RISK MANAGEMENT

COURSE NOTES

Learning Together
Achieving Together

Tel: (+267) 311 48 58 • (+267) 72 309 719 • **Email:** training@kti.co.bw • **Website:** www.kti.co.bw

Table of Contents

Session One: Course Overview

Risk management has long been a key part of project management and it has also become an increasingly important part of organisational best practices. Corporations have realized that effective risk management can not only reduce the negative impact of crises; it can provide real benefits and cost savings.

The risk management framework provided in this course is flexible enough for any organisation. You can apply it to a single project, a department, or use it as a basis for an enterprise-wide risk management program.

Learning Objectives

After you complete this course, you will be able to:

- Define risk and risk management.
- Describe the COSO ERM cube and ISO 31000.
- Establish a risk management context.
- Describe the 7 R's and 4 T's that form the framework of risk management activities.
- Design and complete a basic risk assessment.
- 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.

Why did you take this course? Use this opportunity to consider your personal learning objectives and reasons for taking this course.

Pre-Assignment

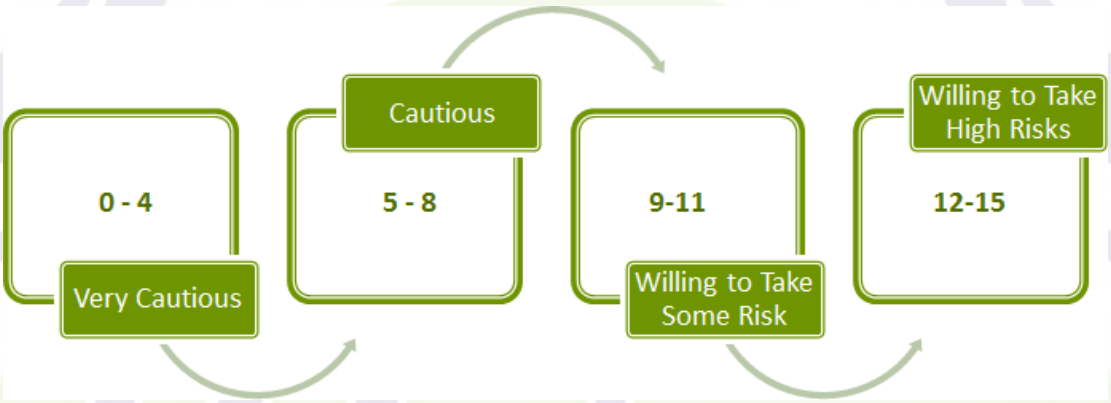
RISK TOLERANCE EXERCISE

Complete this exercise before the course. Read each description and circle whether you agree or disagree with the description on the basis of your management work. Don't look for hidden or double meaning in the descriptions; your first reaction is probably your best.

1.	Taking chances makes sense if there are no low-risk alternatives.	Agree	Disagree
2.	I generally prefer action over waiting.	Agree	Disagree
3.	I am able to recover from mistakes, even really big ones.	Agree	Disagree
4.	I believe in helping new people develop their experience so that they can succeed, rather than giving positions to people with more experience who refuse to try new ways of doing things.	Agree	Disagree
5.	I can accept things that are not done perfectly.	Agree	Disagree
6.	I believe in seizing opportunities when they arrive.	Agree	Disagree
7.	It is better to ask for permission beforehand than to beg for forgiveness afterward.	Agree	Disagree
8.	Success is 50% luck and 50% skill.	Agree	Disagree
9.	I prefer to be paid a set salary rather than pay for performance (or commission), which varies depending on my own efforts and results.	Agree	Disagree
10.	If things go really wrong I recover quickly because I know I did my best.	Agree	Disagree
11.	Safety of myself and others is more important than making more profit.	Agree	Disagree
12.	Repeated failure is a very long road to achievement.	Agree	Disagree
13.	I can tolerate ambiguity and uncertainty without difficulty.	Agree	Disagree
14.	I would rather fail than to not have tried.	Agree	Disagree
15.	When I consider a decision where results are unclear, my greatest concern is for potential losses.	Agree	Disagree

SCORING

- Give yourself one point for each of the following statements with which you agree: 2, 3, 4, 5, 10, 13, 14.
- Give yourself one point for each of the following statements with which you disagree: 1, 6, 7, 8, 9, 11, 12, 15.
- Calculate your total.
- Plot your total on the risk scale.



