Unit 14 Risk Management & Security

Learning Outcomes

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

- ✓ Define risk and risk management
- ✓ Describe the COSO ERM cube and ISO 31000
- ✓ Describe the 7 R's and 4 T's that form the framework of risk management activities
- ✓ Determine the appropriate response to risks and create a plan for those responses
- ✓ Describe the key components of reporting, monitoring, and evaluation of a risk management program

Unit 14

Introduction to Risk Management

The ISO 31000 risk management standard defines risk as, "the effect of uncertainty on objectives." Risks are typically related to one of four areas:

- The organization's long-term strategy (three years, five years, and beyond)
- The way that an organization manages change (for example, during mergers and restructuring)
- The day-to-day operations of the organization
- The general financial health of an organization

Risk can be positive, negative, or neutral. They are, in general, simply a deviation from the norm. Risk is often defined as an event or a consequence. Some examples of risks are:

- Interruptions of the business cycle or business processes arising from government regulation, economic conditions, social conditions, weather systems, natural disasters, and other sources.
- Unforeseen changes in existing strategic partnerships, key business relationships, and vendor/supply sources.
- Changing labor market conditions affecting labor force availability and costs.
- Issues arising from integrations of computer systems, communications networks, accounting systems, and other systems.
- Access to information may be prevented by government or legal restrictions, privacy concerns, or other frameworks that are put in place.
- Security conditions might arise that affect operations.

Types of Risks

Quantitative risks are those that can clearly be quantified. They have an impact on time, people, money, or other resources. An example could be lost revenue, lost production, or delayed time.

Qualitative risks are those that cannot easily be clearly quantified. This may be because you do not have sufficient historical data to determine the likelihood of the risk and/or its impact is not understood well enough for a qualitative impact to be associated with it.

An example: Your organization is opening an oil rig in a new area. You have no concrete data for this particular type of machinery in poor weather, but you do know that other facilities in the area have their production affected in varying amounts each year because of weather.
You should always strive to make all qualitative risks quantitative, if possible, by collecting and analyzing data.

What is Risk Management?

Risk management is defined as a set of principles and processes that help minimize the negative impacts of risks and maximize the positive impacts. Risk management should identify risks, assess them, determine a suitable response, and implement that response. In order for risk management to be successful, it must be integrated into the culture and the day-to-day activities of the organization.
Your risk management process should be PACED:

- **Proportionate** to the size of your organization
- **Aligned** to your organization's mission
- **Complete**
- **Embedded** into the culture of the organization and its day-to-day activities
- **Dynamic** and responsive

Some examples of risk management processes and plans:

- House insurance
- Disaster recovery plans
- Succession planning

Risk management is the process whereby an individual or a corporation analyses potential risks. It also contains strategies for decreasing the expenses associated with these risks. All categories of risk incorporate two kinds of costs.

The first is the cost that will be incurred if a possible loss materializes into an actual loss, such as the cost of re- equipping or restructuring an assembly plant that has been burned to the ground. The second includes expenses for reducing or perhaps eliminating risks of possible loss. This would include all costs equal to the net income which this plant may have generated. For risk management to be productive, both of these types of costs have to be balanced against each

other.
Most people consider risk management to simply comprise buying insurance; however insurance is not the only strategy for managing risk. Several alternative methods can prove to be more economical in various situations. Furthermore, some kinds of risks are simply uninsurable. This means that no insurance company will be willing to issue a policy for protection against them.

Three common risk management techniques are:

Risk Avoidance

An individual can avoid any kind of car accident related risks by not travelling in a car. A business can avoid product failure risk by disregarding new products launches. Both situations exhibit attempts to practice risk avoidance; however, at a particularly high cost.

Individual who evades car accidents by not using cars might have to give up their jobs to do so. Companies that do not take a risk on new product releases would probably not be able to stay competitive, thus move towards business closure.

