected individuals about the business impact analysis process and its purpose.
    2.11. Using the selected methodology, conduct the data collection necessary to support the business impact analysis.
3. Establish the criteria and methodology to be used in conducting the business impact analysis process.
    3.1. Identify and obtain agreement on the quantitative and qualitative evaluation methods for potential financial and non-financial impacts.
    3.2. Create a schedule to conduct the business impact analysis.
4. Analyze the collected data against the approved criteria to establish a recovery time objective (RTO), recovery point objective (RPO), and resources for each operational area and its supporting technology.
    4.1. Analyze the collected data to determine the prioritization of processes. Document all dependencies that exist between each business process and the supporting components, including, but not limited to, data systems and related technology, supply chain, third parties, and other resources. These dependencies may be intradepartmental, interdepartmental, or involve external relationships.
    4.2. Determine the order of recovery for business functions and technology using the collected data analysis.

5. Prepare and present the business impact analysis results to leadership. Gain acceptance of the recovery time objectives, recovery point objectives, and resources as detailed in the business impact analysis.
    5.1. Prepare a draft business impact analysis report using initial findings, highlighting identified deficiencies in a gap analysis.
        5.1.1. Provide a statement of the entity's mission, objectives, and goals,
        5.1.2. Summarize the impact to the entity's mission, objectives, and goals that may result from a disruptive incident.
        5.1.3. Provide a prioritized list of the entity's processes and services including the recovery time objectives and recovery point objectives, the resource requirements needed to recover and resume operations, and a gap analysis between the current recovery capabilities and the objectives, specifically:
            5.1.3.1. Time (recovery time objective versus actual recovery time)
            5.1.3.2. Data (recovery point objective versus actual loss of data)
            5.1.3.3. Resources (recovery resource requirements versus actual recovery resources)
        5.1.4. Issue the draft report to leadership to obtain feedback.
        5.1.5. Review the feedback obtained from leadership and adjust the findings, as needed.
        5.1.6. Schedule workshops or meetings with leadership to discuss any issues with the initial findings.
        5.1.7. Update the findings to reflect any changes arising from the workshops or meetings.
    5.2. Prepare the final business impact analysis report and submit to leadership for approval.
    5.3. Gain acceptance and approval from leadership for the recovery time objectives, recovery point objectives, and resources for each functional area as defined by the findings in the final business impact analysis report.

Professional Practice Four: Business Continuity Strategies

Objectives

1. Select strategies to reduce gaps as identified during the risk assessment and business impact analysis.
2. Identify the major functions of the entity, including potential third-party service providers, with the support of the responsible party for the business impact analysis.

Professional's Role

1. Utilize the data collected during the risk assessment and business impact analysis to identify the available continuity and recovery strategies for the entity's operations that will meet the recovery time objective, recovery point objective, and recovery requirements as identified in the business impact analysis.
2. Protect vital hardcopy records that may be in jeopardy of being destroyed.
3. Utilize the data collected during the risk assessment and business impact analysis to identify continuity and recovery strategies for the entity's technology in order to meet the recovery time objectives and recovery point objectives as defined in the business impact analysis.
4. Identify supply chain issues (for both suppliers and customers) from the business impact analysis that may affect recovery strategy selection.
5. Assess the cost of implementing identified strategies through a cost/benefit analysis.
6. Recommend strategies and obtain approval from leadership to implement.

Activities

1. Utilize the data collected during the risk assessment and business impact analysis to identify the available continuity and recovery strategies for the entity's operations that will meet the recovery time objective, recovery point objective, and recovery requirements as identified in the business impact analysis.
    - 1.1. Review the recovery requirements identified for each of the entity's functional areas.
    - 1.2. Identify alternative business continuity strategies. Potential options include, but are not limited to, the following strategies:
        - 1.2.1. Develop manual workaround procedures.
        - 1.2.2. Develop reciprocal agreements.
        - 1.2.3. Identify internal multi-use space that could be equipped to support recovery. Identify alternative facility strategies. Identify internal dual-use 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 objectives.
        - 1.2.4. Evaluate and identify external alternate site(s). Review alternate site options using the following criteria: location; the availability and suitability of the space; communications capabilities including voice and data; the availability of equipment and materials; and the security and robustness of the site, including the availability of resources.
        - 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 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 personnel to work from home.