Session Two: Understanding Risk

Risk management is an important consideration for every organisation, and is a responsibility for everyone. It's inherent in many of the things that we do, from considering which way a door should open to when to shovel the walkways.

In this session, you'll learn to define risk and risk management, and start using some of the related terms.

Pre-Assignment Review

What are the implications of your score for the risk management efforts that you are about to undertake?

Hint:

Answers could include:

- If you are very risk averse and point out everything as being a risk, it can consume a lot of time and resources.
- If you are willing to take such high risks that the company may continue to be exposed, your focus may need to be on mitigating risk.

Defining Risk and Risk Management

WHAT IS RISK?

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

Risk can be positive, negative, or neutral. They are, in general, simply a deviation from the norm.

TYPES OF RISKS

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 labour market conditions affecting labour 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

EXAMPLES OF RISK

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 organisation 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 analysing 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 organisation.

Your risk management process should be **PACED**:

- **Proportionate** to the size of your organisation
- **Aligned** to your organisation's mission
- **Complete/Comprehensive** in order to be a fully effective risk management approach
- **Embedded** into the culture of the organisation and its day-to-day activities
- **Dynamic** and responsive to emerging and changing risks

Some examples of risk management processes and plans:

- House insurance
- Disaster recovery plans
- Succession planning

WHAT DO YOU THINK SOME OF THE BENEFITS TO RISK MANAGEMENT MIGHT BE?

- Compliance with regulations and laws
- Better decision making
- Reduced operating and legal costs
- More accurate reporting
- Improved image in the community, marketplace, and/or industry
- Competitive advantage

Establishing Your Risk Management Context

Each organisation 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. labour 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 organisation in terms of the number of divisions, revenue of business lines, size of markets, and budgets of functional groups.
- Labour relations in the organisation.
- The structure of the organisation, which can affect risk analysis, planning, and implementation.
- The culture of the organisation with respect to risk tolerance. Is your organisation a conservative family business or an edgy risk-taker?

Key Models

COSO ERM Cube

In 2004, the Committee of Sponsoring Organisations of the Treadway 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 organisations in the United States, and is therefore quite popular. It has gained broad acceptance by many organisations in their efforts to manage risk. It must be noted that since 2004, the complexity of risk has altered, new risks have emerged, so the update to the COSO ERM (Enterprise Risk Management) cube, reflects the evolution of enterprise risk management and the necessity for organisations to refine their approach to managing risk to meet the demands of the evolving business environment.

The cube lays out three categories of objectives:

- Operations
- Reporting
- Compliance

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

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

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

- Entity Level
- Division
- Business Unit
- Function

Source: Compliance Risk Management: Applying the COSO ERM Framework (November 2020), Committee of Sponsoring Organisations of the Treadway Commission.

ISO 31000 Standard and Guide 73

In 2009, the International Organisation 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.

