Chapter IV: Risk Assessment

Objectives

- Define risk terminology
- Define the purpose of Risk Assessment (RA)
- Review the RA process
- Review how threats to an organization are identified
- Identify and evaluate controls
- Explore event probability estimation
- Identify methods of impact estimation
- Analyze risk measurement
- Identify the risks of greatest concern
- Examine the options to manage risks.

Risk

Risk management is the basis of BCM and provides an analytical foundation for decision making regarding the treatment of risk. A key tenet of risk management is that risk cannot be eliminated but that it can be controlled. The appropriate control to employ depends both on the likelihood of the risk occurring and the magnitude of the loss if the risk does occur. Often risk can be quantified; however, when risk cannot be quantified, either because the underlying information does not exist or because it is too expensive to collect, principles of risk management can still be applied. These principles include:

1. Identifying what can go wrong by analyzing the underlying threats and possible crisis events;
2. Identifying what controls are currently in place;
3. Evaluating the current exposure to the organization;
4. Identifying new controls that can be implemented to reduce this exposure;
5. Evaluating whether these controls should be implemented by investigating the costs and benefits.

An **event** (incident) is an occurrence that could have an impact upon the organization. Because BCM deals with events that are improbable, analyzing risks is challenging. It can be difficult to come to grips with uncertainties surrounding highly unlikely events with major potential adverse impact upon the operation of an organization.

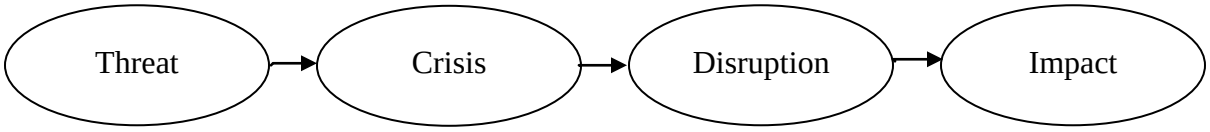
The core of the analysis involves specifying a set of encompassing crisis events which represent 'what can go wrong.' A **threat** (hazard) is a source of potential negative impact. A **crisis** (crisis event) is a manifestation of a threat. If not handled properly, a crisis may have a severe negative impact. A **minor crisis** has limited impact and does not affect the overall functioning capacity of an organization, whereas a **major crisis** has the potential to seriously disrupt the overall operation of an organization. A **disaster** is a major crisis event which imperils an organization. An event may be deemed to be a disaster due to factors such as loss of life, environmental damage, asset damage and duration of disruption. A **catastrophe** is an extreme disaster.

Risk is the possibility of experiencing an event, measured in terms of probability and impact. **Probability** is a measure of the likelihood of an event. A **risk event chain** describes the transition from threat to crisis to disruption to impact. Figure 4.1 depicts a risk event chain. As an example, fire is a threat and a crisis would be a fire affecting a particular facility. The fire can cause a disruption of the processing facility for a length of time. The disruption can result in an impact of asset damage and revenue loss.

The paradigm of the risk event chain provides flexibility in the level of detail to use in analyzing risk. For example, using a broad view during an initial study, an impact can be thought of as resulting from a threat without explicitly studying the transitions through crisis and disruption.

Controls can reduce the probability of transitioning through the risk event chain and can mitigate the resultant impact. It is possible for different crisis events to result in the same disruption; for example, a data center could be destroyed by a fire, flood or explosion. Because identifying all possible crisis events is difficult and impractical, the events chosen for analysis should represent the most significant exposures faced by the organization.

Figure 4.1 - Risk Event Chain



Risk analysis is the process of identifying events, determining causes, and estimating probabilities and impact. **Risk evaluation** is the process of comparing risk levels with established risk criteria. **Risk Assessment (RA)** is the process of risk analysis and risk evaluation. The purpose of RA is to prioritize planning by assessing the likelihood of events and their potential impact on critical functions. RA is fundamental to identifying vulnerability and is a basis for resource allocation and exposure mitigation. **Vulnerability** is a measure of exposure to a threat that increases as the probability and impact of the event increases. **Risk tolerance** is the amount of risk that an organization is prepared to accept. Risk tolerance drives the level of action an organization will take to control identified threats. **Risk management** is comprised of the processes of risk assessment, risk communication and risk treatment. **Risk communication** is the exchange of risk information among stakeholders and **risk treatment** is the selection of procedures for managing risk.

RA is used to determine the most significant threats to an organization and to direct hazard-specific planning to address these threats by prioritization. RA activity should be focused on the most urgent business functions identified during the BIA process.

The steps of RA are:

- Identify significant threats to critical operations.
- Identify and evaluate controls.
- Estimate event probabilities.
- Estimate impacts.
- Determine a risk measure combining impact and probability.
- Prioritize risks.

Senior management reviews the findings of RA and information developed during RA provides a basis for managing risk.

Threat Identification

Threats are ubiquitous and represent possible sources of negative impact to an organization. Threats can be natural, accidental or man-made and can lead to disruptions in operations which can adversely impact an organization. Significant threats that warrant further consideration are identified during RA.

