Developing a Business Risk Management Programme

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Discuss the basic steps involved in creating Enterprise Risk Management Programme
- ✓ Explain the importance of a contingency plan for a business and its main objectives
- ✓ Determine the scope of business impact analysis.

Developing a Business Risk Management Programme

Introduction

Establishing and managing a successful Business Risk Management Programme has no shortcuts. There are only trade-offs concerning levels of risk and resource requirements. Despite the fact that the process of formulating risk management strategies and business continuity/contingency plans can be expensive, lengthy, and very time-consuming, it can make the difference between not surviving a risk-related event or getting through with most things intact. One benefit of this process is that information will be uncovered which can also lead to everyday operational enhancements within the business itself and also with its business partners.

When faced with the huge task of starting a risk management programme in the company, it is best to break the complex tasks into smaller manageable portions.

The following stages form the basic steps for designing a company-wide Risk Management Programme:

- ✓ Risk analysis and assessment;
- ✓ Business continuity and contingency planning;
- ✓ Response and resumption;
- ✓ Business recovery; and
- ✓ Review and re-evaluation

However, these must be broken down further into components or parts in order to actually start working on these activities. Thus, an expanded Risk Management Programme structure would work in the following manner:

- ✓ Programme inception and justification;
- ✓ Programme initiation and management selection;
- ✓ Risk analysis and assessment:
- ✓ Risk identification and awareness
- ✓ Risk analysis or measurement – also known as business impact analyses
- ✓ Risk control or mitigation
- ✓ Legal review

- Business continuity and contingency planning -;
  - ✓ Plan recovery strategies
  - ✓ Contingency plan development
  - ✓ Training and communication programmes
  - ✓ Plan testing
  - ✓ Review and revision, as required
  - ✓ Plan approval

- ✓ Final plan distribution
- ✓ Plan maintenance
- Response and resumption;
- Business recovery; and
- Review and re-evaluation

Programme Vision and Rationalisation

A comprehensive and effective Risk Management Programme cannot be created in just a few weeks. A substantial amount of time, effort and resources will be needed to create a programme that deals with the needs of the entire company. Therefore, absolute support of the company's executive management is required, without which the tasks that are necessary to create the programme will not enjoy top priority, funding or attention. This is especially true if the risk management philosophy is being presented to a company for the first time. An endorsement of the level of effort that will be needed and the purpose of the exercise must come from the executive management or board of directors. Creating an awareness of the need for risk management and its benefits can be addressed in the following ways:

- By emphasising possible risks to the company and by making comparisons to other companies that have suffered severe business disruption and successfully managed the crisis event;
- By pointing out the use of risk management by similar organisations, especially competitors in the same industry; and
- By explaining possible impacts to the company in respect of key performance indicators, such as market share, customer service levels, costs, staff turnover and profitability.

The first step that can be taken to justify the importance of the programme might be to run a high-level impact assessment project. A project like this will vary in length depending on the size of the company and the amount of staff allocated to it. In an ideal world, a high-level impact assessment should take about a month to complete and comprises the following tasks:

- Ascertain the mission-critical operations for the organisation and identify the potential risks;
- Prioritise these mission critical operations ;
- Launch a high-level analysis that exposes the severity of the impact on the business if key operations are lost;
- Detect areas of vulnerability which are easily recognised, like the use of single-source suppliers or dated technology infrastructure; and
- Present a comprehensive report to executive management that describes the structure and process flows of the company at a high level, identifies serious areas of risk exposure and possible management liability and evaluates the scope and cost of continuing with risk mitigation and contingency planning.

Once the programme has received approval from executive management, the actual programme initiation and management selection tasks can be launched.