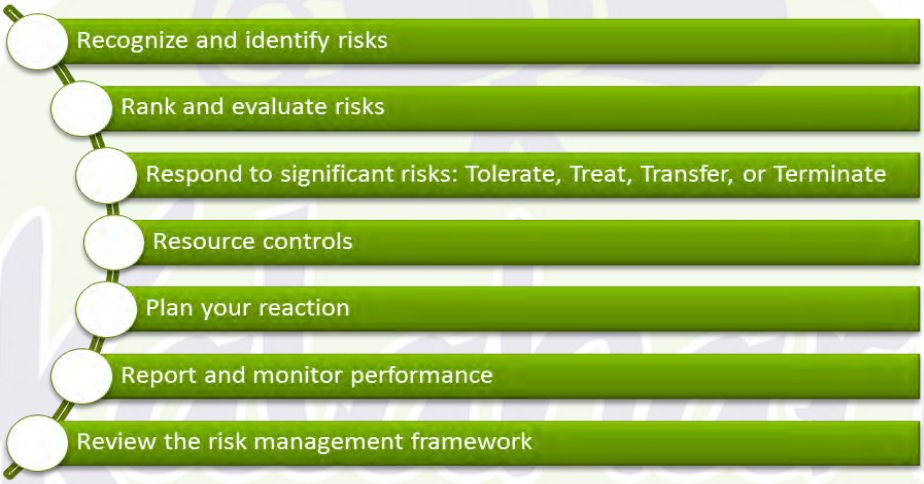
Session Three: Risk Management Activities

As you become more familiar with the risk management role, you may find yourself looking at things that you do a little differently. Look around the room that you are in right now. Are there risks present?

In this session, you'll learn the essentials for identifying and responding to risk in a helpful format of seven R's and four T's.

The Seven R's and Four T's

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.

Session Four: Assessing Risk

Describing risk is one thing. Doing it in a way that really points out its significance and the need for a response is another. Sometimes things that we see on the surface as a risk turn out to be relatively minor, and sometimes they don't.

In this session, you'll learn to gather information and organize it as part of a risk assessment that has practical application.

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 organisation, so if you have a large, complex organisation, you will need a formal, complex risk identification process. If you have a small organisation, 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 organisation'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 organisation's business or operating units, but should be customized for each organisation)
- 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 organisational 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 organisational 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 flow charting
- 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 analyses 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.

EVALUATION METHODS

Once risks have been identified, you can evaluate risks and choose how to rank and evaluate them. One common method is a 3 x 3 matrix.

	Severity		
Likelihood	**Low**	**Medium**	**High**
Likely			Focus efforts here first
Neutral			
Not Likely	Focus efforts here last		

This tool can be customized and expanded to include additional levels of severity and likelihood.

Case Study: General Motors (Part One)

BACKGROUND INFORMATION

General Motors (GM) has long been the world's number-one manufacturer of cars and trucks. Their brand line has included Buick, Cadillac, GMC, Chevrolet, Pontiac, and Saab. Their business model includes overseas operations such as Vauxhall and Opel, Hughes Electronics, Allison Transmission, and GM Locomotive. They also have stakes in other brands, including Isuzu, Subaru, Suzuki, Fiat, and Daewoo.

After years of a downward spiral in their market share, GM finally achieved two straight years of increase in 2002. In 2003, GM planned to continue this gain by launching 30 new gas-powered vehicles.

TASK ONE: RISK ONE

Identify one risk for General Motors' plan.

Risk Area:

- Legal
- Regulatory
- Marketplace
- Financial
- Operating
- Other: _____

Possible Tangible Effects (such as money, time, and resources):

Possible Intangible Effects (such as morale and reputation):

Impact:

- Low
- Medium
- High

Likelihood:

- Unlikely
- Neutral
- Likely

When might this occur?

How long could it last?

What other risks could result?

Task One: Risk One - Possible Answer

Identify one risk for General Motors' plan. The marketplace is beginning to ask for hybrid vehicles but these products are not included in our line-up.

Risk Area: Marketplace

Possible Tangible Effects (such as money, time, and resources): Loss of market share, reduced profit

Possible Intangible Effects (such as morale and reputation): Could affect GM's reputation as a cutting-edge auto manufacturer and industry leader

Impact: Medium

Likelihood: Likely

When might this occur? Rival automakers have their product launch scheduled for Q3 next year.

How long could it last? These vehicles will likely be slow to catch on but will quickly rise in popularity.