On the other hand, there are instances where risk avoidance is an appropriate strategy. Individuals who avoid strolling through a dark city park late at night or those who stop smoking are perhaps avoiding risks in more sensible ways that are likely to benefitthem.

Businesses, such as jewellery shops that lock their products inside their vaults at the end of the work day are working towards risk avoidance by preventing losses through theft. Similarly, several petrol stations only accept credit cards or possibly only exact amounts of money for sales made after dark to avoid the risk of a holdup.

It is pointless to say that no individual or corporation can avoid all risks and neither should anyone make an assumption that all risks are unavoidable.

Risk Reduction

Although a risk may be possible to prevent, it may perhaps be minimized. An individual travelling by car can minimize the probability of injury during a car accident by wearing a seat belt. Business organizations can reduce the likelihood of product failure through careful product planning and comprehensive market testing.

In both situations, the cost incurred to minimize the risk apparently appears to be worth the potential savings. Businesses sometimes experience risks because of their immature operational strategies and inappropriate decision making by the leadership. An operating procedures' evaluation perhaps by company personnel or external experts can frequently identify places in which risk can be decreased.

Some strategies that may be used include:

- Establishment of safety programmes for employees which help to encourage employees
- To be aware of the importance safety measures.
- Purchase and application of safety equipment, such as hand guards for machinery, goggles, and safety shoes for personnel.
- Security guards, robbery alarms, and guard dogs to prevent burglaries at warehouses.

- Use of sprinkler systems, smoke alarms, and fire alarms to decrease the possible risk offire and losses incurred due to fires.
- Accurate and productive financial and accounting regulations to protect business funds and inventories from stealing.

Risks resulting from management decisions can be reduced through productive decision-making. Risks may arise each time a decision is based on insufficient information or made in haste. Nevertheless, the costs associated with minimizing risks increases when managers require overabundant information before they can make a decision.

Risk Assumption

An individual or a business will possibly have to accept certain risks as part of conducting business activities or even as a component of their existence. When people drive to work, they accept the potential risk of an accident; however, wearing a seat belt reduces the risk of injuries in case an accident occurs.

Businesses promoting new products accept the potential risks involved with product failure and minimize this risk with strategies such as market testing and research. Assuming risk is therefore an act of taking responsibility for an injury or loss that may result from the risk.

Generally, it is practical to assume a risk when one or more of the following conditions exist:

- The potential loss is too insignificant to warrant too much concern.
- Practical strategies of risk management have reduced the risk to a minimal level.
- Any insurance coverage available is too expensive.
- No alternate strategies are possible for protection from the loss.

Large businesses with several facilities frequently find a certain kind of risk assumption strategy known as self- insurance to be a practical technique for avoiding huge insurance costs. The process of establishing a monetary fund to be used for paying for the cost of any losses that occur is known as self- insurance.

For example, if the business has approximately 16,000 XYZ grocery stores spread across the country and each of these is worth £400,000, a practical solution for self-insurance against fire losses could be to gather a specific sum, perhaps £600 from each store on an annual basis. The entire fund would then be deposited in an interest-bearing reserve fund. It could then be used if and when required to restore any damage caused by a fire that occurs at XYZ stores.

Any funds not used continue to be an asset of the business. If the fund continues to grow consistently, the yearly contribution from every store may be reduced. Self-insurance does not end risks; instead, it simply provides the means for covering any losses if they occur.

It is however a risky strategy; particularly at the start. If XYZ suffered a substantial financial loss with maybe over twenty-four stores being damaged by fire during the first year that the self-insurance programme had been implemented, the losses would exceed the accumulated funds rendering the entire exercise futile.

Benefits of Risk Management in a Nutshell

Risk management is a process that provides assurance in the following ways:

- By increasing the possibility that objectives will be accomplished.
- Destructive circumstances will be managed in a more practical and sensible manner.
- Beneficial objectives are more likely to be achieved.