Programme Initiation and Management Selection

Executive management should commence the formal risk management programme once the high-level risk assessment project is complete or as soon as it is realistically possible. The following activities provide an outline of the steps necessary to establish and operate a successful risk management programme:

- Select or hire an executive-level or senior management leader (the CRO);
- Establish a company risk management team made up of applicable stake holders;
- Let all staff know about the risk management programme and its purpose;
- Conduct a company-wide inventory of business operations and a high-level impact assessment only if it was not done as a first step, as described previously;
- Develop a company-wide inventory of essential elements that support critical operations;
- Have risk assessment interviews with key staff members from each functional area;
- Conduct a legal review and evaluation;
- Collect, save, and evaluate risk data and report the results;
- Plan, create, and budget for risk prevention measures and event detection processes;
- Evaluate, train for, and implement preventative measures and processes;
- Create contingency plans for risks that cannot be adequately prevented;
- Review, test, train for, and revise contingency plans;
- Accept and distribute final contingency plans;
- Observe results of preventive measures and adapt new processes as required;
- Establish early warning and detection systems; and
- Develop and communicate the programme.

A company-wide risk management team must be created to monitor and guide the programme. This team is responsible for handling potential problems and reduce or eliminate operational failures and income or profit reduction. Enterprise staff that should be recruited as essential members of this team are those with business expertise and skills in the following areas: corporate communications, staff training, project management, business analysis, legal and contract administration, strategic and tactical planning, and financial management and information technology.

All staff members need to be made aware of the programme being introduced and be given an overview of the issues and risks the company intends to address. They must be informed about the contact person in the risk management programme, of the business implications of the identified risks and the plan to deal with these risks. Initial employee information should include how the project is expected to proceed and a description of the resources being focused on the risk management programme.

Continual communication in respect of the status of the project is just as important as the initial awareness communications. On-going awareness can be achieved in many ways like: including a risk management programme column in the company's internal newsletter, designing a risk management newsletter, publishing progress information on the organisation's intranet and distributing e-mails from the programme's management team on a regular basis.

Risk Identification and Assessment

The next step in the risk management programme is to define a strategy and set guidelines for conducting an enterprise-wide inventory of important operations and vital elements that support those operations. This step establishes the overall objectives of the risk exposures on which the company intends to focus.

Risks faced by an organisation tend to originate from three sources:

- The organisation's mission, structure, and culture;
- The assets and resources owned or controlled by the organisation; and
- The company's business partners.

A high-level business impact assessment should be conducted as a first step, prior to the formal risk management programme, if it wasn't done previously. As mentioned above, the purpose of this high-level impact assessment is to identify and prioritise mission-critical operations and their associated risks. If a complete and current contingency plan, namely disaster recovery, business continuity and business resumption is in place, it should have a list of mission-critical operations.

A business impact assessment can be done if a contingency plan does not already exist by ensuring that the following is in place:

- All business operations are identified –including those within the company itself and also business functions that link the company to or interact with external trading partners;
- A questionnaire is designed that will help identify and prioritise mission-critical operations ;
- Meetings with enterprise management for completing the critical business operation questionnaires;
- Questionnaire responses are collected and tabulated; and
- A prioritised list of mission-critical operations based upon tabulated questionnaire responses is available.

An inventory of essential elements that provide direct or indirect support must be conducted for each of the identified operations.

Usually, an inventory of essential elements is needed to facilitate an effective risk assessment in the following categories:

- The organisational structure;

- Enterprise-based performance measurements;
- Office equipment and facilities;
- Telecommunications systems;
- Computer software and equipment;
- Network connectivity within the company and to external environments;
- Architectures, designs and configuration management information in respect of all applications, systems, and networks, which are used in the company;
- Investments, insurance, contracts, and agreements; and
- All business partner relationships including suppliers, vendors, customers, or other third-party organisations that provide products or services

The level of inventory detail that must be collected for each identified risk will be dictated by the previously established inventory strategy.

There are several approaches to collecting the inventory data, including:

- Performing a thorough and detailed-level (micro) inventory;
- Executing only a high-level or macro inventory; and
- Carrying out a combination of both a high-level and where required, a detail-level inventory.