What other risks could result? If we are required to start manufacturing these new vehicles, we will face significant challenges in worker knowledge, manufacturing equipment, and product sourcing.

TASK ONE: RISK TWO

Identify a second for General Motors' plan.

Risk Area:

- Legal
- Regulatory
- Marketplace
- Financial
- Operating
- Other: _____

Possible Tangible Effects (such as money, time, and resources):

Possible Intangible Effects (such as morale and reputation):

Impact:

- Low
- Medium
- High

Likelihood:

- Unlikely
- Neutral
- Likely

When might this occur?

How long could it last?

What other risks could result?

TASK ONE: RISK THREE

Identify a third for General Motors' plan.

Risk Area:

- Legal
- Regulatory
- Marketplace
- Financial
- Operating
- Other: _____

Possible Tangible Effects (such as money, time, and resources):

Possible Intangible Effects (such as morale and reputation):

Impact:

- Low
- Medium
- High

Likelihood:

- Unlikely
- Neutral
- Likely

When might this occur?

How long could it last?

What other risks could result?

TASK TWO

Plot each risk that you identified on the matrix below.

Likelihood	Severity Low	Medium	High
Likely			
Neutral			
Not Likely			

Possible Risks include:

- Volatile financial markets
- Change in emissions standards
- New technologies such as hybrid and electric vehicles
- New automakers in the market
- Changing currency rates
- New hazard standards (such as a reduction in asbestos use)
- Labour strikes and work stoppages
- Political instability in overseas manufacturing areas
- Fuel shortages and price changes
- Increased pressure to produce may result in quality decrease
- More new products increases the possibilities of defects and problems

Session Five: Responding to Risks

Once you have identified the risks and established their priority, you are ready to determine how you will respond. Did you encounter risks on your way to work recently? What were they? How important are they?

In this session, you'll learn to evaluate the risk in the context of the four T's, and decide how you will respond to them.

Risk Responses

There are generally four ways that you can respond to risks. The best risk response plans usually provide a few options, ranked in order of preference. – **The Four T's**

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 organisation 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.

Case Study: General Motors (Part Two)

BACKGROUND INFORMATION

General Motors (GM) has long been the world's number-one manufacturer of cars and trucks. Their brand line has included Buick, Cadillac, GMC, Chevrolet, Pontiac, and Saab. Their business model includes overseas operations such as Vauxhall and Opel, Hughes Electronics, Allison Transmission, and GM Locomotive. They also have stakes in other brands, including Isuzu, Subaru, Suzuki, Fiat, and Daewoo.

After years of a downward spiral in their market share, GM finally achieved two straight years of increase in 2002. In 2003, GM planned to continue this gain by launching 30 new gas-powered vehicles.

TASK

In the chart below, list the risks that you identified in Session Four. Then, outline one or more strategies to mitigate each of them.

	Tolerate	Treat	Transfer	Terminate
Risk One				
Risk Two				
Risk Three				

EXAMPLE

	Tolerate	Treat	Transfer	Terminate
Risk One (Emergence of Hybrids)	Do nothing and continue with existing plan	Add hybrids to line-up	Outsource production of new hybrids to another company	

Session Six: Resourcing Controls

Now you've identified some risks and decided how you will handle them. The next step is to take some action and improve the situation. What kinds of risks are you working with? Do you prefer to start big or small?

In this session, you'll learn about identifying and evaluating controls and what's needed to mitigate your risk.

Identifying and Evaluating Controls

Once a risk has been identified, and you have chosen to treat it, it's time to look at controls that can be put into place to mitigate the risk.

Possible controls can include:

- Re-allocating existing people or equipment
- Additional people
- New equipment
- Skills and training
- New information

Your evaluation should look at:

- Does the control meet laws and regulations?
- How well does each control mitigate the risk?
- What is the cost of the control vs. the implementation benefit?
- What is the sustainability of the control?
- What changes might have to be made to this control?
- What other effects will this control have?