1.3. Different types of operations may have specific needs. For example, manufacturing/distribution may use the following recovery strategies:
    1.3.1. Repair/rebuild at the time of the incident.
    1.3.2. Shift production from one line to another line.
    1.3.3. Shift production to another site with identical processing.
    1.3.4. Retool production at the affected site.
    1.3.5. Utilize existing inventory.
    1.3.6. Utilize excess capacity in other plants.
    1.3.7. Suspend, discontinue, or reduce production.
    1.3.8. Buy back product from customer(s) and redistribute.
    1.3.9. Provide a substitute product in lieu of the unavailable product.
    1.3.10. Outsource production.

2. Protect vital hardcopy records that may be in jeopardy of being destroyed.
    2.1. Documents should be scanned routinely to a cloud storage or other offsite storage solution to meet the recovery objectives for vital records. If an entity chooses to use photocopies of documents, they should be stored at an offsite location. Note that legal requirements for non-original documentation may vary from jurisdiction to jurisdiction. Research the validity of using copies or digital images in lieu of original documents.
    2.2. Review alternate site options using the following criteria as applicable:
        2.2.1. Location
        2.2.2. Accessibility
        2.2.3. Availability and suitability of the space
        2.2.4. Communications capabilities including voice and data
        2.2.5. Availability of equipment and supplies
        2.2.6. Hardening and sustainability requirements for the site, including the availability of resources such as power and water
    2.3. Assess the viability of alternative strategies with requirements set forth in the business impact analysis using the following criteria:
        2.3.1. Ability to meet the defined recovery objectives
        2.3.2. Comparison of potential solutions including advantages and disadvantages, and cost/benefit analysis
    2.4. Review existing insurance coverage.
        2.4.1. Types of insurance may include, but are not limited, to:
            2.4.1.1. Cyber
            2.4.1.2. Extra expense
            2.4.1.3. Business interruption
            2.4.1.4. Contingent business interruption
            2.4.1.5. Liability
            2.4.1.6. Payroll
            2.4.1.7. Property and casualty
            2.4.1.8. Natural disasters (flood insurance)
        2.4.2. Integrate insurance coverage that can be used to support the recovery process.
        2.4.3. Develop a cost/benefit analysis. Compare the anticipated results of potential strategies to the impacts defined in the risk assessment and business impact analysis.

3. Utilize the data collected during the risk assessment and business impact analysis to identify continuity and recovery strategies for the entity's technology in order to meet the recovery time objectives and recovery point objectives as defined in the business impact analysis.
    3.1. Review the recovery requirements identified for the entity's technology in each operational area.
    3.2. Identify alternative technology recovery strategies. Potential options include, but are not limited, to:
        3.2.1. Develop manual workaround procedures for each operational area.
        3.2.2. Implement a technology solution that meets the recovery objectives.
        3.2.3. Consider multiple data centers to regionally disperse data and operations.
        3.2.4. Utilize high availability systems providing for quick restart.
        3.2.5. Utilize third-party services.
        3.2.6. Leverage cloud computing.
    3.3. Identify a recovery site with adequate environmental controls.
    3.4. Identify technology equipment to support a remote workforce.
    3.5. Develop a preliminary cost/benefit analysis for the selected strategies for the entity's technology solution.
    3.6. Identify any logistical, regulatory, or financial delivery issues that may arise.
    3.7. Identify potential supply chain strategies to minimize the impacts based on the risk assessment and business impact analysis.
    3.8. Collaborate with industry representatives, government agencies, and other external contacts to exchange information to determine potential strategies.
4. Identify supply chain issues (for both suppliers and customers) from the business impact analysis that may affect recovery strategy selection.
    4.1. Identify any delivery issues that may arise from relocation to another site.
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 impact on the operational area.
        5.2.1. Consider financial and regulatory issues.
        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 that which is to be recovered.
    5.3. Consider the reduction in financial impact that insurance coverage provides in determining strategies that benefit from such insurance as business interruption, contingent business interruption, supply chain, cyber, and extra expense insurance.
6. Recommend strategies and obtain approval from leadership to implement.
    6.1. Document recommendations for approval from leadership.
    6.2. Obtain approval from leadership.

Professional Practice Five: Incident Preparedness and Response

Objectives

1. Understand the types of incidents that could threaten life, property, operations, or the environment and their potential impacts.
2. Establish and maintain capabilities to protect life, property, operations, and the environment from potential incidents through the implementation of an incident management system to command, control, and coordinate response, continuity, and recovery activities with internal and external resources.

