PROFESSIONAL PRACTICES FOR BUSINESS CONTINUITY PLANNERS: RISK EVALUATION AND CONTROL

SUBJECT AREA 2: RISK EVALUATION AND CONTROL

Determine the events and external surroundings that can adversely affect the organization and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

A. The Professional's Role is to:

1. **Identify Potential Risks to the Organization**
    a. Probability
    b. Consequences/Impact
2. **Understand the Function of Risk Reduction/Mitigation Within the Organization**
3. **Identify Outside Expertise Required**
4. **Identify Exposures**
5. **Identify Risk Reduction/Mitigation Alternatives**
6. **Confirm with Management to Determine Acceptable Risk Levels**
7. **Document and Present Findings**

B. The Professional Should Demonstrate a Working Knowledge in the Following Areas:

1. **Understand Loss Potentials**
    a. Identify exposures from both internal and external sources. These should include, but not be limited to, the following:
        (1) Natural, man-made, technological, or political disasters
        (2) Accidental versus intentional
        (3) Internal versus external
        (4) Controllable risks versus those beyond the organization's control
        (5) Events with prior warnings versus those with no prior warnings
    b. Determine the probability of events
        (1) Information sources
        (2) Credibility
    c. Create methods of information gathering
    d. Develop a suitable method to evaluate probability versus severity
    e. Establish ongoing support of evaluation process
    f. Identify relevant regulatory and/or legislative issues
    g. Establish cost benefit analysis to be associated with the identified loss potential

2. Determine the Organization's Exposures to Loss Potentials

a. Identify primary exposures the organization may face, and secondary/collateral events that could materialize because of such exposures (e.g., hurricane threat could result in several events including high winds, flood, fire, building and roof collapse, etc.)

b. Select exposures most likely to occur and with greatest impact

3. Identify Controls and Safeguards to Prevent and/or Mitigate the Effect of the Loss Potential

Considerations: The actions taken to reduce the probability of occurrence of incidents that would impair the ability to conduct business.

a. Physical protection
   (1) Understand the need to restrict access to buildings, rooms, and other enclosures where circumstances demand a "3-dimensional" consideration
   (2) Understand the need for barriers and strengthened structures to determine willful and accidental and/or unauthorized entry
   (3) Location: physical construction, geographic location, corporate neighbors, facilities infrastructure, community infrastructure

b. Physical presence
   (1) Understand the need for the use of specialist personnel to conduct checks at key entry points
   (2) Understand the need for manned and/or recorded surveillance equipment to control access points and areas of exclusion; including detection, notification, suppression
   (3) Understand security and access controls, tenant insurance, leasehold agreements

c. Logical protection
   (1) Understand the need for system-provided protection of data stored, in process, or in translation; information backup and protection
   (2) Understand detection, notification, suppression
   (3) Understand information security: hardware, software, data, network

d. Location of assets
   (1) Understand the inherent protection afforded key assets by virtue of their location relative to sources of risk
   (2) Personnel procedures
   (3) Preventive maintenance and service as required
   (4) Utilities: duplication of utilities, built-in redundancies (telco, power, water, etc.)
   (5) Interface with outside agencies (vendors, suppliers, outsourcers, etc.)

4. Evaluate, Select, and Use Appropriate Risk Analysis Methodologies and Tools

a. Identify alternative risk analysis methodologies and tools
   (1) Qualitative and quantitative methodologies
   (2) Advantages and disadvantages
   (3) Reliability/confidence factor
   (4) Basis of mathematical formulas used

b. Select appropriate methodology and tool(s) for company-wide implementation

5. Identify and Implement Information-Gathering Activities

a. Develop a strategy consistent with business issues and organizational policy

b. Develop a strategy that can be managed across business divisions and organizational locations

c. Create organization-wide methods of information collection and distribution
   (1) Forms and questionnaires
   (2) Interviews
   (3) Meetings
   (4) Documentation review
   (5) Analysis

6. Evaluate the Effectiveness of Controls and Safeguards

a. Develop communications flow with other internal departments/divisions and external service providers

b. Establish business continuity service level agreements for both supplier and customer organizations and groups within and external to the organization

c. Develop preventive and pre-planning options
   (1) Cost/benefit
   (2) Implementation priorities, procedures, and control
   (3) Testing
   (4) Audit functions and responsibilities

d. Understand options for risk management and selection of appropriate or cost-effective response, i.e., risk avoidance, transfer, or acceptance of risk

7. Risk Evaluation and Control

a. Establish disaster scenarios based on risks to which the organization is exposed. The disaster scenarios should be based on these type of criteria: severe in magnitude, occurring at the worst possible time, resulting in severe impairment to the organization's ability to conduct business.

b. Evaluate risks and classify them according to relevant criteria, including: risks under the organization's control, risks beyond the organization's control, exposures with prior warnings (such as tornadoes and hurricanes), and exposures with no prior warnings (such as earthquakes).

c. Evaluate impact of risks and exposures on those factors essential for conducting business operations: availability of personnel, availability of information technology, availability of communications technology, status of infrastructure (including transportation), etc.

d. Evaluate controls and recommend changes, if necessary, to reduce impact due to risks and exposures
   (1) Controls to inhibit impact exposures: preventive controls (such as passwords, smoke detectors, and firewalls)
   (2) Controls to compensate for impact of exposures: reactive controls (such as hot sites)

8. Security

a. Identify the organization's possible security exposures, including the following specific categories of security risks
   (1) Physical security of all premises
   (2) Information security—computer room and media storage area security
   (3) Communications security—voice and data communications security
   (4) Network security—intranet security, Internet security
   (5) Personnel security

b. Advise on feasible, cost-effective security measures required to prevent/reduce security-related risks and exposures

9. Vital Records Management

a. Identify vital record needs in the organization, including paper and electronic records

b. Evaluate existing backup and restoration procedures for vital records

c. Advise on and implement feasible, cost-effective backup and restoration procedures for all forms of the organization's vital records