UNIT – 1

Q.1 Explain the process of risk management.

Ans: Risk management is the identification, assessment, and prioritization of risks.

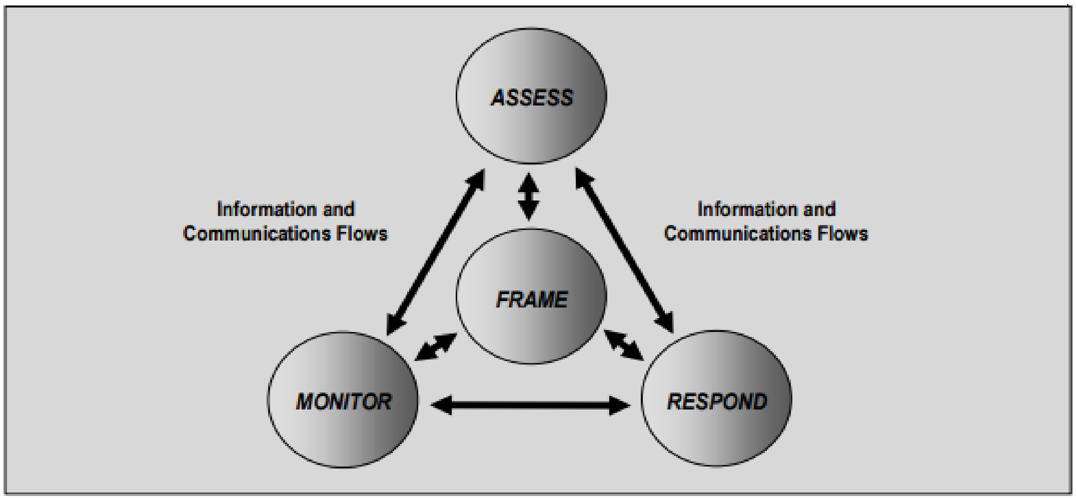
Risk management processes include:

(I) framing risk

(ii) Assessing risk

(iii) Responding to risk

(iv) Monitoring risk.


ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

1. Framing Risk

- The first component of risk management process is **Framing risk**.
- This phase describes the environment in which risk-based decisions are made.
- The purpose of this phase is to produce the risk management strategy such as how organizations plans to assess risk, respond to risk and monitoring risk.
- This risk management strategy establishes a foundation for managing risk and describes the boundaries on which risk-based decisions are taken within organizations.

2. Assessing Risk

- The second component of risk management process is **Assessing risk**.
- The purpose of this phase is to identify threats to organizations, internal and external vulnerabilities to organizations, the harm occur because of threats and vulnerability in the organization and likelihood that harm will occur.
- The end result is a determination of risk.

3. Responding to risk

- The third component of risk management process is **responding to risk**.
- This phase describe how organizations respond to risk once that risk is determined based on the results of a risk assessment.
- The purpose of this phase is to provide consistency and organization wide response to the risk that is frame by organization.

4. Monitoring risk

- The fourth component of risk management process is **Monitoring risk**.
- The purpose of this phase is to monitor the ongoing effectiveness of risk response, identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

Q.2 what are the steps for risk assessment?

Ans:

- The risk assessment component of risk management—providing a step-by-step process for organizations on:
  (I) how to prepare for risk assessments
  (ii) How to conduct risk assessments
  (iii) How to communicate risk assessment results to key organizational personnel
  (iv) How to maintain the risk assessments over time.
- Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks.
- Organizations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy.
- The frequency of the risk assessments and the resources applied during the assessments, commensurate (equal) with the expressly defined purpose and scope of the assessments.
- Risk assessments address the potential adverse impacts to organizational operations and assets, individuals, other organizations that arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems.

Q.3 what are steps to Prepare for a risk assessment?

Ans: There are four step to prepare risk assessment are as follows:

(I) how to prepare for risk assessments
(ii) How to conduct risk assessments
(iii) How to communicate risk assessment results to key organizational personnel

(iv) How to maintain the risk assessments over time.

Q.4 what are the different risk assessment approaches?

Ans:

- A specific assessment approach can be selected based on organizational culture and attitudes toward the concepts of uncertainty and risk communication.
- There are three different risk assessment approaches such as quantitatively, qualitatively, or semi-quantitatively.

1. **Quantitative Assessments**
   - Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers.
   - This type of assessment most effectively supports cost-benefit analyses of alternative risk responses.
   - However, the meaning of the quantitative results may not always be clear and may require interpretation and explanation to explain the assumptions and constraints of u the results.
   - For example, organizations may typically ask if the numbers or results obtained in the risk assessments are reliable or if the differences in the obtained values are meaningful or insignificant.
2. **Qualitative Assessments**
   - Qualitative assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories such as very low, low, moderate, high, very high).
   - This type of assessment supports communicating risk results to decision makers.
   - In most cases the range of values in qualitative assessments is comparatively small, so making the relative prioritization or comparison within the set of reported risks difficult.
   - The repeatability and reproducibility of qualitative assessments are increased by the annotation (addition) of assessed values.
3. **Semi-Quantitative Assessments**
   - Semi-quantitative assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts.
   - This type of assessment can provide the benefits of both quantitative and qualitative assessments.
   - The bins or scales translate easily into qualitative terms that support risk communications for decision makers while also allowing relative comparisons between values in different bins or even within the same bin.

- The role of expert judgment in assigning values is more evident than in a purely quantitative approach.

Q.5 what are the different risk analysis approaches?

Ans:

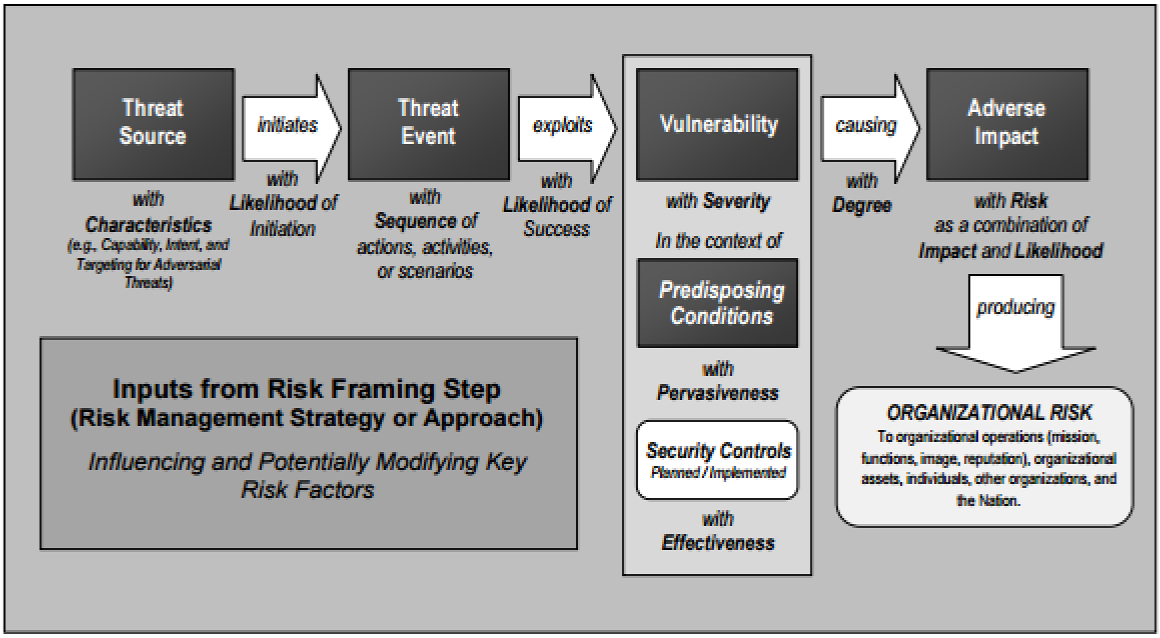
- Analysis approaches differ on the bases of starting point of the risk assessment and level of detail in the assessment.
- An different analysis approach can be : (I) Threat-oriented (ii) Asset/Impact-oriented (iii) Vulnerability oriented
- A threat-oriented approach identify threat sources and threat events, and focuses on the development of threat scenarios.
- A vulnerabilities are identified in the presence of threats, and for adversarial threats, impacts are identified based on adversary intent.
- Asset/impact-oriented approach identify the impacts or consequences of critical assets.
- A vulnerability can occur because of weaknesses and deficiencies in organizational information systems or the environments in which the systems operates.
- In addition to the of the analysis approach, organizations can apply more rigorous analysis techniques such as graph-based analysis.
- Graph-based analysis provide an many-to-many relationships between:
  (I) Threat sources and threat events i.e., a single threat event can be caused by multiple threat sources and a single threat source can cause multiple threat events
  (ii) Threat events and vulnerabilities i.e. a single threat event can exploit multiple vulnerabilities and a single vulnerability can be exploited by multiple threat events.
  (iii) Threat events and impacts/assets i.e., a single threat event can affect multiple assets or have multiple impacts, and a single asset can be affected by multiple threat events.
- Graph-based analysis provide ways to use specific threat events to generate threat scenarios.
- Graph-based analysis techniques can also provide ways to account for situations in which one event can change the likelihood of occurrence for another event.

Q.6 Explain generic risk model in detail.

Ans:

- Risk models define the risk factors and the relationships among those factors.
- Risk factors in risk models used as inputs to determining levels of risk in risk assessments.
- Risk factors are also used in risk communications to determine strongly effects of levels of risk in particular situations.

- Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition.


Threat Source
initiates
with Likelihood of Initiation
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
exploits
with Likelihood of Success
with Sequence of actions, activities, or scenarios
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step (Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

- **Threats**
  - A threat is an event which produce adversely impact on organizational operations and assets, individuals, other organizations.
  - Threats decomposed into two parts such as threat sources and threat events.
  - Threat sources include: (I) Hostile cyber or physical attacks (ii) human errors of omission (iii) structural failures of organization-controlled resources (IV) natural and man-made disasters, accidents, and failures beyond the control of the organization.
  - Threat events are caused by threat sources.
- **Vulnerabilities and Predisposing Conditions**
  - A vulnerability is a weakness in an information system, system security procedures, and internal controls.
  - Most information system vulnerabilities can be associated with security controls that either have not been applied or have been applied, but retain some weakness.
  - Vulnerabilities are not identified only within information systems. Vulnerabilities can be found in organizational governance structures such as lack of effective risk management strategies, poor intra-agency communications, and inconsistent decisions about business functions.

  - A predisposing condition is a condition that exists within an organization, a mission or business process, enterprise architecture, information system or environment of operation, which increases or decreases the likelihood of threat events.
  - Vulnerabilities resulting from predisposing conditions that cannot be easily corrected.

- **Likelihood**
  - The likelihood is a weighted risk factor based on an analysis of given threat and it is capable of identifying set of vulnerabilities.
  - Likelihood is typically based on: (I) adversary intent (ii) adversary capability (iii) adversary targeting.
  - The likelihood of threat occurrence can also be based on the state of the organization
  - Such as enterprise architecture, information security architecture, information systems, and environments in which those systems operate.
- **Impact**
  - The level of impact from a threat event is the result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
  - Impact can be experienced by a variety of organizational and non-organizational stakeholders including heads of agencies, mission and business owners, information owners, mission/business process owners, information system owners, or individuals/groups in the public or private sectors.

Q.7 what are the key characteristics of OCTAVE approach?

Ans:

- OCTAVE is a risk based assessment and planning technique for security.
- OCTAVE is self-directed means people from an organization assume responsibility for setting the organization’s security strategy.
- The technique influence people’s knowledge of their organization’s security-related practices and processes to capture the current state of security practice within the organization.

- **Key- characteristics of OCTAVE approach**
  - OCTAVE is an asset-driven evaluation approach that provide functionality are as follows:

- Identify information-related assets such as information and systems)that are important to the organization
- Focus risk analysis activities on those assets and identify the most critical asset in the organization.
- Consider the relationships among critical assets, the threats to those assets, and vulnerabilities that can expose assets to threats.

- OCTAVE is organized around these three basic aspects that are

1. Build Asset-Based Threat Profiles

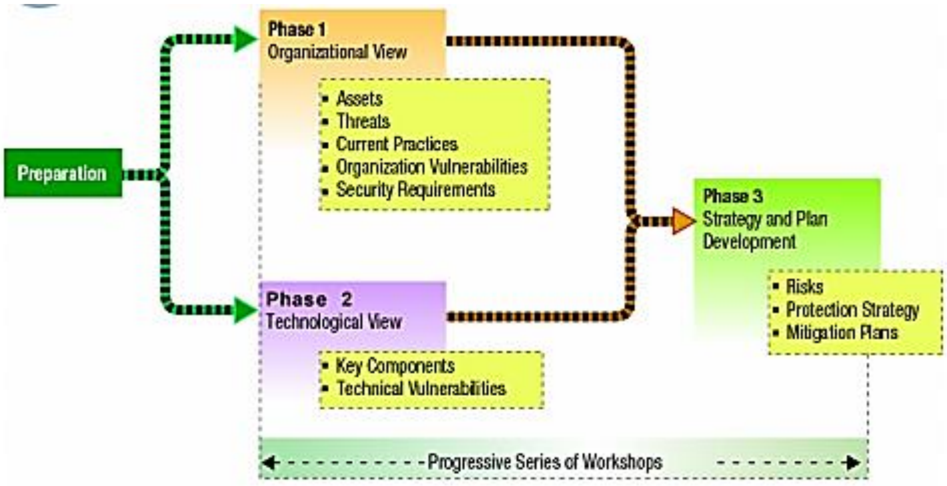
- This is an organizational evaluation. The analysis team determines what is important to the organization and what is currently being done to protect those assets.
- The team then selects those assets that are most important to the organization and describes security requirements for each critical asset.
- Finally, it identifies threats to each critical asset and creates the threat profile for that asset.