Professional's Role

1. Identify hazards that could threaten life, damage property, interrupt operations, or contaminate the environment.
2. Identify applicable health and safety, fire, life safety, national security, environmental, cyber, and information security regulations enforceable by federal, state/provincial/regional, and/or local government.
3. Identify the availability and capabilities of internal and external resources required to protect life, property, and the environment for the identified types of incidents.
4. Identify and assess incident preparedness and response plans based on the risk assessment and vulnerabilities of assets at risk, as well as the availability and capabilities of existing internal and external resources.
5. Conduct a resource needs assessment.
6. Review incident preparedness and response plans.
7. Recommend the development, and assist with the implementation of, an incident management system for command, control, and coordination of resources during response activities.
8. Review incident preparedness and response plans and procedures with response personnel, and assist with the coordination of relevant internal and external agencies and resources.
9. Obtain and document formal leadership approval of plans and procedures.

Activities

1. Identify hazards that could threaten life, damage property, interrupt operations, or contaminate the environment.
    - 1.1. Hazard categories include natural hazards (biological, geological, meteorological), human-caused accidental and intentional acts (chemical, nuclear), and technology-related causes.
    - 1.2. For each category of hazard, identify foreseeable scenarios and note the following information:
        - 1.2.1. Probability of occurrence
        - 1.2.2. Magnitude or scope
        - 1.2.3. Area(s) of impact
        - 1.2.4. Vulnerabilities of assets at risk that make them susceptible to the hazard
        - 1.2.5. Existing prevention and mitigation strategies
    - 1.3. For each type of incident, identify potential impacts including, but not limited to, casualties, property damage, environmental contamination, reputational, financial, regulatory, and/or inability to conduct mission critical activities.
2. Identify applicable health and safety, fire, life safety, national security, environmental, cyber, and information security regulations enforceable by federal, state/provincial/regional, and/or local government.
    - 2.1. Comply with applicable regulatory and entity requirements for incident preparedness and response.

3. Identify the availability and capabilities of internal and external resources required to protect life, property, and the environment for the identified types of incidents.
    3.1. Identify and establish relationships with internal departments and external agencies that have responsibilities for incident preparedness and response.
    3.2. Gather incident preparedness and response plans from internal resources including environmental health and safety (EHS), security, facilities management, human resources, and others.
    3.3. Contact public agencies including, but not limited to, homeland security, emergency management, emergency medical services, fire departments, law enforcement, hazardous materials, rescue, and cyber incident response in order to identify requirements, practices, and resources, as well as establish liaison relationships.
4. Identify and assess incident preparedness and response plans based on the risk assessment and vulnerabilities of assets at risk, as well as the availability and capabilities of existing internal and external resources.
    4.1. Life safety measures including, but not limited to, evacuation, shelter-in-place, lockdown, “run, hide, fight”, and accountability of personnel responding to, or affected by, the incident.
    4.2. Health, hygiene, and safety protocols including response to medical emergencies.
    4.3. Property protection such as the supervision and operation of building systems and equipment, including utilities; heating, ventilation, and air conditioning (HVAC); fire detection and suppression; and communications and warning systems.
    4.4. Property conservation activities to prepare a facility for forecasted severe weather or another disruptive incident.
    4.5. Containment of spills or leaks of hazardous materials to prevent injury and environmental contamination. Supervision and operation of systems designed to contain hazardous materials onsite. Requirements for notification to, and reporting on, incidents to environmental authorities.
    4.6. Response time and capabilities of the public fire department, emergency medical services, rescue service, and hazardous materials contractor.
5. Conduct a resource needs assessment.
    5.1. Resources needed to protect life, property, and environment
    5.2. Qualified internal and external personnel to respond to incidents
    5.3. Systems and equipment, including, but not limited to, detection, alarm, communications, warning, suppression, and containment available for incident response
    5.4. Applicable mutual aid or partnership agreements are documented and current
    5.5. Gaps between required resources and the availability and capability of internal and external resources
    5.6. Gaps between requirements and the availability and capabilities of resources
6. Review incident preparedness and response plans and assess abilities.
    6.1. Monitor threats and hazards and promptly detect incidents.
    6.2. Warn persons in danger or potentially in danger to take protective action.
    6.3. Alert internal and external first responders.
    6.4. Report incidents to the responsible person, department, and/or agency.
    6.5. Escalate the response as the situation analysis dictates.
7. Recommend the development, and assist with the implementation of, an incident management system for command, control, and coordination of resources during response activities.
    7.1. Develop an incident management organization with defined roles, responsibilities, lines of authority, delegation of authority, and succession of authority.
    7.2. Gain an understanding of local, state, and federal incident command and incident management systems.
    7.3. Develop procedures for situation analysis, incident action plan development, management of internal and external resources, and the procurement of additional resources.
    7.4. Develop procedures for incident briefings to include initial and periodic situation reports.
    7.5. Document communications during an incident.