Case Study: General Motors (Part Three)

BACKGROUND INFORMATION

General Motors (GM) has long been the world's number-one manufacturer of cars and trucks. Their brand line has included Buick, Cadillac, GMC, Chevrolet, Pontiac, and Saab. Their business model includes overseas operations such as Vauxhall and Opel, Hughes Electronics, Allison Transmission, and GM Locomotive. They also have stakes in other brands, including Isuzu, Subaru, Suzuki, Fiat, and Daewoo.

After years of a downward spiral in their market share, GM finally achieved two straight years of increase in 2002. In 2003, GM planned to continue this gain by launching 30 new gas-powered vehicles.

TASK

Choose one or more of your identified risks to treat. Identify what controls you could use to mitigate that risk.

Risk	Control

EXAMPLE

Emergence of Hybrids	• Create a team to monitor marketplace changes and trends. • Develop a facility to build the vehicles.

Session Seven: Reaction Planning

Are you someone who naturally considers different scenarios? Or are you more likely to jump in and see how things turn out? Neither approach is completely right or wrong; they simply represent different styles. ***This session*** you'll consider worst-case scenarios and contingency planning, an essential aspect to learning about managing risk.

The Worst-Case Scenario

You should build a contingency plan for each major risk that has been identified. What will you do if the risk does occur? The plan should detail the following elements.

WHEN

- How will we know when the risk will happen?
- What will alarms look like?
- When should we start acting?

WHO

- Who has responsibility for this risk?
- What other resources might they need?
- Who else should be informed?

WHAT

- What will happen when the risk occurs?
- What will we do when the risk happens? (Depending on the risk, this plan could be very detailed or very simple. A step-by-step, timed plan may be necessary.)
- What consequences could the risk have?
- What other risks might this event create?

WHERE

- Where is the risk going to happen?

BACKGROUND INFORMATION

General Motors (GM) has long been the world's number-one manufacturer of cars and trucks. Their brand line has included Buick, Cadillac, GMC, Chevrolet, Pontiac, and Saab. Their business model includes overseas operations such as Vauxhall and Opel, Hughes Electronics, Allison Transmission, and GM Locomotive. They also have stakes in other brands, including Isuzu, Subaru, Suzuki, Fiat, and Daewoo.

After years of a downward spiral in their market share, GM finally achieved two straight years of increase in 2002. In 2003, GM planned to continue this gain by launching 30 new gas-powered vehicles.

TASK

Choose one risk and outline a reaction plan.

Example: Outline a plan to create a facility to build hybrid cars.

Session Eight: Reporting and Monitoring

As with any business practice, we need to be familiar with reporting and monitoring functions in order to keep other people and management in touch with what is going on in the company.

In this session, you'll explore measuring, reporting, and monitoring as part of the risk management function.

The Reporting Structure

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

SARBANES-OXLEY ACT AND TURNBULL REPORT

The Sarbanes–Oxley Act of 2002 ... also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. A number of provisions of the Act also apply to privately held companies, such as the willful destruction of evidence to impede a federal investigation. The bill, which contains eleven sections, was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The sections of the bill cover responsibilities of a public corporation's board of directors, add criminal penalties for certain misconduct, and require the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law. (https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act)

Internal Control: Guidance for Directors on the Combined Code (1999) also known as the "Turnbull Report" was a report drawn up with the London Stock Exchange for listed companies. The committee which wrote the report was chaired by Nigel Turnbull of The Rank Group plc. The report informed directors of their obligations under the Combined Code with regard to keeping good "internal controls" in their companies, or having good audits and checks to ensure the quality of financial reporting and catch any fraud before it becomes a problem. (https://en.wikipedia.org/wiki/Turnbull_Report)

While the above mentioned regulations originated in the US and UK, the rest of the world takes guidance from them. It does not apply to all organisations. **Sarbanes-Oxley** will apply for financial institutions and those will be covered under **The Banking Act** and the **NBFIRA Act** in Botswana. The disclosure requirements within the acts will have taken guidance from **Sarbanes-Oxley**. **Turnbull** will apply to companies listed on the **BSE (Botswana Stock Exchange)** and those will be covered under the **BSE Act**. These are not specific risk-management regulations, but rather, risk management disclosures covered within these acts will have drawn from Sarbanes-Oxley and Turnbull. In accounting, there is also the King Report, which sets out guidelines on how accounting reports should be structured and what should be reported. It contains guidelines on how risk should be reported as well. It is an international standard.