If time and financial constraints are an issue, one way to achieve the essential elements inventory could be to conduct a high-level inventory and then, to proceed with a risk assessment based on summarised inventory data. This approach has the advantage that allows a quick inventory collection to be done that can then be used to begin the risk assessment process. However, it has the disadvantage of introducing the risk of overlooking critical operations, functions or essential elements, creating an incomplete baseline from which to conduct a risk assessment. The company needs to weigh the advantages and disadvantages of each inventory approach. The inventory approach chosen must provide essential data to enable the more specific identification of potential risks to mission-critical operations. At the end of this process, the results of the inventory will help establish the extent of the risk management programme, the overall strategy of the programme and its impact on the organisation.

Determining Mission-Critical Operations

A strategy for quickly identifying areas that would suffer operational, financial, legal and/or regulatory loss in the event of an interruption is through a business impact analysis. Management should rate the impact that an interruption in an operation would have on the critical success factors for the organisation by using the severity of impact of an operation's interruption as the main rating factor.

These critical success factors include, but are not limited to the following:

- Internal controls – Would the organisation's internal controls, measurements, and reporting be threatened by an adverse incident?

- Safety and security – Would the safety and security of the employees or the physical assets of the organisation be in danger?
- Communications – Would the company's communication abilities, such as electronic data interchange with its business partners be interrupted?
- Revenue generation – Would the company's ability to service its customers and generate revenue be disrupted by the event?
- Reputation – Would the organisation's image or brand be damaged due to the risk event or other supplementary effects?
- Legal – Would the business be violating any regulatory requirements or contractual agreements?
- External reporting – Would the incident prevent the organisation from generating external reports, such as financial statements, tax returns, etc?

All of these aspects must be listed and examined for each of the operations or business functions listed. Help may be needed from a company's trading partners or affiliated businesses to create an inventory of critical success factors for the processes that extend beyond the immediate enterprise.

The next step is to identify the impact that an incident would have on a specific business function, and prepare an estimate of the loss that will be felt for the duration of an expected disruption. This process will need additional input from business unit managers and members of the risk management team who facilitate this process.

The next stage in business impact analysis is to prioritise the list of business functions to identify what is truly *mission-critical* for the business. For each of the functions identified, the following classifications indicating a recommended recovery timeframe should be attached:

1. *Highest category of availability*: This means that immediate resumption of business functions is essential. No downtime of this function or business process can be permitted. Generally, this will require a fully equipped and staffed alternative site to be in place and available 24/7;
2. *Short period of downtime can be tolerated*. Four hours or less downtime is acceptable for these functions, but work must be resumed within four hours. Once again, an alternative site must be available which can be staffed and functional within a four-hour timeframe;
3. *Resumption of function is required the same day, but a specialised alternate site is not required*. Business functions can continue in any type of alternative location, such as an employee's home or a borrowed office;
4. *24 hours of downtime is acceptable for this business function;*
5. *24–72 hours allowed for business to resume for this function; and*
6. *More than 72 hours is acceptable for resumption of the business function*.

All internal and external dependencies must be taken into account and documented when creating the list of business functions and resumption criteria.

Assessing and Analysing the Risks

After identifying and prioritising mission-critical operations and collecting an inventory of essential elements that support those operations, the risk management team can continue with the next step of the project. Practical alternatives and guidelines must now be defined that will be used to assess, quantify and evaluate risk; gather risk assessment information and store accumulated risk assessment data in a manner that allows risk analysis and reporting to be performed. Conducting a risk assessment of the possible risks to which the company is exposed is central to the contingency planning process. The types of disasters can vary based upon several factors, including but not limited to:

- The past performance level of local utility companies in providing continuous services;
- The history of the area's exposure to natural disasters;
- The company's geographic location; and
- The amount of physical accessibility to the organisation.

Risk Evaluation Criteria

Risk Measurement Criteria should be identified in order to select an appropriate approach that can be used to assess risks involved. There are five main factors used to evaluate the probability and severity of the failure of a company's operation or essential supporting elements, the organisation's exposure, timing, and the volatility of the event's occurrence.