7.6. Establish a physical or virtual emergency operations center (EOC) for the coordination of response, continuity, and recovery activities.
    7.6.1. Physical emergency operations centers should be sized to house the anticipated number of persons and equipped to support occupancy for the duration of the types of incidents identified.
    7.6.2. The emergency operations center should be equipped with the types of communications capabilities necessary to support the scope and duration of foreseeable incidents.
    7.6.3. Procedures should be established for emergency operations center management, operations, planning, logistics, and finance/administration, defining roles and responsibilities, communications, and information flow. Secure copies of policies, plans, and procedures must be immediately available to emergency operations center staff.
8. Review incident preparedness and response plans and procedures with response personnel, and assist with the coordination of relevant internal and external agencies and resources.
    8.1. Identify documents, such as pre-incident plans, emergency action plans, and hazardous materials management plans, that must be submitted to public agencies.
9. Obtain and document formal leadership approval of plans and procedures.

Professional Practice Six: Plan Development and Implementation

Objectives

1. Document plans to be used during an incident that will enable the entity to continue to function.
2. Define the exercise/testing criteria to validate that the plans will accomplish the desired goal.

Professional's Role

1. Use the approved strategies developed in Professional Practice Four: Business Continuity Strategies 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. Consider plan types based on the needs of the entity.
4. Publish the plan documents.

Activities

1. Use the approved strategies developed in Professional Practice Four: Business Continuity Strategies 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 designated authorities.[1]
        - 1.1.3. Complete all required tasks for plan implementation, which may include, but are not limited to:
            - 1.1.3.1. Acquiring internal and external recovery and business continuity plan resources
            - 1.1.3.2. Establishing response, recovery, and restoration processes
            - 1.1.3.3. Establishing processes 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 required to document the plans.
        - 2.1.1. Ensure alignment with the scope of the planning process.
        - 2.1.2. Comprehensive business continuity plans address resources, people, facilities, and technology. Business continuity plan components may include regulatory requirements, strategic (delegation of authority), operational, incident response, recovery, restoration, and return-to-normal operations.
        - 2.1.3. Strategic considerations may include, but are not limited to:
            - 2.1.3.1. The amount of advance warning
            - 2.1.3.2. Whether the term will be short or long
            - 2.1.3.3. Whether the impacts will be local or regional, regional, or specific to an entity's sites
            - 2.1.3.4. Whether there is cascading impact potential brought about by a cascading event. A cascading event occurs when the incident has the potential for creating additional adverse effects.
    - 2.2. Define the roles and responsibilities for plan development, including the following actions:
        - 2.2.1. Identify the tasks to be undertaken, including exercise/testing.
        - 2.2.2. Develop a timeline for plan completion, including exercise/testing.
        - 2.2.3. Develop a process for reviewing, evaluating, and recommending tools, which may include, but are not limited, to planning software, exercise/testing software, databases, specialized software, and templates.
        - 2.2.4. Develop templates that can be used to capture information on processes, technology, and other plan components.
        - 2.2.5. Identify other supporting documentation.
        - 2.2.6. Ensure that there are imbedded mechanisms to facilitate maintenance, such as defined version control.

[1] See Professional Practice One: Program Management for further detail on defining the reporting structure.

2.3. Define the content requirements for the plan, which may include, but are not limited, to:
    2.3.1. Governance, policies and procedures, distribution control, confidentiality requirements, and authority levels
    2.3.2. The scope and objectives, including assumptions, aligned to the entity's mission, goals, objectives, and business continuity policies, including the identification of time-sensitive operations and the resources needed to support them
    2.3.3. Organizational structures of teams as well as the roles and responsibilities of each team
    2.3.4. Plan activation procedures: initial assessment, escalation, reporting processes, declaration, plan activation, recovery, rescinding declaration, and resumption of normal operations