Risk Management techniques do not necessarily stop risks from occurring. The objective of risk management is not to eliminate risk, instead it is aimed at managing risks related to all situations, so that possible opportunities may be increased and negative effects lowered significantly.

Risk Management Tools

Tools used for managing risk can be categorized into two methodologies; risk financing and risk control.

Risk Financing

Risk financing focuses on arranging finances to be available for covering losses that arise from any risks that still remain after risk control methods have been applied. This includes the tools of transfer and retention.

Risk Control

Risk control aims to reduce risk of loss through implementing the methods of reduction and prevention. Risk control includes the strategies that can reduce at least the possible costs. Such procedures comprise risk avoidance in addition to different tactics for limiting risk through control efforts and loss avoidance.

Risk Prevention

Risk protection must be applied in circumstances that have catastrophic potential with risk that cannot be transferred or minimized. Generally, such situations exist in events with severity and high frequency. If extensive prevention is used, the business will not be in a position to achieve its main objectives.

A product manufacturer cannot eliminate the risk of product liability through risk avoidance, while staying in business. Prevention is therefore, the final option in working with risk and should be used only if there is no other option.

Risk Reduction

Risk reduction contains all strategies that can decrease the possibility of loss, or even the possible severity of the losses that occur. As stated in the description, loss prevention emphasizes preventing the possibility that a loss occurs, which means governing the occurrence.

Strategies for risk reduction concentrate on reducing the severity of the losses that actually take place, such as installing sprinkler systems to manage a fire that does get started. Such tactics are control measures.

Several other methods for decreasing the severity of losses include distribution or segregation of assets, and also salvage efforts. Asset dispersion will not reduce the number of explosions or fires that could occur; however, it can decrease the potential severity of losses that do take place.

The ultimate approach for classification of risk reduction measures is based on the timing of their application, such as before the occurrence of the loss, during the occurrence of the event, or right after the loss has occurred.

Risk Management as a Business Factor

Risk management plays an important role in contributing towards the corporation's basic objectives and goals in several ways by guaranteeing that the company will not be held back from pursuing its various objectives because of losses connected to pure risks.

Risk management can directly affect the profit made by the corporation by controlling the cost of risk it incurs. Based on the fact that profits depend on the amount of costs in relation to income, the extent to which risk management strategies can reduce costs can directly increase the profits. Similarly, risk management can decrease costs by implementing risk control procedures to the extent that the expense incurred on loss control and prevention measures is less than the volume of losses that are avoided, and expenditure on uninsured losses is minimized.

Along with limiting costs connected to losses, income can also be maximized through risk management practices. Risk managers may suggest acquiring political risk insurance that is reasonably priced and available, and management can decide to follow their recommendation, which may generate increased profits. Risk managers are responsible for pure risk management and may select from several alternative risk management techniques. They are generally in a position to make extensive contributions towards the organization's operating outcomes.

Establishing Your Risk Management Context

Each organization is unique, and it is crucial that you identify the context in which your risk management framework must operate. Consider:

- The regulatory or legal environment you operate in with respect to both internal practices (e.g. labor laws and regulations, liability claims, etc.) and how you relate to your customers and vendors.
- Communication methods you will use to notify and communicate with your stakeholders, as a range of techniques may be required to suit different stakeholder groups.
- The size of the organization in terms of the number of divisions, revenue of business lines size of markets, and budgets of functional groups.
- Labor relations in the organization.
- The structure of the organization, which can affect risk analysis, planning, and implementation.
- The culture of the organization with respect to risk tolerance. Is your organization a conservative family business or an edgy risk-taker?

Key Models

COSO ERM Cube

In 2004, the Committee of Sponsoring Organizations of the Tread way Commission (COSO) published a risk management standard known as the COSO ERM (Enterprise Risk Management) cube. It was designed to match up to Sarbanes-Oxley regulatory requirements for organizations in the United States, and is therefore quite popular.