Rating the chance of a performance failure helps to highlight potential failures that pose real or highly likely dangers to the business. This separate and distinctive rating step helps to focus mitigation and contingency planning energy on appropriate high probability risk areas. Some risks occur quite frequently but are low in severity, while other risks rarely occur but may be severe. Gathering failure frequency data from staff, vendors or suppliers responsible for an essential element can help ascertain relatively accurate failure probability estimates for most aspects under their area of concern. In the same way, getting the severity and frequency of natural disasters for a given geographic location from subject matter experts will provide forecasts for these types of occurrences. The severity factor answers the question '*how bad can it get?*' The higher the severity, the greater the risk is to the company.

The following factors should be considered when rating the possible severity of impact of a performance failure:

- Failure tolerance is an indication of the maximum acceptable length of time for the loss of an essential element or operation. In other words, how long after a failure occurs will customer service feel the impact? Put another way, how often during a specified length of time (for example, one month) is an essential element used in support of a business operation?
- The impairment level of the failure, which is the maximum impact that will be felt due to the failure if it is not resolved speedily.

- The time horizon from failure to full impairment, which is the time difference (if there is one) between the failure event itself and the full impact of its effects. For instance, a failure of the general ledger system may ultimately cause severe impairment to a company's ability to produce financial statements, but the full effect of the loss may only be felt during the month end runs. Other circumstances may intensify the time horizon. If a production line fails, the failure may be recovered from before there are any significant impacts to the organisation if, for example, there is a three months' sales worth stock currently in inventory. Generally though, the longer the duration of the exposure, the higher the risk.
- A contingency plan should reduce the ultimate impact experienced through performance failure.

In order to assign a severity impact to the interruption of an operation or an essential element failure, a precise and easily understood rating scale is needed, for example:

A = Total impairment

B = Considerable impact

C = Moderate impact

D = Minor impact

E = Negligible impact on the company or supported operation

Assigning severity ratings to operations and essential elements provides the raw data required to conduct a performance failure impact analysis. Severity impact ratings frequently provide sufficient information for management to make informed choices regarding mitigation and contingency strategies. The effect of an operation or element's failure provides a clear indication of that operation or element's importance to the business. The prospect of a failure actually arising should not alter the importance of the specific operation or element to the company. Therefore, a rating model based upon severity of impact produces a candid means to establish a prioritised list of mission-critical operations and essential supporting elements.

The organisation's exposure implies the maximum amount of damage that will be experienced from a risk event. Simply stated, in the absence of other factors, the risk to the company associated with a specific event increases as its exposure increases. The exposure factor can be reduced by transferring the risk to an external party such as an insurer, or it can be managed by allocating additional capital to cover it.

The volatility of an event describes the variations of circumstances that dictate the potential outcome of the risk. This is an important aspect of the risk as it dictates that the more volatility that is present, as in some market conditions, the higher the corresponding risk. For instance, investment in derivatives is an extremely risky venture because their underlying market conditions are volatile, particularly in illiquid markets.

Developing a Risk Survey

When a risk assessment approach has been selected, it is used to guide the formation and use of an appropriate assessment survey tool. A set of comprehensive and business-unit-specific questions is developed for use during the series of risk assessment interviews that are held with key staff from each functional area of the business. These interviews help to identify and quantify risks related to the potential for failure of an essential element, offer insight about the dependencies between mission-critical operations, and supporting essential elements and provide information on which to base mitigation and contingency planning activities.

Identifying unfavourable and beneficial events is very important to uncover the full spectrum of potential risks. Whether the organisation is considering possible effects of the death of a key executive in the organisation or better interest rates than forecasted, this is the time to brainstorm about worst-cases scenarios, including events that may not be immediately obvious.

Organisations may not realise the full extent of their liability exposure. For example, a company in the chemical industry may fully understand its liability at manufacturing plants, but the impact of lesser pipeline failures or a problem with shipping products it is not so obvious. If a chemical producer stores a product for which it is liable at a railhead and there is a spill or chemical release, what happens? While it is easy to consider the big, obvious issues, the complications lie, as always, in the unique and smaller details.