3. Coordinate the effort to document recovery plans for the entity's operations and the supporting infrastructure. Consider plan types based on the needs of the entity.
    3.1. Incident management plan(s), which should include the following:
        3.1.1. Life-safety procedures including evacuation and shelter-in-place
        3.1.2. Incident command and control procedures
        3.1.3. Roles and responsibilities for the personnel participating in incident management
        3.1.4. Emergency operations center (EOC) location
        3.1.5. The process for conducting an assessment, which should include:
            3.1.5.1. Limiting the entity from further loss including a cost/benefit analysis of repair versus replacement of entity assets
            3.1.5.2. Estimated time needed to repair or replace entity resources
            3.1.5.3. Restoration methods for entity resources
            3.1.5.4. Approval process for restoration and insurance claim filing
            3.1.5.5. Salvage process
    3.2. Crisis management plan(s)[2], which should include the following:
        3.2.1. Members of the crisis management team
        3.2.2. An outline of the procedures for incident response, crisis communications, and recovery
        3.2.3. Notification procedures to interested parties at appropriate intervals during an incident (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 hazardous materials (HAZMAT) services, investors, the governing board of directors or other relevant leadership authority, labor representatives, neighboring occupants and other interested groups (such as customers, vendors, or suppliers)
    3.3. Recovery site activation plan(s), which should include the following:
        3.3.1. Alert procedures
        3.3.2. Declaration procedures
        3.3.3. Recovery infrastructure, which may include:
            3.3.3.1. Administration and logistics
            3.3.3.2. New equipment or just-in-time deliveries
            3.3.3.3. Technical services and procedures
            3.3.3.4. End-user interface
            3.3.3.5. Business operations
            3.3.3.6. Inter-site logistics and communications
            3.3.3.7. Production recovery process and procedure
            3.3.3.8. Logistics involved in arranging for the travel and housing of recovery staff; transporting the resources needed for recovery, maintenance, and security of the recovery facility; and providing for the procurement of additional resources

[2] See also Professional Practice Five: Incident Preparation and Response and Professional Practice Nine: Crisis Communications.

3.4. Operational recovery plan(s), including:
    3.4.1. Recovery teams, including both primary and alternate members
    3.4.2. 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. Business continuity plan(s), 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. Technology recovery plan(s), which should include the following:
    3.6.1. Recovery teams including primary and alternate members
    3.6.2. Mobilizing and managing alternate resources, including such resources as may be required for:
        3.6.2.1. Storage, which may include, but is not limited to, network attached storage devices and data storage devices
        3.6.2.2. Voice and data communications hardware, which may include, but are not limited to, local area network (LAN) switches, power over ethernet switches, and managed/unmanaged switches
        3.6.2.3. Hardware and software requirements, which may include, but are not limited to, servers, tape drives/tape library, application software, operating systems, applications, and security software
        3.6.2.4. Infrastructure requirements, which may include, but are not limited to, power sources and controllers; heating, ventilation and air conditioning (HVAC); cabling; and access security
        3.6.2.5. Information security requirements, which may include, but are not limited to, firewalls, access authentication, malware protection, encryption, and equipment requirements
    3.6.3. The technology recovery plan(s) should outline a detailed procedure for the recovery of the technology environment, including the following steps:
        3.6.3.1. Identify application and dependencies
        3.6.3.2. A process for change management
        3.6.3.3. A process for problem management
        3.6.3.4. A plan for exercising/testing and maintenance
3.7. Plan(s) to rescind recovery site activation plan(s) and other emergency actions

4. Publish the plan documents.
    4.1. Provide a final draft of the plan, including exercising/testing recommendations, to business process owners.
    4.2. Obtain approval from leadership.
    4.3. Establish procedures for the distribution and control of plans.
    4.4. Ensure access to information is available even when the information technology (IT) environment is compromised.
    4.5. Publish and distribute the plans or portions of the plans to those with authorization to receive information.

Professional Practice Seven: Awareness and Training Programs

Objectives

1. Establish and maintain training and awareness programs that result in personnel being able to respond to disruptive 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 entity's functions.
3. Prioritize the awareness and training requirements for entity 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