2. Identify Infrastructure Vulnerabilities

- This is an information infrastructure evaluation. The analysis team examines network access paths, identifying classes of information technology i.e. related to each critical asset.
- The team then determines the extent to which resistant to the network attacks.

3. Develop Security Strategy and Plans

- During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides how to protect them.
- The team creates a protection strategy for the organization and plans to address the risks to the critical assets, based upon an analysis of the information gathered.



Q.8 Explain reactive approach to Risk management with proper diagram.

Ans:

- A reactive approach can be an effective tactical response to security risks that have been exploited and turned into security incidents
- The reactive approach can help organizations to better use their resources.
- Recent security incidents may help an organization to predict and prepare for future problems.
- The following six steps when you respond to security incidents can help you manage them quickly and efficiently:

1. Protect human life and people's safety

- This should always be your first priority.
- For example, if affected computers include life support systems, shutting them off may not be an option; perhaps you could logically isolate the systems on the network by reconfiguring routers and switches without disrupting their ability to help patients.

2. Contain the damage

- Containing the harm that the attack caused helps to limit additional damage. Protect important data, software, and hardware quickly.
- Minimizing disruption of computing resources is an important consideration, but keeping systems up during an attack may result in greater and more widespread problems.
- For example, if you contract a worm in your environment, you could try to limit the damage by disconnecting servers from the network. However, sometimes disconnecting servers can cause more harm than good.

- Use your best judgment and your knowledge of your own network and systems to make this determination.

3. Assess the damage

- We should begin to determine the extent to which damage that the attack caused then we contain the situation. Immediately make a duplicate of the hard disks in any servers that were attacked and put those aside for forensic use later.
- It is important so that you can restore the organization's operations as soon as possible while preserving a copy of the hard disks for investigative purposes.
- We should implement a contingency plan so that normal business operations and productivity can continue.

4. Determine the cause of the damage

- It is necessary to understand the resources at which the attack was aimed and what vulnerabilities were exploited to gain access or disrupt services.
- Review the system configuration, patch level, system logs, audit logs, and audit trails on both the systems that were directly affected as well as network devices that route traffic to them.
- These reviews often help you to discover where the attack originated in the system and what other resources were affected.

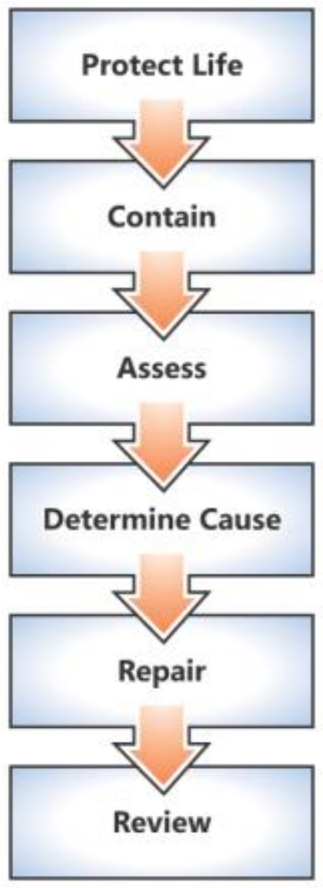
5. Repair the damage

- It is very important that the damage be repaired as quickly as possible to restore normal business operations and recover data lost during the attack.
- The organization's business continuity plans and procedures should cover the restoration strategy.
- The incident response team should also be available to handle the restore and recovery process.
- During recovery, contingency procedures are executed to limit the spread of the damage and isolate it.

6. Review response and update policies

- After the documentation and recovery phases are complete, we should review the process thoroughly.

- Determine with our team the steps that were executed successfully and what mistakes were made.
- In almost all cases, we will find that our processes need to be modified to allow you to handle incidents better in the future.



Q.9 Explain proactive approach to risk management. What are the benefits over reactive approach?

Ans:

- Instead of waiting for bad things to happen and then responding to them afterwards, you minimize the possibility of the bad things ever occurring in the first place.
- You make 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.
- Security risk management methodologies shares some common high-level procedures:

  1. Identify business assets.

  2. Determine what damage an attack against an asset could cause to the organization.

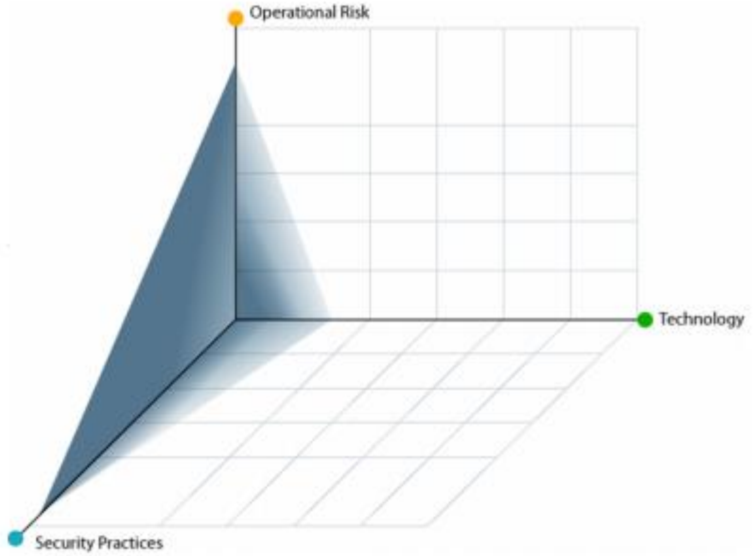
  3. Identify the security vulnerabilities that the attack could exploit.