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

Session Nine: Reviewing and Evaluating the Framework

Any time you are creating something new, it's helpful to step back and approach it from someone else's perspective to see if any elements need more explanation or extra detail.

In this session, you'll work with a review checklist and consider how to apply what you've learned when you get back to work.

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 organisations
- 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

Scaling the Program

Remember, the review should be proportionate to your organisation. If your organisation is small, an afternoon meeting to review your risk management program may be sufficient. For larger organisations, 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 organisation?

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

Session Ten: Personal Action Plan

Now that you have completed this course on **Risk Management**, how will you use the things you have learned? Creating a personal action plan can help you to stay on track, and on target. When you take responsibility for yourself and your results, you get things done.

In this session, you will be asked questions to help you plan your short-term and long-term goals. This final exercise is a way for you to synthesize the learning that you have done, and to put it into practice.

Starting Point

I am already doing these things well:

Where I Want to Go

I want to improve these areas:

I have these resources to help me:

How I Will Get There

	As a result of what I have learned in this workshop, I am going to…	My target date is…	I will know I have succeeded when…	I will follow up with myself on…
Objective 1				
Objective 2				
Objective 3				

Course Summary

Congratulations! You have completed the course "Risk Management."

In this course, we talked about using tools to assess situations or risks in the workplace. We started by exploring your risk tolerance, and then moved on to define risk and risk management as well as some key models for developing understanding.

Next, we started to get familiar with the seven R's and four T's of risk management. This included recognize and identify risks; rank and evaluate risks, respond with tolerating, training, transferring, or terminating; resource controls; reactions; report and monitor; and review.

With all this in mind, we moved on to a template for applying the risk assessment process, and an evaluation method to help determine the severity of the risk itself. Then we applied the template and evaluation techniques to a case study.

Next, we moved on to apply the four T's of tolerate, treat, transfer, and terminate in a little more detail by analysing some key considerations. We then learned how to identify and evaluate a range of controls, and again applied this to a case study.

To wrap things up, we learned about reporting and monitoring. We finished the course with information on reviewing and evaluating the template with a helpful checklist.

You should now feel ready to use risk management techniques and tools to accurately evaluate and manage risk in your workplace.

Recommended Reading List

If you are looking for further information on this topic, we have included a recommended reading list below.

"A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000." *The Institute of Risk Management.* 2010. http://www.theirm.org/documents/SARM_FINAL.pdf.

Committee of Sponsoring Organisations of the Treadway Commission. "Enterprise Risk Management - Integrated Framework (Executive Summary)." *Committee of Sponsoring Organisations of the Treadway Commission.* June 2017 https://www.coso.org/Pages/default.aspx

Committee of Sponsoring Organisations of the Treadway Commission. "Compliance Risk Management: Applying the COSO ERM Framework. *Committee of Sponsoring Organisations of the Treadway Commission.* November 2020 https://www.coso.org/Pages/default.aspx

Crouhy, Michel, Dan Galai, and Robert Mark. *The Essentials of Risk Management.* McGraw-Hill, 2005.

Hampton, John. *Fundamentals of Enterprise Risk Management.* AMACOM, 2009.

International Organisation for Standardization. *ISO 31000:2009.* 2009.

International Organisation for Standardization. *ISO Guide 73:2009.* 2009.

Project Management Institute. *A Guide to the Project Management Body of Knowledge (5th Edition)*. Project Management Institute, 2013.

