*Chapter 3.2*

# Risk Analysis

# Aim

To equip students with the concept of Risk analysis and its various methods, qualitative and quantitative risk analysis

# Instructional Objectives

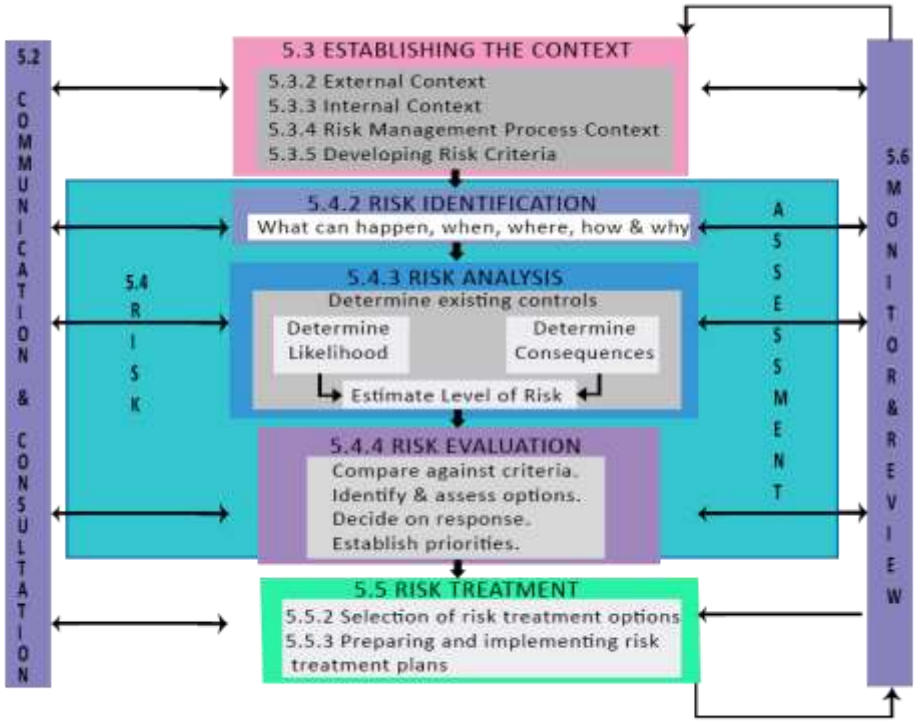
After completing this chapter, you should be able to:

- Explain Risk analysis
- Outline various risk analysis methods
- Elaborate on qualitative and quantitative risk analysis
- Describe Risk-IT Framework of ISACA

# Risk Analysis

# Meaning of Risk Management

Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk.



# Steps in Risk Analysis

- Determine the existing controls
- Determine Likelihood of risk
- Determine the Consequences
- Estimate the Level of risk

# Quiz / Assessment

1) Under which phase does ‘Estimating the level’ come in the risk management process?
   a. Risk Identification
   b. Risk Analysis
   c. Risk Treatment
   d. Risk Evaluation

# Quiz / Assessment

2) The 4 steps in Risk analysis are determining the existing controls, the risk likelihood, the risk consequences and _____.
   a. Establishing internal context
   b. Establishing external context
   c. Decide on the response
   d. Estimate the Level of risk

# Quiz / Assessment

3) Based on the Risk analysis methodology adopted, the _____is determined.
   a. Level of risk
   b. Degree of risk
   c. Parameters of risk
   d. Analysis of risk

# Risk Analysis Methods

# Risk Analysis Methods

- Qualitative risk analysis
- Quantitative risk analysis
- Pseudo Quantitative Risk Analysis

# Publicly Available Risk Assessment Standards

| | | |
|---|---|---|
| ISO / IEC 31000:2009 – Risk Management standard | ISO / IEC 31010:2009 – Risk Management – Risk Assessment Techniques | NIST 800 – 39 – Managing Information Security Risk |
| NIST 800 –30 – Guide for conducting Risk Assessments | COBIT 5 for Risk | COSO Enterprise Risk Management |

# Qualitative and Quantitative Analysis

# Qualitative Risk Analysis

- This is more subjective in nature.
- It is scenario based
- The assessor will answer “What-if” types of questions for the various threat and vulnerability scenarios.
- No numerical values will be associated.

# Quantitative Risk Analysis

All the assets and components are associated with numerical and their potential losses.

All elements viz., asset value, threat frequency, efficiency of security and safeguards, cost of implementing security and safeguards, uncertainty and probability will be associated with a value.