A checklist of questions is a good way to stimulate thinking when drawing up a comprehensive survey to address the large and the small issues that may impact the company. For example:

Functional Area Questions to Consider

Business Operation

Production	What factors might interrupt the production of goods and services?
Distribution	What factors might interrupt activities with existing channels, such as suppliers, wholesalers, retailers and the Internet?
Customer service	What factors could disrupt relationships with purchasers of goods and services?
Post-sales service	What factors could interrupt servicing after the sale is made?
Changing markets	What factors could prove costly as a result of changes in consumer demand?
Changing technology	What factors could prove costly as a result of changes in technology?
Legal or government	What factors could interrupt activities or be costly as a result of existing or new laws and regulations?
Business liability	
Product	What hazards exist because products are used or misused or might be

	potentially defective?
Environment	What hazards could prove costly because of pollution or other accidents?
Facilities	What hazards exist because of physical facilities or operations?
Employees	What risks exist from current or former workers?
Trading partners	What hazards exist from buyers or suppliers of goods or services?
Third parties	What hazards exist from unrelated parties?
Risks to physical or intellectual assets	
Catastrophes	What hazards exist from floods, earthquakes and similar occurrences?
Governmental	What hazards could prove costly as a result of governmental actions?
Computer systems	What hazards could disrupt telecommunications systems?
Property exposures	What hazards exist from fire, explosion, utility failures and similar occurrences?
Functional area	**Questions to consider**
Financial considerations	
Fixed assets productive	What factors could interrupt sources of long-term debt and equity funds to finance assets?
Working capital	What factors could interrupt sources of liquid assets and short term debt?

Some general questions that may be asked when discussing various points can include:

- If the demand for the product is higher than expected in forecasted plans, how should the increased demand be met?
- What actions should our company take to reduce the effects caused by the occurrence of certain man-made or natural disasters, like the loss of patent protection, a hostile takeover attempt, loss of computer capabilities or the destruction of manufacturing facilities due to earthquakes, tornadoes, or hurricanes?
- If forecasted sales objectives are not reached, how can profit losses be avoided?
- If a major competitor withdraws from a particular market, what should the business do to deal with the potential void?
- What actions should be taken if a technological advancement or emerging market condition makes our new product obsolete sooner than the business thought it would?

Risk Control and Alleviation

Now that the mission-critical operations and essential supporting elements of the business have been identified and prioritised according to their importance and criticality to the overall success of the company, this information can be used to create risk mitigation plans.

Various methods, or *fixes*, can be used during mitigation planning that address risk issues. *Fix* methods must be clearly defined and then assigned to each essential element being subjected to this planning process. These fix methods include but are not limited to:

- Quick fixes – adjustments or corrections of an essential element that requires much less time than other potential solutions;
- Partial replacement – generally applied to a system: replacing an unreliable or non-working part or function in a system with a working part or function.
- Full redundancy or replacement – involves two approaches: full redundancy refers to having a working part or function available for use if the existing part or function fails. Full replacement means the complete replacement of a failed or defective system or essential element with a functioning one;
- Hire and train additional staff – a manual alternative to the above methods whereby all or part of a failed or defective automated process is replaced; and
- Outsourcing – using a third-party organisation to correct failures or defects of a given essential element.

A plan outline to be used for individual mission-critical operations, and which, with all operations considered together, forms the enterprise risk mitigation plan, must be established and be based upon the strategy and project scope decisions established when the business rules guidelines were adopted at the beginning of the mitigation planning process. At this point, it is necessary to estimate, justify, and formally allocate the budget needed to execute the plans in order to avoid delays in implementing the newly developed mitigation plans. The budget must at least include the funds required to purchase computer equipment and software, pay vendors for services and fund new facilities or infrastructure or any other expenses that will be incurred during the process of implementing the mitigation plans. This budget is then dedicated to mitigation plan implementation activities.

Testing and Implementing Preventive Measures

A crucial part of having a Risk Management Programme is the test planning and testing of risk mitigation plans. Official acceptance testing guarantees the functional viability of each plan. Test planning is important to the critical path of this part of the project because of the scalable nature of testing. The formal test plan for each mitigation plan is unique and specific to a corporate function or group of related functions. The quality assurance process must be comprehensive because of the sheer size of this project. Testing and quality assurance issues must be addressed to see if any changes are required to the company's Quality Assurance Programme.