1. Establish the objectives and components of the business continuity awareness and training program.
   - 1.1. Define the awareness and training program.
   - 1.2. Recommend awareness and training schedule.
   - 1.3. Obtain leadership support for the program.
   - 1.4. Obtain commitment from personnel.
2. Identify the awareness and training requirements across the entity's functions.
   - 2.1. Define and document the desired level of business continuity awareness and training across the entity.
   - 2.2. Define and document awareness and training resource and budget requirements.
3. Prioritize the awareness and training requirements for entity personnel.
   - 3.1. When designing an awareness program, it is important to consider which internal personnel must understand the relevant components of the business continuity program. Topics include, but are not limited to:
     - 3.1.1. Business continuity program objectives, scope, and components
     - 3.1.2. Incident notification and expectations as well as incident preparedness and response procedures
   - 3.2. When designing a training program, it is important to consider which personnel must be trained in which components of the business continuity program. Required topics in which personnel should be trained, may include, but are not limited to:
     - 3.2.1. Incident reporting
     - 3.2.2. Alert notifications
     - 3.2.3. Evacuation and shelter-in-place procedures
     - 3.2.4. Scenario-based walkthroughs that exercise/test operations and technology business continuity plan elements
   - 3.3. Required management training, may include, but is not limited to:
     - 3.3.1. Incident identification and reaction exercises/tests
     - 3.3.2. Scenario-based operations and technology walkthroughs
   - 3.4. Required topics in which business continuity team members should be trained, may include, but are not limited to:
     - 3.4.1. Evacuation and shelter in place exercises/tests
     - 3.4.2. Scenario-based walkthroughs
     - 3.4.3. 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:
        4.1.1. Conduct a survey of needs to assess the current state of awareness and training in order to determine if it is in alignment with the goals set by leadership. Survey participants could be at various levels and may include diverse parties such as functional management, plan participants, technology, and the broader business population.
        4.1.2. Use the collected data to identify trends and gaps.
        4.1.3. Review previous exercise/test results and conduct gap analyses.
    4.2. Benchmark the current levels of awareness and training within the entity against desired levels, and initiate a plan to address awareness and training gaps.
    4.3. Design the training process to include the following:
        4.3.1. Define objectives, identify, and select delivery methods, including, but not limited to, scenario-based exercises/tests and communications.
        4.3.2. Define the roles and responsibilities for the training program.
        4.3.3. Create a written training plan and supporting policies.
        4.3.4. Obtain leadership approval.
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 awareness and training program, which may include, but are not limited to, courseware, websites, social media tools, applications, conferences, webinars, user groups and associations, white papers and other publications, certifications bodies, and 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 self-evaluation by participants.
    6.4. Review the results of the awareness and training program activities periodically. Provide a report to leadership on the outcomes of the program.
    6.5. Evaluate the awareness and training program periodically to ensure the current needs of the entity are met.
    6.6. Ensure that the awareness program is part of the new hire onboarding process.

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

Objectives

1. Establish a business continuity plan exercise/test, assessment, and maintenance program to improve the state of readiness of the entity.

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. Provide written recommendations based on the exercise/test results, including revisions to strategies and plans if desired outcomes cannot be met.

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 business continuity program meets its objectives.
        - 1.1.2. Identify any gaps in the business continuity program, and provide remedies to remove the gaps and improve the program's execution.
    - 1.2. Obtain the necessary support and leadership approvals for the development of the exercise/test program.
        - 1.2.1. Document the exercise/test program criteria.
        - 1.2.2. Define any exercise/test program assumptions.
        - 1.2.3. In order to create a comprehensive program, identify the types of exercises/tests 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; 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.
        - 1.2.4. 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/reporters, monitors, auditors/reviewers, facilitators, suppliers, and outsourced service providers.
        - 1.2.5. Use the entity's risk assessment mitigation priorities (refer to Professional Practice Two: Risk Assessment) to create realistic scenarios. Include activities that reference the recovery strategies and the ability to achieve objectives within established timeframes. Determine the exercise/test requirements and draft a detailed plan for the activities.
            - 1.2.5.1. Define and document objectives for the exercise/test.
            - 1.2.5.2. Define and document the scope of the exercise/test.
            - 1.2.5.3. Define the exercise notification process, which may include announced or unannounced exercises. Develop a specific schedule for the exercise/test to be conducted on, at least, an annual basis or more frequently to meet regulatory requirements or changes in the entity's structure (which may include acquisitions and mergers, reorganizations, consolidations, sales of portions of entity) and/or operations. Develop a multi-year exercise/test schedule that incorporates lessons learned from previous exercises/tests and increasingly contains greater exercise/test entity elements.
            - 1.2.5.4. Define and document quantitative and qualitative evaluation criteria in alignment with the objectives of the exercise/test. This includes measuring the results of the exercise/test against the recovery time objectives and recovery point objectives defined in the business impact analysis. Identify activities that must occur prior to the exercise/test, which may include, but are not limited to, the following:

1.2.5.4.1. Identify the resources required to conduct the exercise/test.
1.2.5.4.2. Identify the participants necessary to participate in the exercise/test.
1.2.5.4.3. Distribute communications that explain the objectives of the exercise/test and the roles of all parties (including law enforcement, emergency services, and the media). Provide a list of hardware, software, supplies, equipment, and other resources required for the exercise/test.
1.2.5.4.4. Document and communicate the resource requirements necessary to conduct the exercise/test.
1.2.5.4.5. Specify whether the exercise/test will use a production or non-production environment.
1.2.5.4.6. Specify the time, date, and location(s) of the exercise/test. Provide a timetable of events and circulate to all the participants.
1.2.5.4.7. Establish a cancellation plan for the exercise/test should the exercise/test fail to achieve specified objectives, which precludes the possibility that the exercise/test will reach scheduled completion.