# Quiz / Assessment

4) Which are the three main Risk Analysis Methodologies?
   a. Qualitative Risk Analysis, Quantitative Risk Analysis and Pseudo Qualitative Risk Analysis
   b. Qualitative Risk Analysis, Quantitative Risk Analysis and Pseudo Quantitative Risk Analysis
   c. Risk IT, COBIT Risk, ISO 31000 and ISO 31010
   d. Risk Matrix, Risk Rating, Risk Number and Risk Priority

# Quiz / Assessment

5) Which of the following is the ISO Standard for Risk Management?
   a. ISO 27000 : 2013
   b. ISO 9001: 2015
   c. ISO 27001 : 2013
   d. ISO 31000: 2009

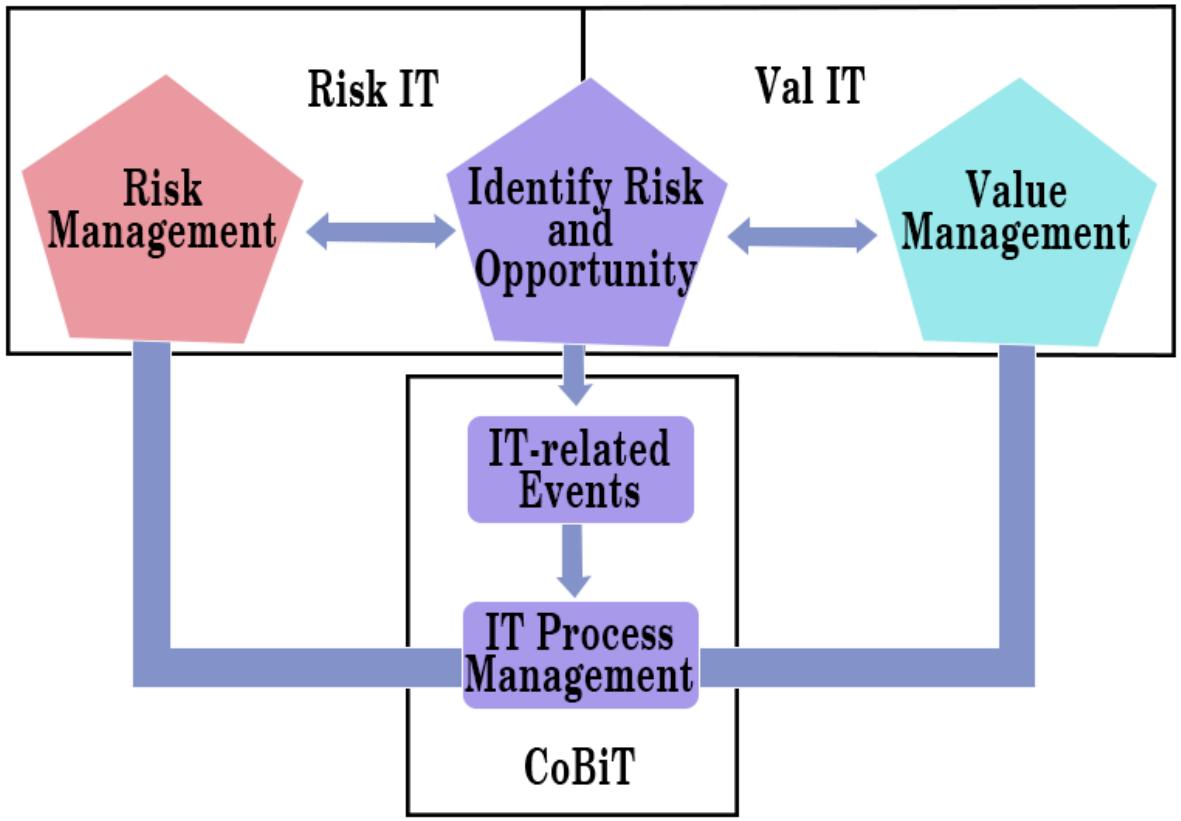
# Quiz / Assessment

6) The ISO 31000: 2009 is a certification standard. This statement is
   a. True
   b. False