The following questions address some of the quality assurance issues that must first be answered:

- How are baseline test standards selected?
- Where and what test results will be saved for future appraisals?
- What kinds of tests are required?
- What are acceptable test results?
- How and where is the test environment to be established?
- If a separate test environment cannot be established, what are the risks associated with unintentional harm to the production environment?
- What are the differences between the test and production environments?
- Who is responsible for conducting the tests and storing the results?
- Who will create test scripts and documents?
- Is there a standard database for system-wide testing?

Before Risk Mitigation Plans are implemented, it is essential to implement staff training about new processes and procedures. The amount of training required varies widely and depends upon the extent of operational changes to be made to accommodate the mitigation plans. This may be challenging for many, but particularly long-term employees, because changing old habits can be very difficult.

A *training needs assessment* must be carried out to answer questions about the specific training that will be required and who needs to be trained.

Conducting legal reviews

A review and evaluation from a legal perspective of liability related to an interruption of mission-critical operations is an important part of the Risk Management Programme. It involves a detailed review of all contracts, agreements, documented performance standards and management liability to shareholders. This includes revising all contractual relationships with third parties, including but not limited to, customers, suppliers, and vendors and identifying obligations related to maintenance or other outsourced services being supplied to the company.

Special attention should be paid to the following conditions when creating the legal risk strategy:

- Areas where the effect of an interruption to operations far outweighs the remedies available;
- The possibility of such a problem occurring seems likely; and
- Recovering from the potential problem is difficult and expensive for the business.

Other recommendations include, but are not limited to, the following:

- Risk Management Programme activities that are required for regulatory compliance should be implemented;
- Operational and procedural changes necessary to avoid injury and improve safety risks should be implemented;

- An outline of the policies and procedures related to business partner management should be prepared;
- Current legal activities required to support the risk management programme should be conducted;
- Required changes in the insurance coverage should be made; and
- Financial practices essential for compliance with reporting and disclosure guideline should be implemented.

Developing Contingency Plans

The company must be prepared for a worst-case scenario even if the best risk-avoidance efforts have been implemented. For example, if multiple serious incidents occur across organizational and geographical boundaries, accompanied with disruptions to communication and power supply, the company needs a means to collect, filter, prioritise and escalate issues up the appropriate management ladder. Operational reliability and stability must be sustained to ensure the company survives. This is the main objective of contingency planning. Therefore, a comprehensive contingency plan must include the following goals:

- Ensure that potential harm to the company employees and visitors are reduced or completely eliminated;
- Reduce damage to or loss of company assets;
- Make sure that important resources will be available to ensure that business can continue to meet customer needs during an interruption;
- Ensure that an alternative processing location for the restoration of mission-critical operations can be setup speedily;
- Be cost-effective;
- Reduce the need for decision making during a disastrous situation; and
- Provide a standard for testing and updating the contingency plan.

Before launching the contingency planning task, the Risk Management team should collect and analyse any existing records on organisational processes and capabilities which the company may already possess that address issues surrounding worst-case scenarios. It might not be necessary to rewrite the existing plans merely to conform to new formats. However, the plans and the processes used to develop them, must be evaluated to ensure that they are suitable for contingency planning purposes and leveraged to the greatest extent possible. Using these existing plans and processes should minimise the effort needed to develop an overall company contingency plan, and it could encourage re-using the procedures employed to develop those plans.

Developing Recovery Strategies

After the essential and critical business functions have been identified and their effects on the organisation during the course of an interruption have been evaluated, the next step is to identify the resources required to continue to perform these necessary business functions.

These generally fall into one of the following categories:

- Operations – including staffing and supplemental staffing if required. Functions affecting direct customer service are normally given a high priority within this category;
- Key business partners – including suppliers, vendors, or other third-party organisations providing important products or services to the business;
- Facilities – including an inventory of items and fixed assets needed to resume essential functions, development of a facility recovery plan and identification of alternative physical work environments;
- Information systems – including duplication of all vital computing equipment, the required operating environment and data recovered from off-site storage. This category also includes the requirements for distributed processing capability if that is a support resource to an essential function; and
- Telecommunications – including resumption of voice and data communications.

