University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

PSIT302 & PSIT3P2 – Information Security Management (ISM)

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

Unit I – Survey of Risk Management Practices

- Comparing Approaches to Risk Management
  - Reactive Approach
  - Proactive Approach
- Approaches to Risk Prioritization
  - Quantitative
  - Qualitative

Unit I : Comparing Approaches to Risk Management

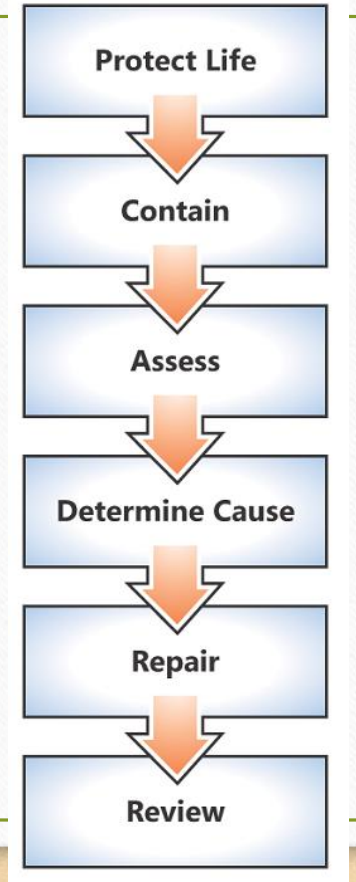
- Many organizations are introduced to security risk management by the necessity of responding to a relatively small security incident.
- As more and more issues relating to security arise and begin to impact the business, many organizations get frustrated and want an alternative to this reactive approach
- Where reactive approach can be used once the incident takes place
- Alternative is Proactive Approach

Unit I : Comparing Approaches to Risk Management – Reactive Approach

- A reactive approach can be an effective tactical response to security risks that have been exploited and turned into security incidents
- Alternatively imposing a small degree of rigor to the reactive approach can help organizations of all types to better use their resources.
- Recent security incidents may help an organization to predict and prepare for future problems

Unit I : Comparing Approaches to Risk Management – Reactive Approach

- Following six steps when you respond to security incidents can help you manage them quickly and efficiently



Unit I : Comparing Approaches to Risk Management – Proactive Approach

- Making plans to protect your organization's important assets by implementing controls that reduce the risk of vulnerabilities being exploited by malicious software, attackers, or accidental misuse.
- An effective proactive approach can help organizations to significantly reduce the number of security incidents that arise in the future, but it is not likely that such problems will completely disappear.
- Therefore, organizations should continue to improve their incident response processes while simultaneously developing long-term proactive approaches.

Unit I : Comparing Approaches to Risk Management – Proactive Approach

- Each of the security risk management methodologies shares some common high-level procedures:
  - Identify business assets.
  - Determine what damage an attack against an asset could cause to the organization.
  - Identify the security vulnerabilities that the attack could exploit.
  - Determine how to minimize the risk of attack by implementing appropriate controls.

Unit I : Approaches to Risk Prioritization

- There are many different methodologies for prioritizing or assessing risks, but most are based on one of two approaches or a combination of the two: quantitative risk management or qualitative risk management.
- Quantitative Risk Assessment
  - In quantitative risk assessments, the goal is to try to calculate objective numeric values for each of the components gathered during the risk assessment and cost-benefit analysis.
  - For example, you estimate the true value of each business asset in terms of what it would cost to replace it, what it would cost in terms of lost productivity, what it would cost in terms of brand reputation, and other direct and indirect business values.

Unit I : Approaches to Risk Prioritization
Quantitative Risk Assessment

- Valuing Assets
  - The overall value of the asset to your organization

  - The immediate financial impact of losing the asset.
  - The indirect business impact of losing the asset
- Determining the SLE (Single Loss Expectancy)
- Determining the ARO (Annual Rate of Occurrence)
- Determining the ALE (Annual Loss Expectancy)
- Determining Cost of Controls
- ROSI (Return On Security Investment) = (ALE before control) – (ALE after control) – (annual cost of control)

Unit I : Approaches to Risk Prioritization Quantitative Risk Assessment

Results of the Quantitative Risk Analyses

- The input items from the quantitative risk analyses provide clearly defined goals and results. The following items generally are derived from the results of the previous steps:
  - Assigned monetary values for assets
  - A comprehensive list of significant threats
  - The probability of each threat occurring
  - The loss potential for the company on a per-threat basis over 12 months
  - Recommended safeguards, controls, and actions

Unit I : Approaches to Risk Prioritization
Qualitative Risk Assessment

- In Quantitative, organizations do not try to assign hard financial values to assets, expected losses, and cost of controls. you calculate relative values.
- Risk analysis is usually conducted through a combination of questionnaires and collaborative workshops
- Involves people from a variety of groups within the organization such as information security experts; information technology managers and staff; business asset owners and users; and senior managers.

Unit I : Approaches to Risk Prioritization
Qualitative Risk Assessment

- The benefits of a qualitative approach are that it overcomes the challenge of calculating accurate figures for asset value, cost of control, and so on, and the process is much less demanding on staff.
- Qualitative risk management projects can typically start to show significant results within a few weeks, whereas most organizations that choose a quantitative approach see little benefit for months, and sometimes even years, of effort.
- The drawback of a qualitative approach is that the resulting figures are vague;
- Some Business Decision Makers (BDMs), especially those with finance or accounting backgrounds, may not be comfortable with the relative values determined during a qualitative risk assessment project.

	Quantitative	Qualitative
Benefits	• Risks are prioritized by financial impact; assets are prioritized by financial values. • Results facilitate management of risk by return on security investment. • Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage). • Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	• Enables visibility and understanding of risk ranking. • Easier to reach consensus. • Not necessary to quantify threat frequency. • Not necessary to determine financial values of assets. • Easier to involve people who are not experts on security or computers.
Drawbacks	• Impact values assigned to risks are based on subjective opinions of participants. • Process to reach credible results and consensus is very time consuming. • Calculations can be complex and time consuming. • Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. • Process requires expertise, so participants cannot be easily coached through it.	• Insufficient differentiation between important risks. • Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis. • Results are dependent upon the quality of the risk management team that is created.