  4. Determine how to minimize the risk of attack by implementing appropriate controls.

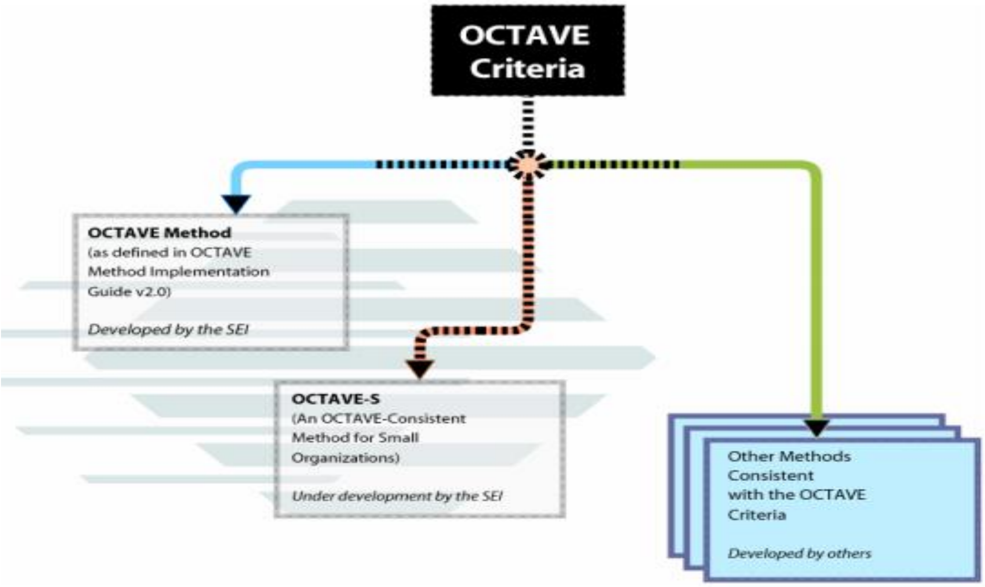
Q.10 Write a short note on OCTAVE

Ans:

- OCTAVE is a risk based assessment and planning technique for security.
- OCTAVE is self-directed means people from an organization assume responsibility for setting the organization's security strategy.
- The technique influence people's knowledge of their organization's security-related practices and processes to capture the current state of security practice within the organization.
- OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues.
- It is a flexible evaluation that can be tailored for most organizations.
- When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization.
- OCTAVE balancing the three key aspects such as operational risk, security practices, and technology.



- There are three types of criteria for OCTAVE method:
  OCTAVE methodology is very extensive, which ensures detailed data verification. However, an in depth analysis of resources is not always necessary. For such cases, **OCTAVE-S** has been developed. It is used in small or medium sized companies (employing not more than 100 people).
  Other method consistent with OCTAVE criteria


OCTAVE Criteria
OCTAVE Method
(as defined in OCTAVE Method Implementation Guide v2.0)
Developed by the SEI
OCTAVE-S
(An OCTAVE-Consistent Method for Small Organizations)
Under development by the SEI
Other Methods Consistent with the OCTAVE Criteria
Developed by others

Q.11.What are the various domains & corresponding processes of COBIT?

Ans: There are four types of domain are as follows:

- Plan & Organize (PO)
- Acquire & Implement (AI)
- Deliver & Support (DS)
- Monitor & Evaluate (ME)

1. Plan & Organize (PO)

- This domain have following processes:
- PO1 Define a Strategic IT Plan and direction
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment (ITIL related: Financial Management for IT Services)
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks PO10 Manage Projects

2. Acquire & Implement (AI)

- This domain have following processes:
  - AI1 Identify Automated Solutions
  - AI2 Acquire and Maintain Application Software
  - AI3 Acquire and Maintain Technology Infrastructure
  - AI4 Enable Operation and Use
  - AI5 Procure IT Resources
  - AI6 Manage Changes (ITIL related: Change Management)
  - AI7 Install and Accredit Solutions and Changes (ITIL related: Release Management)

3. Deliver & Support (DS)

- This domain have following processes:
  - DS1 Define and Manage Service Levels (ITIL related: Service Level Management)
  - DS2 Manage Third-party Services
  - DS3 Manage Performance and Capacity (ITIL related: Capacity Management)
  - DS4 Ensure Continuous Service (ITIL related: IT Service Continuity Management)
  - DS5 Ensure Systems Security (ITIL related: Security Management)

- DS6 Identify and Allocate Costs (ITIL related: Financial Management for IT Services)
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents (ITIL related: Incident Management)
- DS9 Manage the Configuration (ITIL related: Configuration Management)
- DS10 Manage Problems (ITIL related: Problem Management)
- DS11 Manage Data (ITIL related: Availability Management)
- DS12 Manage the Physical Environment
- DS13 Manage Operations

4. Monitor & Evaluate (ME)

- ME1 Monitor and Evaluate IT Processes
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Regulatory Compliance
- ME4 Provide IT Governance

Q. 13 Explain with diagram OCTAVE method.

Ans:

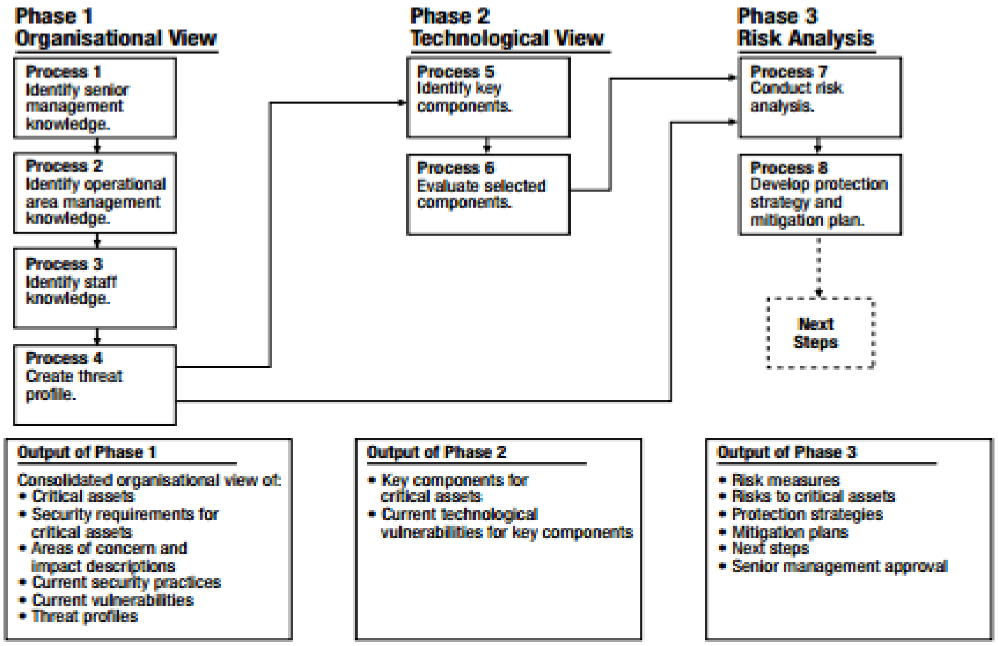
- The OCTAVE Method was developed with large organizations across 300 employees or more.
- Size is not the only consideration when deciding to use the OCTAVE Method.
- The OCTAVE Method comprises the three phases required by the OCTAVE criteria.
- The processes in those phases are described are as follows:

➢ **Phase 1: Build Asset-Based Threat Profiles**

  - This phase are gather information across the organization and defining threat profiles for critical assets.
  - Process 1: Identify Senior Management Knowledge – The analysis team collects information about important assets, security requirements, threats and vulnerabilities from a representative set of senior managers.
  - Process 2: Identify Operational Area Knowledge – The analysis team collects information about important assets, security requirements, threats, and vulnerabilities from managers of selected operational areas.
  - Process 3: Identify Staff Knowledge– The analysis team collects information about important assets, security requirements, threats and vulnerabilities from general staff and IT staff members of the selected operational areas.