The cube lays out four categories of objectives:

- Compliance
- Operational
- Reporting
- Strategic

This is followed by eight rows of components that are needed to achieve those objectives:

- Control Activities
- Event Identification
- Information and Communication
- Internal Environment
- Monitoring
- Objective Setting
- Risk Assessment
- Risk Response

The third dimension illustrates an organization's various business units:

- Subsidiary
- Business Unit
- Division
- Entity Level

Source: Enterprise Risk Management Integrated Framework, Executive Summary (September 2004), Committee of Sponsoring Organizations of the Treadway Commission (http://www.coso.org/documents/coso_erm_executivesummary.pdf)

ISO 31000 Standard and Guide 73

In 2009, the International Organization for Standardization published a guide and a standard for risk management.

ISO Guide 73 defines generic risk management terms to provide a consistent foundation for frameworks and processes. ISO Standard 31000 provides best-practice principles about risk management.
Because this is an international standard, much broader based, and very recent, this is the standard that we will focus on during this course.

The Risk Management Process

This graphic shows the seven R's and four T's that traditionally represent the key activities of risk management:

We will review each of these activities during this course.

A Risk Assessment Process

Types of Processes

The first step in risk management is to recognize and identify risks. Remember, your risk assessment process should be proportionate to your organization, so if you have a large, complex organization, you will need a formal, complex risk identification process. If you have a small organization, a short, informal process may suffice. Either way, you need to spend time recognizing and identifying risks.

Sample Template

You should have a template to track and record all relevant information. The template will vary in complexity according to your organization's needs, but basic information should include the following elements.

Basic Information

- Risk identifier, such as a number
- Date risk reported
- Who the risk was identified by

Description of Risk

- Classification (usually based on organization's business or operating units, but should be customized for each organization)
- Why is it a risk?
- Is this a hazard, opportunity, or uncertainty?
- Tangible impact (people, time, money, etc.)
- Non-tangible impact (reputation, morale, objectives, etc.)
- Data gathered or studies completed

Timeline

- When might the risk occur?
- How long could it last?
- Could it reoccur?
- What signals or alarms will we see?

Scope of Risk

- What could happen as a result of this risk?
- What is the likelihood of the overall risk and each consequence?
- What data do we have about the consequences of this risk?
- What other risks could occur from this risk?

Ratings and History

- Rate the impact (low, medium, or high) and the likelihood (likely, neutral, not likely)
- Outline previous experience with this risk
- Describe risk attitude and organizational tolerance for the risk

Existing Risk Systems

- Existing controls and estimated effectiveness
- Monitoring procedures
- Improvement recommendations and information
- Related policy or procedural information

Identifying Risks

How do you identify risks? Some common methods include:

- Using real or hypothetical case studies
- Drawing on personal and organizational experience
- Looking at similar projects and learning from their experience
- Consulting experts
- Mind mapping or brainstorming techniques
- Considering points of failure
- Extrapolating from past incidents reports or complaints
- Interviewing and/or surveying stakeholder groups
- Using systems analysis techniques like flowcharting
- Operational modeling
- Formal auditing or inspections
- Conducting new studies or consulting previous studies

Work breakdown structure analysis You can also use formal analyses such as:

- **SWOT:** Stands for Strength, Weakness, Opportunities, and Threats. A good system to create a broad picture of any situation.
- **PESTLE:** Stands for Political, Economic, Social, Technological, Legal, and Environmental. Used to assess the current market conditions and create a strategic plan.
- **HAZOP:** Stands for HAZard and OPerability study. Provides a structure and system to examine a process or operation to identify risks.
- **FMEA:** Stands for Failure Mode and Effects Analysis. A system that analyzes system failures and their effects.

In order to ensure your risk identification is complete:

- Information gathering should always be a group activity.
- Gather hard data whenever possible.

Responding to Risks

The Four T's

The best risk response plans usually provide a few response options, ranked in order of preference. There are generally four ways that you can respond to risks.

Tolerate

Accept that the risk exists and tolerate the possible consequences.