# Risk-IT Framework of ISACA

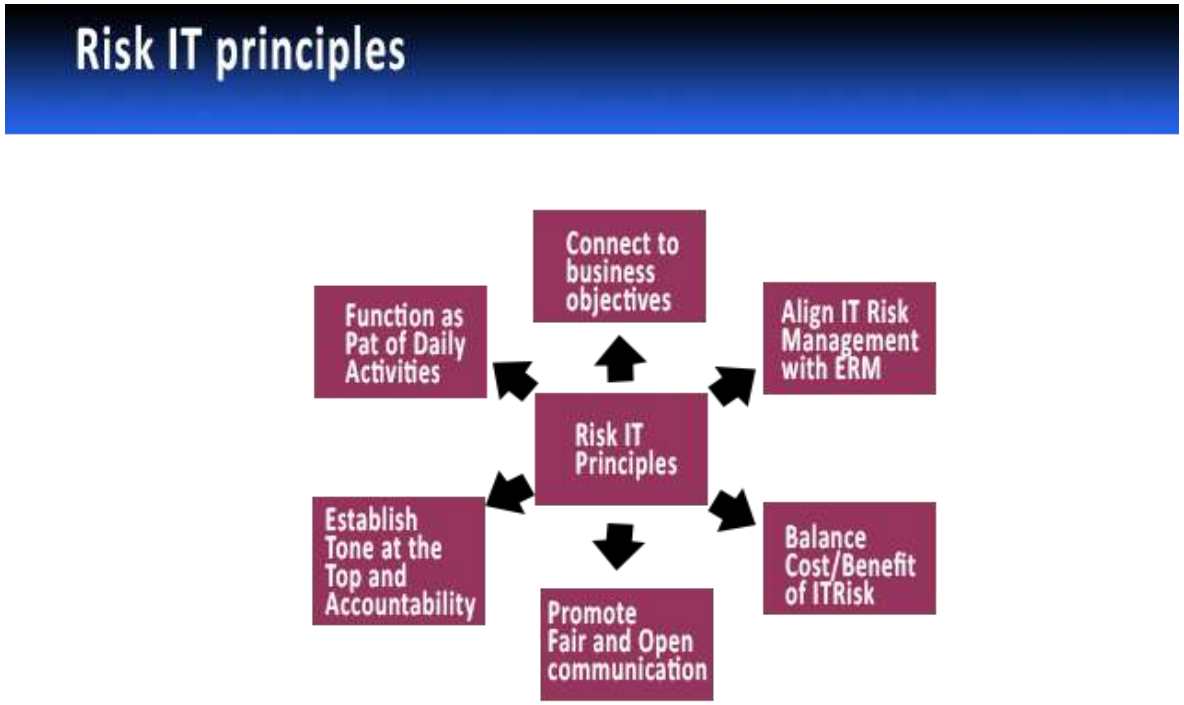
# Risk-IT

Risk IT is a framework through which companies can identify, manage and govern IT Risks.