- Process 4: Create Threat Profiles – The analysis team selects three to five critical information-related assets and defines the threat profiles for those assets.

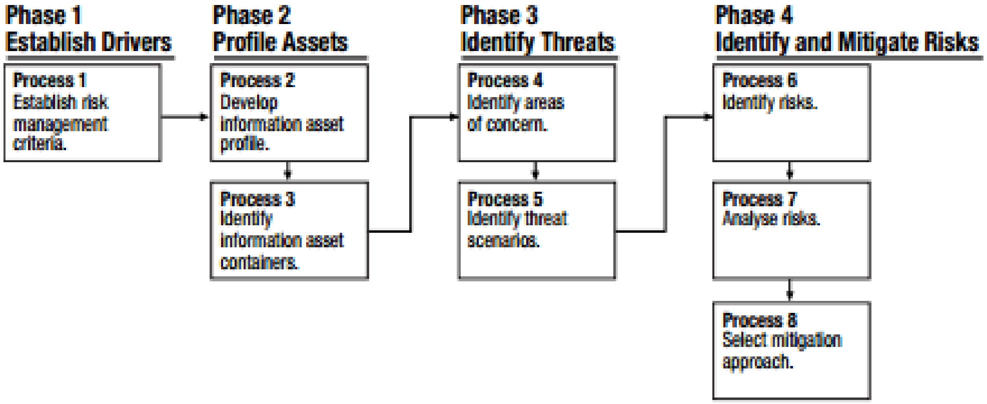
- **Phase 2: Identify Infrastructure Vulnerabilities**
  - During this phase, the analysis team evaluates key components that supports for technological vulnerabilities.
  - Process 5: Identify Key Components – A set of key components from the systems that support to identify critical information-related assets
  - Process 6: Evaluate Selected Components – Tools are run to evaluate the selected components, and the results are analyzed to refine the threat profiles for the critical assets.
- **Phase 3: Develop Security Strategy and Plans**
  - The primary purpose of this phase is to evaluate risks to critical assets and develop an organizational protection strategy and risk mitigation plans.
  - Process 7: Conduct Risk Analysis – An organizational set of evaluation criteria are defined to determining the threats to critical assets.
  - Process 8: Develop Protection Strategy – The team develops an organization-wide protection strategy that improving the organization’s security practices as well as mitigation plans to reduce the important risks to critical assets.


Phase 1
Organisational View
Process 1
Identify senior management knowledge.
Process 2
Identify operational area management knowledge.
Process 3
Identify staff knowledge.
Process 4
Create threat profile.
Phase 2
Technological View
Process 5
Identify key components.
Process 6
Evaluate selected components.
Phase 3
Risk Analysis
Process 7
Conduct risk analysis.
Process 8
Develop protection strategy and mitigation plan.
Next Steps
Output of Phase 1
Consolidated organisational view of:
• Critical assets
• Security requirements for critical assets
• Areas of concern and impact descriptions
• Current security practices
• Current vulnerabilities
• Threat profiles
Output of Phase 2
• Key components for critical assets
• Current technological vulnerabilities for key components
Output of Phase 3
• Risk measures
• Risks to critical assets
• Protection strategies
• Mitigation plans
• Next steps
• Senior management approval

Q.14 Explain with diagram OCTAVE allegro.

Ans:

- The OCTAVE Allegro approach comprises eight processes and is organized into four phases:
- **Phase 1: Establish drivers**—the organization develops risk measurement criteria consistent with organizational drivers.
- **Phase 2: Profile assets**—Information assets that are determined to be critical are identified and profiled. This profiling process establishes clear boundaries for the asset; identifies its security requirements; and identifies all of the locations where the asset is stored, transported or processed.
- **Phase 3: Identify threats**—Threats to critical information assets are identified in the context of the locations where the asset is stored, transported or processed.
- **Phase 4: Identify and mitigate risks**—Risks to information assets are identified and analyzed and the develop the mitigation approaches.


Phase 1
Establish Drivers
Process 1
Establish risk management criteria.
Phase 2
Profile Assets
Process 2
Develop information asset profile.
Process 3
Identify information asset containers.
Phase 3
Identify Threats
Process 4
Identify areas of concern.
Process 5
Identify threat scenarios.
Phase 4
Identify and Mitigate Risks
Process 6
Identify risks.
Process 7
Analyse risks.
Process 8
Select mitigation approach.

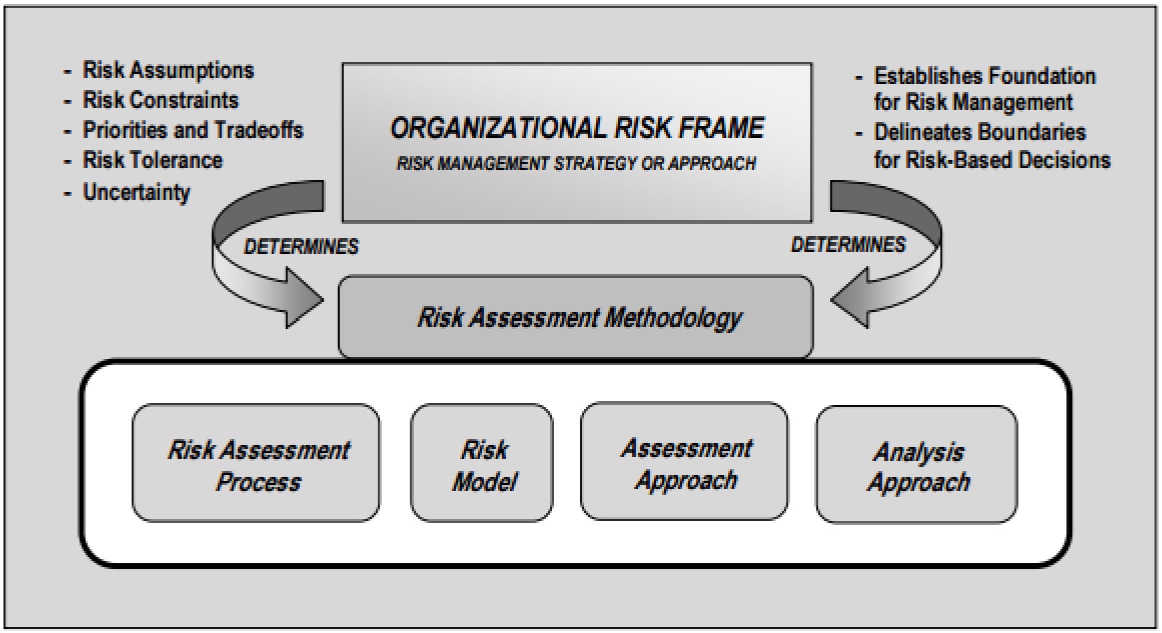
Q.15 What are the various risk framing components & explain relationship among them?