1.2.6. Conduct the exercise/test as planned.
1.2.6.1. Should an actual incident occur during an exercise/test, there must be a predetermined mechanism for cancelling the exercise/test and invoking the actual business continuity process. This may differ from the cancellation plan in 1.2.5.4.7.
1.2.6.2. Record the exercise/test events.
1.2.6.3. Document the exercise/test results.
1.2.6.4. Declare an end to the exercise/test.
1.2.6.5. Perform the shut-down procedures at the conclusion of the exercise/test.
1.2.6.6. Perform any necessary cleanup activities.

1.2.7. Identify activities that must be completed following the exercise/test.
1.2.7.1. Conduct debriefing sessions to review the results of the exercise/test. Identify lessons learned and actions for improvements.
1.2.7.2. Report on the results of the exercise/test. Provide a comprehensive summary with recommendations.
1.2.7.3. Document an action plan for implementing the recommendations that resulted from the exercise/test.
1.2.7.4. Note any outstanding issues identified as a result of the exercise/test or that existed prior to the exercise/test.
1.2.7.5. Identify action items including responsibilities assigned to specific participants and timeframes for resolution.
1.2.7.6. Monitor the progress to completion of the identified action items. Document the lessons learned from the exercise/test including expected versus actual results and unexpected results.
1.2.7.7. Communicate the results of the exercise/test.

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 elements. Identify specific personnel and their areas of responsibility.
2.1.2. Prepare maintenance schedules and review procedures.
2.1.3. Create procedures to facilitate maintenance of the plan.
2.1.4. Select maintenance tools.
2.1.5. Monitor the maintenance activities.
2.1.6. Establish a change control process for the plan.

2.2. Ensure that scheduled plan maintenance addresses all approved recommendations from the exercise/test. Report on maintenance activities to the relevant parties. Define a change management process for the plan maintenance program.
    2.2.1. Analyze any entity changes that would result in updates to the business continuity program and the planning process. Develop change control procedures to monitor changes. Integrate the procedures with any existing change control process.
    2.2.2. Create proper version control. Develop procedures for the re-issue, distribution, and circulation of the plan to the relevant parties.
    2.2.3. Identify plan distribution lists.
    2.2.4. Develop a process to update plans based on the response to audit findings.
    2.2.5. Implement the change control process.
3. Identify appropriate governance.
    3.1. Review the expectations of the organizational parties, which may include regulations, public health guidelines, industry requirements, the internal needs of the entity, service level agreements, and/or other environmental factors. Identify entity-wide processes including a recurring review, enhancement, and continuous improvement process.
    3.2. Identify appropriate governance models based on industry, national, or international standards.
    3.3. Define the frequency and scope of exercises/tests that meet the needs of the entity.
    3.4. Ensure approval by the designated organizational parties.
4. Establish an audit[3] process for the business continuity program.
    4.1. Determine a schedule for conducting a first-party (self-assessment) audit.
    4.2. Prepare to support other audits that may occur, which may include, but are not limited to, internal audit or external audit such as second-party (customer), third-party, or regulatory body/government. Document any audit requirements.
    4.3. Select or develop tools that may be necessary to conduct the audit.
    4.4. 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; plan maintenance; 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.
    4.5. Audit the change control process for the plan documentation and business continuity program.
    4.6. Review response to the audit findings.
    4.7. Confirm that the responses are submitted and that the action plans are documented. Verify that all completed actions are captured in the plan with supporting documentation.
5. Provide written recommendations based on the exercise/test results, including revisions to strategies and plans if desired outcomes cannot be met.
    5.1. Obtain leadership approval to address revisions to strategies and plans as needed. 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 communication methods including reporting level of detail. Consider graphic representations or comparison reports targeted to specific audiences in coordination with the entity communications team. Establish a monitoring process ensuring that appropriate actions have been taken as a result of the reported audit findings. This process should include issues tracking, the party responsible for correcting the issue, the target date for completing the correction, and the dates of opening/closing for the item.

[3] For the purposes of this document, the term audit refers to both audits and assessments.

Professional Practice Nine: Crisis Communications

Objectives

1. Create and maintain a crisis communications plan.
2. 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. Review and update the crisis communications plan on at least an annual basis or more frequently if exercise/test results, regulations or changes to the entity warrant.

