SUBJECT AREA 2 - RISK EVALUATION and CONTROL

Determine the risks (events or surroundings) that can adversely affect the organization and its resources (example(s) include: people, facilities, technologies) due to business interruption; the potential loss of such events can cause and the controls needed to avoid or mitigate the effects of those risks. As an outcome of the above, a cost benefit analysis will be required to justify the investment in controls.

A. THE PROFESSIONAL'S ROLE IS TO:

A. 1 Obtain Information about the Organization's Risk Tolerance from Management

A. 2 Identify and Implement Information Gathering Activities

A. 3 Identify Potential Exposures/Risks to the Organization based on Risk Category

A. 4 Qualify and Prioritise the Exposures Identified

A. 5 Identify Controls and Safeguards to Avoid and Mitigate the Effect of the Loss Potential

A. 6 Evaluate the Effectiveness of Controls and Safeguards

A. 7 Document and Present Risk Assessment to Senior Management for Approval

B. THE PROFESSIONAL SHOULD DEMONSTRATE A WORKING KNOWLEDGE IN THE FOLLOWING AREAS:

B. 1 Obtain Information about the Organization's Risk Tolerance from Management

B.1.a. Interview the Organization's Legal Counsel and other pertinent areas (such as Financial Officer, Operations Officer, Risk Officer, etc…) to identify the relevant risk related issues

B.1.b. Work with management to select an appropriate cost benefit analysis model

B.1.c Establish the measurement criteria necessary to quantify risk tolerance

B. 2 Identify and Implement Information Gathering Activities

B.2.a. Determine methods of information gathering

(i) Determine information sources

(ii) Determine the credibility of the information sources

B.2.b. Develop a strategy to gather information consistent with business issues and organizational policies.

B.2.c. Develop a strategy to gather information that can be managed across business divisions and organizational locations

B.2.d. Create organization-wide methods of information collection and distribution

(i) Forms and questionnaires

(ii) Interviews

(iii) Meetings

(iv) Documentation review

(v) Analysis

B. 3 Identify Potential Exposures/Risks to the Organization Based on Risk Categories

B.3.a. Identify the categories of risk associated with a risk analysis process. Risk categories include, but are not limited to:

(i) Facility Risk

(ii) Security Risks (both physical and data integrity)

(iii) Reputation

(iv) Procedural

(v) Information Technology (including operational infrastructure)

(vi) People

(vii) Supply Chain (including outsourcing)

(viii) Compliance

B.3.b. Identify exposures from both internal and external sources. Internal and External sources include, but are not limited to:

(i) Natural, man-made, or technological

(ii) Accidental versus intentional

(iii) Internal versus external

(iv) Controllable exposures/risks versus those beyond the organization's control

(v) Events with prior warnings versus those with no prior warnings

B. 4 Qualify and Prioritize the Exposures Identified

B.4.a. Develop a quantifiable method to evaluate exposures/risks in terms of probability and severity

B.4.b. Identify alternative risk analysis methodologies and tools

(i) Qualitative and quantitative methodologies

(ii) Advantages and disadvantages

(iii) Reliability/confidence factors

(iv) Basis of mathematical formulas used

B.4.c. Select appropriate methodology and tool(s) for company-wide implementation

B.4.d. Evaluate risks and classifies them according to relevant criteria including, but not limited to:

(i) Risks under the organization's control

(ii) Risks beyond the organization's control

(iii) Exposures with prior warnings (such as tornadoes and hurricanes)

(iv) Exposures with no prior warnings (such as earthquakes)

B.4.e. Evaluate impact of risks and exposures on those factors essential for conducting business operations:

(i) Availability of personnel

(ii) Availability of information technology

(iii) Availability of communications technology

(iv) Status of infrastructure (including transportation), etc…

B. 5 Identify Controls and Safeguards to Avoid and Mitigate the Effect of the Loss Potential

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

B.5.a. Physical protection

(i) Identify requirements necessary to restrict access at all pertinent levels (e.g., building, room, etc.)

(ii) Investigate the need for barriers and strengthened structures to determine wilful and accidental and/or unauthorized entry

(iii) Location: physical construction, geographic location, corporate neighbors', facilities infrastructure, community infrastructure

(iv) Identify the need for the use of specialist personnel to conduct checks at key entry points

(v) Evaluate the need for manned and/or recorded surveillance equipment to control access points and areas of exclusion; including detection, notification, suppression (e.g., sensors, alarms, sprinklers)

(vi) Review security and access controls, tenant insurance, leasehold agreements

B.5.b. Logical protection

(i) Assess the need for system-provided protection of data stored, in process, or in translation; information backup and protection

(ii) Evaluate information security: hardware, software, data, and network monitoring (e.g., detection, notification, etc.)

B.5.c. Location of assets

(i) Evaluate the inherent protection afforded key assets by virtue of their location relative to sources of risk.

(ii) Personnel procedures

(iii) Preventive maintenance and service as required

(iv) Utilities: duplication of utilities, built in redundancies (telco, power, water, etc.)

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

B.5.d. Identify the organization's possible security exposures and risks, including but not limited to:

(i) Physical security of all assets (premises, equipment, etc.)

(ii) Information security - computer room and media storage area security

(iii) Communications security - voice and data communications security

(iv) Network security - intranet security, Internet security

(v) Personnel security

B.5.e. Develop preventive and pre-planning options

(i) Cost/benefit

(ii) Implementation priorities, procedures, and control

(iii) Testing

(iv) Audit functions and responsibilities

(v) Understand options for risk management and selection of appropriate or cost-effective responses (examples include: risk avoidance, transfer, or acceptance of risk).

B. 6 Evaluate the Effectiveness of Controls and Safeguards

B.6.a. Evaluate security-related communications flow with other internal areas and external service providers.

B.6.b. Evaluate business continuity service level agreements for both supplier and customer organizations and groups within and external to the organization.

B.6.c. Evaluate controls and recommends changes, if necessary, to reduce impact due to risks and exposures

(i) Controls to inhibit impact exposures: preventive controls (such as passwords, smoke detectors, and firewalls)

(ii) Controls to compensate for impact of exposures: reactive controls (such as hot sites)

B.6.d. Establish disaster scenarios based on risks to which the organization is exposed. The disaster scenarios should be based on situations severe in magnitude, occurring at the worst possible time, resulting in severe impairment to the organization's ability to conduct business.

B.6.e. Advise on feasible, cost-effective security measures required to prevent/reduce security-related risks and exposures

B.6.f. Establish ongoing support of evaluation process

B. 7 Document and Present Risk Assessment to Senior Management for Approval

B.7.a. Prepare risk assessment report

B.7.b. Present findings of risk assessment

(i) Controls satisfactory

(ii) Recommend new controls

(iii) Recommend control improvements

(iv) Consider appropriate areas to transfer risk

(v) Document areas that management accepts risk

B.7.c. Determine next steps to begin the development of Business Continuity strategies

(i) Consider impacts from BIA

(ii) Consider risks and exposures from risk analysis