Ans:

- Organizations can use a single risk assessment methodology or can employ multiple assessment methodologies.
- Organization risk frame determines the various Risk Assessment methodology such as Risk Assessment Process, Risk Model, Assessment Approach, and Analysis Approach.
- The selection of a specific methodology depending on following factor
  (I) the time frame for investment planning or for planning policy changes.
  (ii) The complexity/maturity of organizational mission/business processes.

(iii) The phase of the information systems in the system development life cycle
(iv) The criticality/sensitivity of the information and information systems supporting the core organizational missions/business functions.

- **Risk Assessment Process**
  Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks.
- **Risk Model**
  Risk models define the risk factors to be assessed and determine the level of risk in risk assessment.
- **Assessment Approach**
  An assessment approach can be selected based on organizational culture and attitudes toward the concepts of uncertainty and risk communication. There are three assessment approach such as quantitatively, qualitatively, or semi-quantitatively.
- **Analysis Approach**
  Analysis approaches differ with respect to the starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated. An analysis approach can be: (I) threat-oriented; (ii) asset/impact-oriented; or (iii) vulnerability oriented.


- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

Q.16 how are the values of asset derived in quantitative risk assessment approach?

Ans:

- Determining the monetary value of an asset is an important part of security risk management.
- To assign a value to an asset, we have to calculate the following three primary factors:
- **The overall value of the asset to your organization**
  - This factor Calculate or estimate the asset's value in direct financial terms.
  - For example the impact of temporary disruption of an e-commerce Web site that normally runs seven days a week, 24 hours a day, generating an average of $2,000 per hour in revenue from customer orders. You can state with confidence that the annual value of the Web site in terms of sales revenue is $17,520,000.
- **The immediate financial impact of losing the asset**
  - example and assume that the Web site generates a constant rate per hour, and the same Web site becomes unavailable for six hours, the calculated exposure is .000685 or .0685 percent per year. By multiplying this exposure percentage by the annual value of the asset, you can predict that the directly attributable losses in this case would be approximately $12,000.
- **The indirect business impact of losing the asset**
  - In this example, the company estimates that it would spend $10,000 on advertising to counteract the negative publicity from such an incident. Additionally, the company also estimates a loss of .01 or 1 percent of annual sales, or $175,200. By combining the extra advertising expenses and the loss in annual sales revenue, you can predict a total of $185,200 in indirect losses in this case.

Q. 17. List various risk models. Explain

- **Ans: Threats**
  - A threat is an event which produce adversely impact on organizational operations and assets, individuals, other organizations.
  - Threats decomposed into two parts such as threat sources and threat events.
  - Threat sources include: (I) Hostile cyber or physical attacks (ii) human errors of omission (iii) structural failures of organization-controlled resources (IV) natural and man-made disasters, accidents, and failures beyond the control of the organization.
  - Threat events are caused by threat sources.

- **Vulnerabilities and Predisposing Conditions**
    - A vulnerability is a weakness in an information system, system security procedures, and internal controls.
    - Most information system vulnerabilities can be associated with security controls that either have not been applied or have been applied, but retain some weakness.
    - Vulnerabilities are not identified only within information systems. Vulnerabilities can be found in organizational governance structures such as lack of effective risk management strategies, poor intra-agency communications, and inconsistent decisions about business functions.
    - A predisposing condition is a condition that exists within an organization, a mission or business process, enterprise architecture, information system or environment of operation, which increases or decreases the likelihood of threat events.
    - Vulnerabilities resulting from predisposing conditions that cannot be easily corrected.
- **Likelihood**
    - The likelihood is a weighted risk factor based on an analysis of given threat and it is capable of identifying set of vulnerabilities.
    - Likelihood is typically based on: (I) adversary intent (ii) adversary capability (iii) adversary targeting.
    - The likelihood of threat occurrence can also be based on the state of the organization
    - Such as enterprise architecture, information security architecture, information systems, and environments in which those systems operate.
- **Impact**
    - The level of impact from a threat event is the result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
    - Impact can be experienced by a variety of organizational and non-organizational stakeholders including heads of agencies, mission and business owners, information owners, mission/business process owners, information system owners, or individuals/groups in the public or private sectors.

Q. 18. Explain the following risk models I. Threats ii. Likelihood iii. Impact

Ans:

- **Threats**
  - A threat is an event which produce adversely impact on organizational operations and assets, individuals, other organizations.
  - Threats decomposed into two parts such as threat sources and threat events.
  - Threat sources include: (I) Hostile cyber or physical attacks (ii) human errors of omission (iii) structural failures of organization-controlled resources (IV) natural and man-made disasters, accidents, and failures beyond the control of the organization.
  - Threat events are caused by threat sources.
- **Likelihood**
  - The likelihood is a weighted risk factor based on an analysis of given threat and it is capable of identifying set of vulnerabilities.
  - Likelihood is typically based on: (I) adversary intent (ii) adversary capability (iii) adversary targeting.
  - The likelihood of threat occurrence can also be based on the state of the organization
  - Such as enterprise architecture, information security architecture, information systems, and environments in which those systems operate.
- **Impact**
  - The level of impact from a threat event is the result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
  - Impact can be experienced by a variety of organizational and non-organizational stakeholders including heads of agencies, mission and business owners, information owners, mission/business process owners, information system owners, or individuals/groups in the public or private sectors.