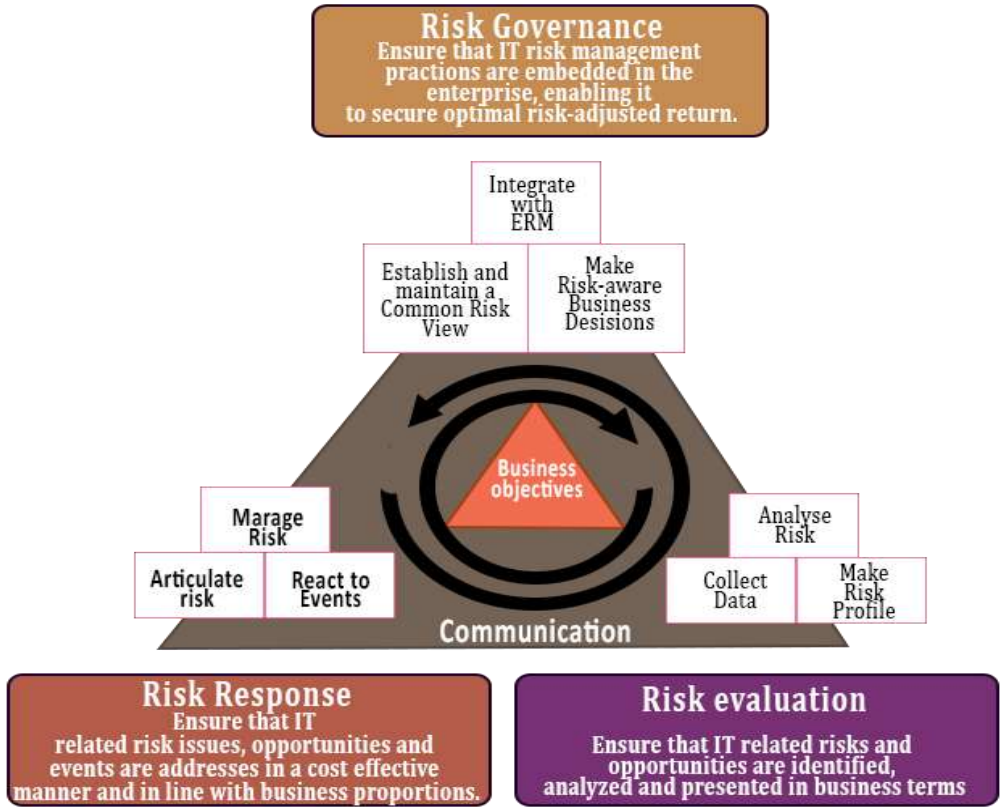
# RISK IT Principles

Risk IT is built on the following principles



# RISK IT Domains and Processes

The Risk management process in Risk IT has nine different processes.



# Quiz / Assessment

7) Risk IT is _____.
   a. A framework for Risk Management and governance
   b. A standard devised by the ISO
   c. A NIST standard
   d. A standard developed in response to FISMA

# Quiz / Assessment

8) Which domain involves identification, analysis and presentation of the IT risk in terms of business?
   a. Risk evaluation
   b. Risk identification
   c. Risk enhancement
   d. Risk management

# Quiz / Assessment

9) _____ is a framework through which companies can identify, manage and govern IT Risks.

a. COBIT
b. Risk
c. Risk IT
d. FISMA

# Quiz / Assessment

1) Explain the Risk Assessment Methodology – FMEA with an example.
2) Explain the purpose of the three domains in Risk IT.
3) Describe the Risk IT principles.

# Activity

## Online Activity

**Online Activity**
**(45 min)**

- Do an online research on Risk-IT Framework of ISACA and write an article on risk management frameworks.

*Note: Refer Table of Content for the activities*

# Summary

- Risk analysis is used to understand the nature, sources, and causes of the risks that are identified and to estimate the level of risk.
- Risk analysis is used to study impacts and consequences and to examine the controls that currently exist.
- The foremost publicly available standards and guidelines for implementing Risk Management are:
  - ISO / IEC 31000:2009 – Risk Management standard
  - ISO / IEC 31010:2009 – Risk Management – Risk Assessment Techniques
  - NIST 800 – 39 – Managing Information Security Risk
  - NIST 800 –30 – Guide for conducting Risk Assessments
  - COBIT 5 for Risk
  - COSO Enterprise Risk Management

# Summary

- Quantitative Risk Analysis is objective in nature and based on metrics. It involves complex calculations and hence requires a lot of time and effort.
- Qualitative Risk Analysis extremely subjective. This is a simpler methodology as there are no complex calculations involved.
- There are different risk assessment methodologies that can be used to perform risk assessment. They are: Asset Audit, Pipeline Model, HAZOP – Hazard and Operability Procedure.
- Failure Mode and Effects Analysis (FMEA) is one of the most structured systematic techniques for failure analysis.
- The different modes of FMEA are - Functional, Design and Process FMEA. Sometimes FMEA is extended to include criticality analysis and called FMECA.
- Organisations can identify, manage and govern IT Risks via Risk IT is a framework.

# e-References


- *The Risk IT Framework*. Retrieved 2009, from http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf
- Risk Assessment Tools-A-primer. Retrieved 2003, from http://www.isaca.org/Journal/archives/2003/Volume-2/Pages/Risk-Assessment-Tools-A-Primer.aspx
- https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwi3_uW6-N_KAhUDTY4KHfxWB9MQFghEMAU&url=http%3A%2F%2Fwww.isaca.org%2FKnowledge-Center%2FRisk-IT-IT-Risk-Management%2FDocuments%2FRiskIT-Overview--6Jan10.ppt&usg=AFQjCNF4FkLPZY7jtbfki4VVBuBJo-5k1A&sig2=wCIAQtEkEql2QtI0AtIXPQ

# External Resource


- Weill, P. & Ross, J. (2004). *IT governance*. Boston: Harvard Business School Press.
- Harkins, M. (2013). *Managing risk and information security*. [New York]: Apress.
- Peltier, T. (2010). *Information security risk analysis, third edition*. Boca Raton, Fla.: CRC Press.