Generic threats to consider include:

Acts of war	Flood	Radiation leak
Armed attack	Freeze	Riot
Blackmail	Hostage situation	Terrorism
Blizzard	Hurricane	Tornado
Chemical spill	Insurrection	Transportation disruption
Contamination	Kidnapping	Tsunami
Earthquake	Power outage	Volcano eruption
Fire	Product defect	Workplace violence

There are other categories of threats that can have a negative impact on an organization. A holistic approach towards risk management needs to include an analysis of all threats such as those of financial, economic, market, fraudulent and negligence origin. The relevance of a threat depends upon many factors including: geographic location, infrastructure, political conditions and economic conditions. A systematic way to collect and analyze threat data is to begin with a broad view and then continue to a detailed view. For example, using a sequence such as region, community and building may be useful. Threats can be identified in the general region (e.g. hurricane), in the community (e.g. power outage) and in the building (e.g. fire).

For natural threats, the gathering of data with sufficient detail and accuracy can usually be accomplished by research on the Internet. General information for weather and seismic threats is usually easily obtained. When evaluating man-made, accidental and other non-natural threats, there are often a large number of variables involved. Information for man-made, accidental and other threats tend to be less location-specific and more judgment is often required.

The manifestation of a threat as a crisis may lead to a disruption. In identifying possible disruptions it is helpful to draw upon the information gathered in the BIA. Some outages that should be addressed include:

- Destruction of a processing area due to fire or bomb.
- Destruction of a building by fire, bomb or earthquake.
- Flooding of a processing area of adjacent areas due to hurricane, storm or ruptured water pipe.
- Inaccessibility to a building due to fire or bomb threats.
- Outages in communications, electric power, steam supply or air conditioning due to fire or flood.
- Lack of processing personnel due to a strike, transportation problems or snowstorm.

Those specific events which impact operations and cause disruptions beyond the RTO are then identified.

Part of the difficulty in assessing certain threats is a result of the type of organization under analysis. The two business case studies included in this book illustrate these differences. Another part of the difficulty in assessing certain threats is a result of a large number of controls, exposures and variables. Consider the following examples:

- Example 1 – An organization with a technology department that has an IT alternate site plan and backup data center that can be activated rapidly will be able to recover quickly from a major crisis. An organization without these planning and resources available will most likely not be able to recover quickly. Also, a technology department with good physical controls (e.g. raised floors, fire suppression system, dedicated HVAC, and backup electric generator) at the data center is less likely to experience a major crisis than an organization that does not have good physical data center controls in place.
- Example 2 – An organization with good security controls (e.g. proper procedures, monitored security system, dedicated security personnel) can avoid many security breaches. Security will also be impacted by the general crime rate in the area and the exact nature of the organization.
- Example 3 – A manufacturing organization that requires the use of hazmat materials can reduce the likelihood of a hazardous release and can contain a release better if a good hazard response plan is in place. Many other factors are important. Has the hazmat team been properly trained and properly equipped? What types of chemicals are used? How are the chemicals stored?
- Example 4 – The RA of a terrorist attack is most difficult to make. The type, level and location of the event will all be factors that are often hard to pinpoint. RA must consider the likelihood of a terrorist attack on the organization and in the immediate area. Plus RA must consider the impact, if any, of a major terrorist attack at a distant location. Certain organizations may be impacted by overseas terrorist attacks.

Controls Identification and Evaluation

Controls are devices and procedures that prevent the occurrence of a crisis event or mitigate the impact of a threat. Controls include physical security, preventive maintenance, information security and personal procedures. The effectiveness of existing controls should be evaluated. The evaluation of controls includes determining the benefits of the controls, identifying costs, developing options and improving the controls. After determining any outstanding risks to the organization, potential cost-effective controls are identified and recommended for management approval.

Some controls reduce the probability that an event will occur; other alternatives reduce losses by providing some business continuity during a disaster or improving workplace safety. Generic control checklists are useful in exploring alternatives. For each function, the generic alternatives are further developed with appropriate details for the specific location. The annualized cost of each alternative is calculated and compared to the reduction in the expected annualized risk exposure. Some decisions are obvious; others require more detailed quantifications and sensitivity analysis. Recommendations regarding additional planning, improvements to existing procedures and physical controls to mitigate damages, injuries and loss of life should be identified.

Building Evacuation and Safety Procedures

The two most common safety procedures are building evacuation and shelter-in-place. Most individuals understand how to conduct a building evacuation as these procedures have been regularly practiced in the school system. Shelter-in-place procedures have historically not been practiced as frequently as building evacuation procedures.

It is important that formal plans be developed to address both building evacuation and shelter-in-place procedures. Plans should include the identification of safe gathering areas, routes to gathering areas and procedures to make a headcount at the gathering areas.

The need to communicate emergency instructions during a crisis event is central to the effectiveness of executing the procedure. Communicating accurate and sufficiently detailed information presents an important challenge. Typically alarms alert everyone to conduct a building evacuation.

At a minimum, some type of siren is needed to alert everyone that a dangerous condition exists and a shelter-in-place needs to be performed. In addition to a siren, it is very important to utilize an intercom or other communication system. Emergency information regarding a hostile intruder, hazardous release or tornado cannot be effectively communicated by a siren alone.

Depending on the specific threat there are important differences in the exact shelter-in-place procedures. For a hostile intruder threat, doors need to be locked, windows and window treatments should be closed, and everyone should get out of sight. For a tornado threat, with time permitting, employees in outside rooms should relocate to interior corridors – this procedure is not recommended in a hostile intruder situation.

... Continued...