Consider a range of available solutions to deal with the failure of an operation, process or essential element when planning for operational contingency:

- Using retired employees to provide supplementary staffing resources;
- Invest in cellular or satellite telephones for emergency communications;
- Stockpile additional supplies from a key supplier;
- Arrange for space to store additional supplies/raw materials;
- Arrange for supplies to deliver via an alternative mode of transportation; and
- Revert to old manual procedures for currently automated processes.

Regardless of the other conditions for which the business function resumption procedures account, they must *always* consider the following two major scenarios:

1. The facilities or services, on which the business functions usually depends upon, are not available and critical business functions must continue without them. These can include electricity, water, and manufacturing materials, etc.
2. The building and its contents in which the function usually takes place are not accessible and recovery may need to happen at an alternative site.

Investigate all available options for meeting the goal of resuming business operations within the mandated timeframe. Develop cost estimates and compare them against the potential costs to the business resulting from a resumption failure.

Business function resumption options include:

- Transfer work activities from the affected site to another within the organisation that has appropriate facilities;
- Alternatives are conference rooms, training rooms, or cafeterias that can be equipped temporarily to support business functions;
- Dedicated alternative sites, built and equipped by the company, may be used to resume business functions; and
- Reciprocal agreements with other business units to accommodate the disrupted functions. This may involve halting non-critical functions within the company that have not been affected by the incident, until full recovery of the disrupted function has been achieved.

Identify critical staff resources that are required to respond to a disaster. Develop an organisational chart depicting the command and control structure of a crisis management team and its relationship to the company's actual organisational structure. Identify the members of the crisis management team and their roles and responsibilities by establishing standard operating guidelines for each team. This ensures that the company has a command and control structure in place that will be able to respond to an event successfully, thus reducing the impact on critical operations.

Documenting the Plan

Document the business resumption strategies that have been identified and agreed on, and develop the final contingency plan.

The plan should include the following aspects:

- The preliminary introduction that includes the reason and purpose for the plan, the scope of the plan, people involved, and the range of events that are covered;
- A definition of the crisis management structure, providing an appropriate organisational chart along with roles and responsibilities of the team members;
- Policies and procedures to be activated when a crisis occurs. These include detection and notification processes, site damage evaluation procedures, alternative site notification policies, and the procedures for retrieval of off-site records or materials, etc.;
- Information and procedures for establishing and activating the emergency operations centre, including location information;
- Emergency notification lists for each business unit. These should contain phone numbers, cell phone or pager numbers, and home phone numbers, etc. for each team member identified as a participant in the business resumption team, as defined later in this section;

- Contact information for internal and external vendors, key customers and other commonly used numbers that may be required during an emergency, such as local or national government agencies, building or facilities security agencies, off-site storage vendors, insurance agents, etc.; and
- Information about any events requiring specialised personnel or equipment for site damage assessment or hazardous material containment, including copies of any contracts for services or pre-event agreements.

Each plan must have fully documented procedures for handling an incident that results in the activation of the plan.

When the plan has been drafted, the ERM process continues with creating a communications and training programme designed to educate the employees about the plan and how to use it. This also prepares the company for the important testing phase, which will then provide input for any plan revisions.

To conclude, we can see that dealing with business risk is a huge challenge for every company. Given the complexity of today's business relationships and the possibility that failures may occur, a risk management programme will enable a company to deal with risks effectively, even though no one can really predict the most adverse events that could cause business interruption. Therefore, an effective risk management programme is critical for a company's overall success. The essential ingredients of assessment, awareness, identification, crisis response, mitigation, and contingency planning, as well as, rigorous project management are vital in order to successfully minimise the company's exposure to risk.

Further Reading:

- ✓ ***Julia Graham, David Kaye, (2006), a Risk Management Approach to Business Continuity***
- ✓ ***Adam Jolly, (2003), Managing Business Risk***