Activities

1. Design, develop, and implement a crisis communications plan.
    - 1.1. Review any existing crisis communications plan, identifying and documenting gaps.
    - 1.2. Leverage the results of the risk assessment as outlined in Professional Practice Two: Risk Assessment in order to identify potential incidents for which communications should be planned.
    - 1.3. Define the objectives, scope, and communications plan structure.
    - 1.4. Establish the location, roles, and responsibilities for the crisis communication team.
        - 1.4.1. Identify and document the primary location for the crisis communication team's operations. It may be a physical or virtual location. Identify a secondary site.
        - 1.4.2. Identify the governance structure for developing internal messaging.
        - 1.4.3. Identify the function that will serve as the primary contact for outgoing media communications.
    - 1.5. Identify internal and external interested parties for crisis communications. They may include, but are not limited to, public health contact tracing, employees and their families, investors, customers, vendors and suppliers, outsourced operations, cybersecurity information sharing organizations, 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.
    - 1.6. Develop and document the interested party notification process.
        - 1.6.1. Determine the tone, content, and frequency of communications before, during, and after the incident.
        - 1.6.2. Identify means of communication, which may include, but are not limited to, face-to-face meetings, personal phone calls, home visits, incident notification systems, email and group distribution lists, conference calls, intranet systems, press conferences, incident information lines, media sources (such as print, radio, television), the internet, social media platforms, and blogs/vlogs.
    - 1.7. Establish guidelines to identify the incident and its potential impacts.
    - 1.8. Establish guidelines for the initial communication before, during, and following an incident.
    - 1.9. Identify and assign members to the crisis communications team.
    - 1.10. Obtain leadership approval of the crisis communications plan and notification process.
    - 1.11. Develop guidelines for communications with the incident response team.
    - 1.12. Document sample communications that can be used as templates during an incident.
    - 1.13. Ensure there is an approval process for all outgoing communications.

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, approval and response procedures, as well as the proper tools 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 Professional Practice Eight: Business Continuity Plan Exercise/Test, Assessment, and Maintenance. Ensure that the crisis communications plan is integrated into all exercises/tests.
    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 debrief to determine lessons learned after the exercise/test. Document the corrective action items.
4. Review and update the crisis communications plan on at least an annual basis or more frequently if exercise/test results, regulations or changes to the entity warrant.

Professional Practice Ten: Coordinating with External Agencies and Resources

Objectives

1. Establish policies and procedures to coordinate response activities with applicable public entities and private resources in accordance with Professional Practice Five: Incident Preparedness and Response.

Professional's Role

1. Identify and establish incident response procedures for the entity in accordance with Professional Practice Five: Incident Preparedness and Response.
2. Identify applicable incident preparedness and response guidelines and the agencies having jurisdiction over the entity.
3. Coordinate incident response procedures with external agencies and resources.

Activities

1. Identify and establish incident response procedures for the entity in accordance with Professional Practice Five: Incident Preparedness and Response.
2. Identify applicable incident preparedness and response guidelines and the agencies having jurisdiction over the entity.
   - 2.1. Identify regulatory agencies with jurisdiction over the entity. Agencies may include, but are not limited to, public health, facility officials, fire marshals, law enforcement, regulators, occupational safety and health, and other governmental organizations.
   - 2.2. Identify requirements for the submission of information about the entity's facilities (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.
   - 2.5. Develop or update emergency preparedness and response procedures to comply with laws, regulations, and other government-authorized directives. Coordinate with the entity's compliance and/or legal teams.
   - 2.6. Report prescribed information to regulatory agencies.
   - 2.7. Monitor changes to laws, regulations, and directives. Modify procedures to maintain compliance.
   - 2.8. Obtain leadership approval of incident response procedures with external agencies.
3. Coordinate incident response procedures with external agencies and resources.
   - 3.1. Identify the agency and/or resource(s) that will act as the first responder to the incident.
   - 3.2. Develop and document emergency alerting procedures and requirements (such as mandatory reporting of hazmat, injuries, and other incidents).
   - 3.3. Identify representatives from the first responder agencies/resources and establish liaison relationships with the relevant personnel.
   - 3.4. Invite personnel from first responder agencies/resources 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 business continuity management incidents and scenarios as outlined in Professional Practice Five: Incident Preparedness and Response.
   - 3.6. Coordinate, conduct, and participate in exercises/tests with agencies/resources and first responders to increase awareness and compliance with regulations.
   - 3.7. Debrief following exercises/testing activities. Document exercise/test results, lessons learned, and actions to be taken to improve response capabilities.
   - 3.8. Provide exercise/test results to leadership and other designated organizational functions.
   - 3.9. Update the incident response plans using the lessons learned and feedback from exercises/tests in accordance with the schedule established in Professional Practice Eight: Business Continuity Plan Exercise/Test, Assessment, and Maintenance.