Treat

Perform an action to mitigate the risk. For example, if you know that the bank may not approve you for as much money as you need, you may want to look for other sources of funding.

Transfer

Transfer the responsibility or the consequences of the risk to a third party. This is often done through a guarantee or insurance.

Terminate

Stop the activity that causes the risk.

Key Considerations

Keep the following points in mind when choosing a mitigation strategy.

- Any strategy should do as much as possible to ensure normal business practices are not interrupted or are delayed as little as possible.
- In any large company, a risk materializing will almost certainly require media engagement to make announcements, clarify details, and provide on-going information to stakeholders and the general public about what your organization is doing. Managing the media should be part of your plan.
- Direct communication with stakeholders is critical. It should be either general but informative or very specific to the impact the risk has on them.
- If there is any chance that people may be injured or worse, you should include medical support in your planning. This can mean having an emergency response team standing by or providing emergency support numbers to your staff.
- Depending on the risk, you may be required by law to obtain insurance against it occurring. If this is not the case but insurance is available you should perform a cost/benefit analysis to determine if insurance should be part of your risk mitigation strategy.

Reporting and Monitoring

The Reporting Structure

When your organization establishes its risk management framework, a reporting hierarchy should also be established. Your reporting structure will differ depending on the complexity of your risk management program. Some common setups include:

- A part-time risk manager
- A risk management committee
- A full-time risk management champion
- A risk management team
- A risk management department with an internal audit team

Reporting and Monitoring Framework

Your organization will need to develop a checklist of items that will need to be reported on and monitored on a regular basis. This checklist should include:

- What data is to be gathered
- What form it is to be presented in
- Templates to be used
- When data should be gathered and reported
- Who is responsible for measuring, reporting, and monitoring

Reporting Checklist

Items that will need to be reported on include:

- Changes to risks
- Near misses and incidents
- Changes that will affect the risk management program, such as legislative changes, industry developments, and changes in supporting elements of risk planning

Depending on your organization, you may also need to provide reporting according to external guidelines, such as Sarbanes-Oxley or Turnbull.

Monitoring Checklist

Items that should be monitored include:

- Effectiveness of risk controls
- Cost of controls vs. benefit achieved
- Laws and legislation
- Industry climate
- Alignment of risk management plan with corporate goals

Reviewing and Evaluating the Framework

A Review Checklist

A plan for periodic review and evaluation of the risk management framework is a critical element of any risk management program. Typically a thorough review is performed annually.

Things that should be covered in the review process include:

- Analysis of risk response measures and whether they achieved the desired result, and did so efficiently
- Review of reporting and monitoring procedures
- Knowledge gap analysis for risk assessments (Were people able to find the information they needed?)
- Compliance check with appropriate regulations and organizations
- Opinions of key external and internal stakeholders
- Self-certification
- Risk disclosure exercise, to identify future risks
- Repeat of risk assessment
- Lessons learned
- Recommendations and implementation plan

Remember, the review should be proportionate to your organization. If your organization is small, an afternoon meeting to review your risk management program may be sufficient. For larger organizations, the review process may take weeks or even months and require outside assistance.

Back at Work

What kind of risk management framework would be most appropriate for your organization?

What kind of review procedures would need to be put in place?

Further Reading:

- ✓ *Risk Management in Project Organisations, (2005), By Peter Edwards, Paul Bowen*
- ✓ *Risk Management: Survival Tools for Law Firms, (2007), By Anthony E. Davis, Peter R. Jarvis*
- ✓ *Risk Assessment and Risk Management,(1998), edited by Ronald E. Hester, Roy M. Harrison*
- ✓ *Risk Management, (2006), By Satyajit Das*
- ✓ *RAMP - Risk Analysis and Management for Projects: A Strategic Framework for, (2005), By Institution of Civil Engineers (Great Britain)*
- ✓ *Managing Reputational Risk: Curbing Threats, Leveraging Opportunities, (2004),*