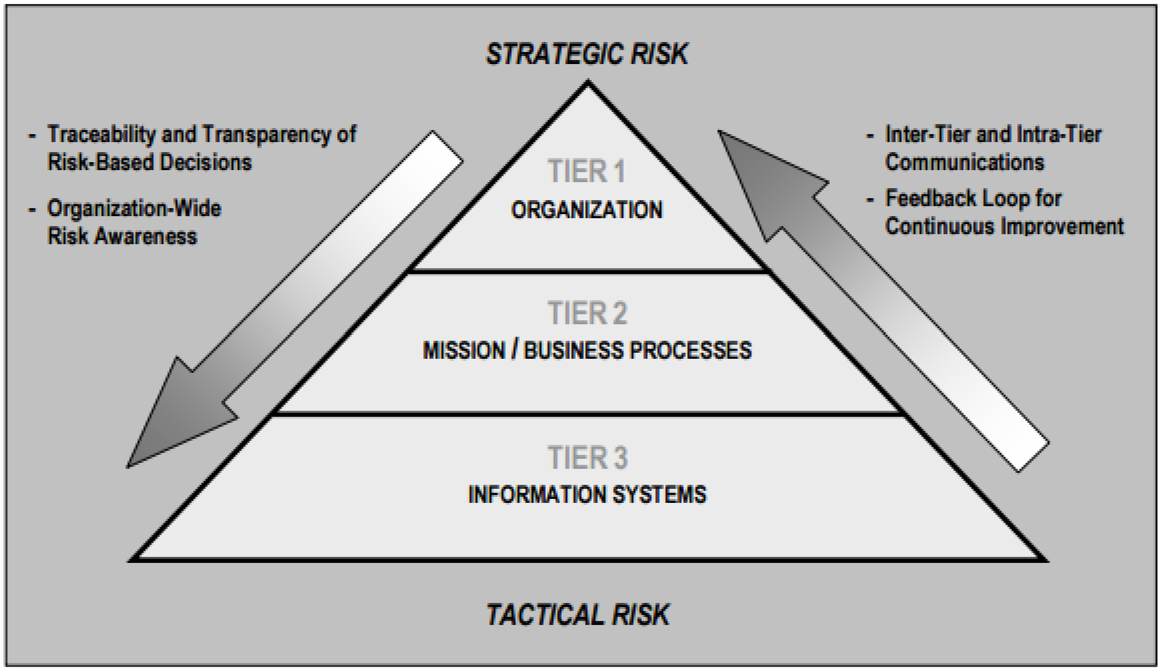
Q. 19 with neat diagram explain the risk management hierarchy

Ans:

- Risk assessments can be conducted three tiers in the risk management hierarch such as **organization level, mission/business process level, and information system level.**
- Risk assessments support to take decisions at the different tiers of the risk management hierarchy.
- At Tier 1 i.e. organization level risk assessments can affect

(I) organization-wide information security programs, policies, procedures, and guidance
(ii) Investment decisions for information technologies/systems
(iii) Minimum organization-wide security controls
(iv) Monitoring strategies and ongoing authorizations of information systems and common controls

- At Tier 2, risk assessments can affect
  (I) Enterprise architecture/security architecture design decisions
  (ii) The selection of common controls
  (iii) The selection of suppliers, services, and contractors to support organizational missions/business functions
  (iv) The interpretation of information security policies with respect to organizational information systems and environments in which those systems operate.
- At Tier 3, risk assessments can affect
  (I) design decisions
  (ii) Implementation decisions
  (iii) Operational decisions


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Q.20 how risk assessment is carries out at the organization tier of risk management hierarchy.

Ans: There are 2 organization tier for risk assessment are as follows:

- At Tier 1, risk assessments support organizational strategies, policies, guidance and processes for managing risk.
- Tier 1 risk assessments may address the :

  (I) the specific types of threats directed at organizations that may be different from other organizations and how those threats affect policy decisions.

  (ii) Impact on organizations from the loss or compromise of organizational information either intentionally or unintentionally.

  (iii) The use of new information and computing technologies such as mobile and cloud and the potential effect on the ability of organizations to successfully carry out their missions/business operations while using those technologies. However, more realistic and meaningful risk assessments are based on assessments conducted across multiple mission/business lines.
- The ability of organizations to effectively use Tier 2 risk assessments as inputs to Tier 1 risk assessments is shaped by such considerations as:

  (I) the similarity of organizational missions/business functions and mission/business processes.

  (ii)In decentralized organizations or organizations with varied missions/business functions and/or environments of operation, expert analysis may be needed to normalize the results from Tier 2 risk assessments.
- Finally, risk assessments at Tier 1 take into consideration the identification of mission-essential functions from Continuity of Operations Plans prepared by organizations when determining the contribution of Tier 2 risks. Risk assessment results at Tier 1 are communicated to organizational entities at Tier 2 and Tier 3.

Q. 21 how risk assessment is carries out at the information system of risk management hierarchy?

Ans: (refer Question no: 19)

Q.22 Explain the quantitative risk assessment.

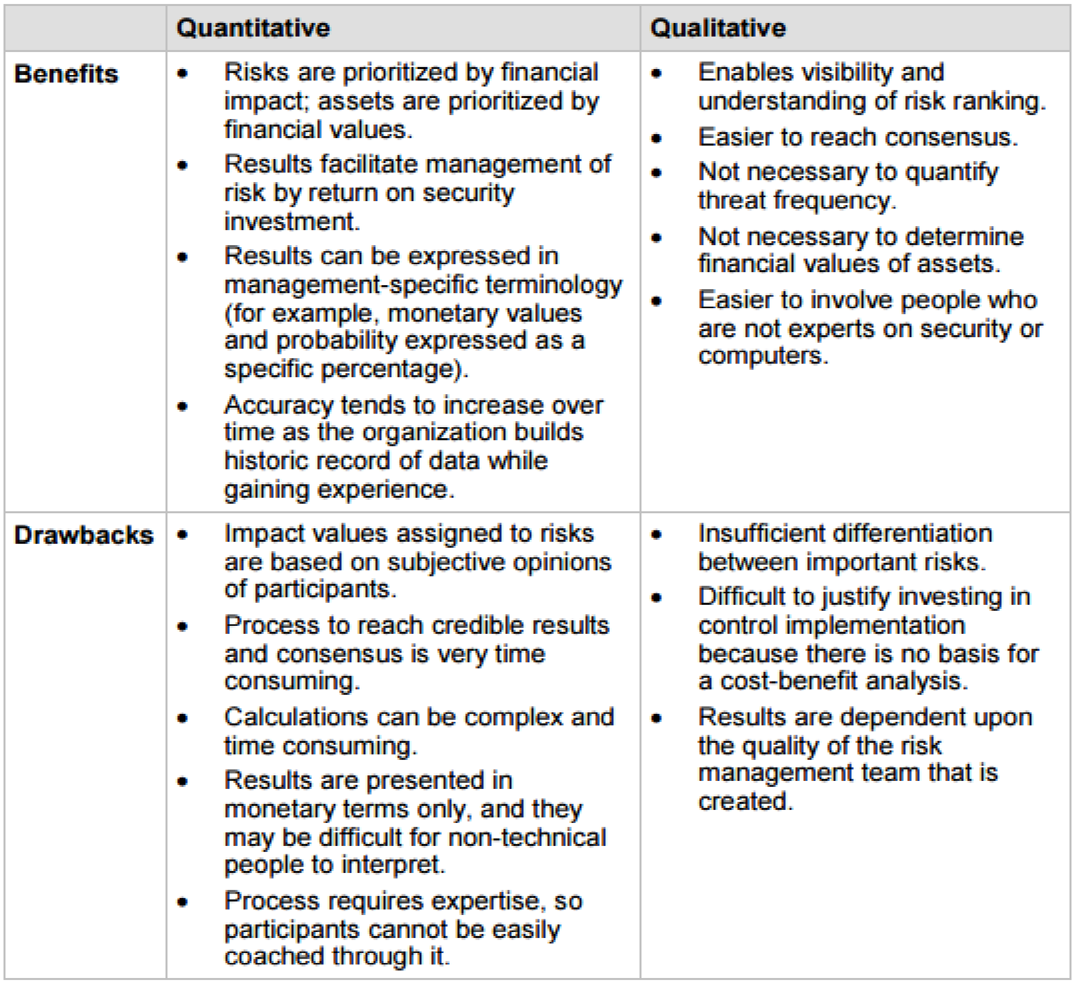
Ans:

- Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers.
- This type of assessment most effectively supports cost-benefit analyses of alternative risk responses.
- However, the meaning of the quantitative results may not always be clear and may require interpretation and explanation to explain the assumptions and constraints of u the results.

- For example, organizations may typically ask if the numbers or results obtained in the risk assessments are reliable or if the differences in the obtained values are meaningful or insignificant.
- 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.
- 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(not cleared); 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.

Q.23 Compare the quantitative and qualitative risk assessment approaches.

Ans:



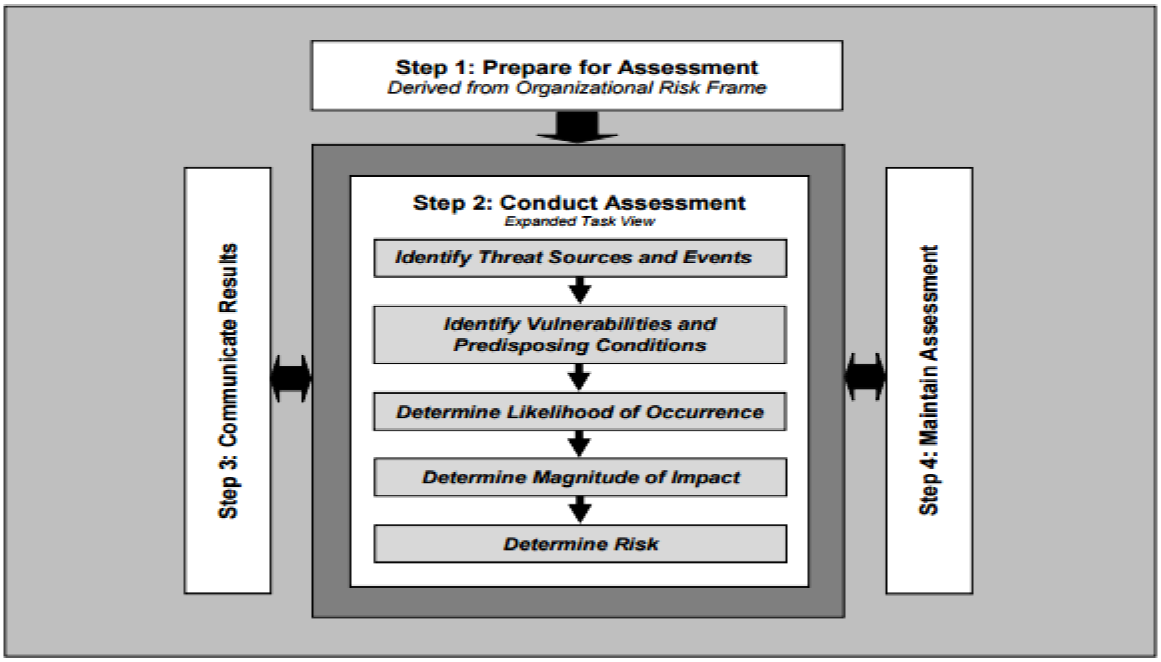
	Quantitative	**Qualitative**
Benefits	• Risks are prioritized by financial impact; assets are prioritized by financial values. • Results facilitate management of risk by return on security investment. • Results can be expressed in management-specific terminology (for example, monetary values and probability 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.

Q. 24 List and explain the steps in risk assessment process.

Ans: There are four steps in risk assessment process are as follows:

- **STEP 1: PREPARE FOR THE ASSESSMENT**
  - The first step in the risk assessment process is to prepare for the assessment. The objective of this step is to establish a context for the risk assessment.
  - Preparing for a risk assessment includes the following tasks:
    1. Identify the purpose of the assessment
    2. Identify the scope of the assessment
    3. Identify the assumptions and constraints associated with the assessment
    4. Identify the sources of information to be used as inputs to the assessment
    5. Identify the risk model and analytic approaches to be employed during the assessment.
- **STEP 2: CONDUCT THE ASSESSMENT**
  - The second step in the risk assessment process is to conduct the assessment. The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions.
  - Conducting risk assessments includes the following specific tasks:
    1. Identify threat sources that are relevant to organizations
    2. Identify threat events that could be produced by those sources
    3. Identify vulnerabilities within organizations that could be exploited by threat Sources through specific threat events
    4. Determine the likelihood that the identified threat sources would initiate specific threat events
    5. Determine the adverse impacts to organizational operations and assets.
- **STEP 3: COMMUNICATE AND SHARE RISK ASSESSMENT RESULTS**
  - The third step in the risk assessment process is to communicate the assessment results and share risk-related information.
  - The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions.
  - Communicating and sharing information consists of the following specific tasks:
    1. Communicate the risk assessment results
    2. Share information developed in the execution of the risk assessment, to support other risk management activities.
- **STEP 4: MAINTAIN THE ASSESSMENT**

- The fourth step in the risk assessment process is to maintain the assessment.
- The objective of this step is to keep current, the specific knowledge of the risk organizations incur.
- Maintaining risk assessments includes the following specific tasks:
  1. Monitor risk factors identified in risk assessments and understanding subsequent changes to those factors.
  2. Update the components of risk assessments reflecting the monitoring activities carried out by organizations.


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment