Unit - 1

**Q.1. Explain the process of risk management.**

**Ans:**

**RISK MANAGEMENT PROCESS:**

Risk management processes include:

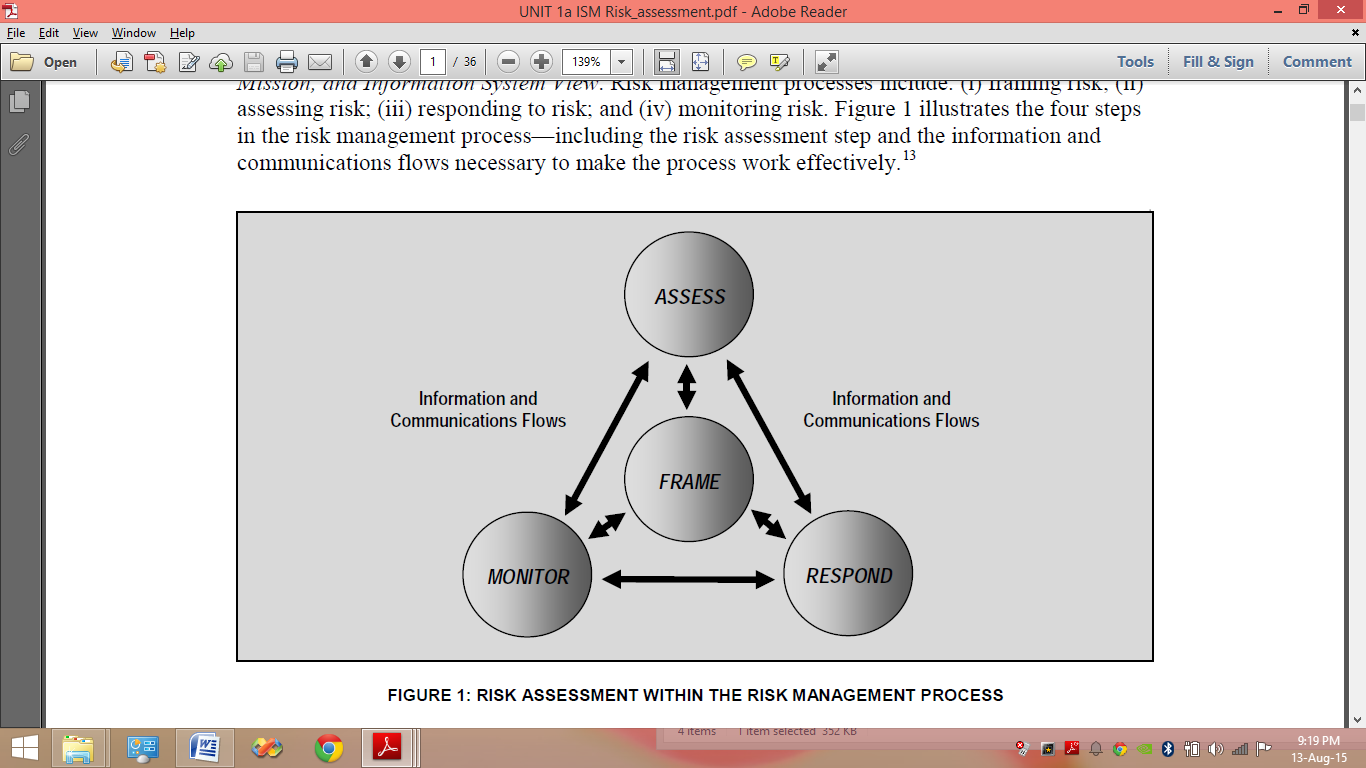
(i) framing risk;

(ii) assessing risk;

(iii) responding to risk; and

(iv) monitoring risk.

Figure 1 illustrates the four steps in the risk management process—including the risk assessment step and the information and communications flows necessary to make the process work effectively.



1. **Frame:**

* The **first component** of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made.
* The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.
* The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

1. **Assess:**

* The **second component** of risk management addresses how organizations *assess* risk within the context of the organizational risk frame.
* The purpose of the risk assessment component is to identify:

(i) threats to organizations (i.e., operations, assets, or individuals) or threats

directed through organizations against other organizations or the Nation;

(ii) vulnerabilities internal and external to organizations;

(iii) the harm (i.e., adverse impact) that may occur given the potential

for threats exploiting vulnerabilities; and

(iv) the likelihood that harm will occur. The end result is a determination of risk

(i.e., typically a function of the degree of harm and likelihood of harm

occurring).

1. **Respond:**

* The **third component** of risk management addresses how organizations *respond* to risk once that risk is determined based on the results of a risk assessment.
* The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by:

(i) developing alternative courses of action for responding to risk;

(ii) evaluating the alternative courses of action;

(iii)determining appropriate courses of action consistent with organizational risk tolerance; and

(iv) implementing risk responses based on selected courses of action.

1. **Monitor:**

* The fourth component of risk management addresses how organizations *monitor* risk over time.
* The purpose of the risk monitoring component is to:

(i) determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame);

(ii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and

(iii) verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

**Q. 2. What are the steps for risk assessment?**

**Ans:**

* 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; and

(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.
* Rather, 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—with the frequency of the risk assessments and the resources applied during the assessments, commensurate 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, and the economic and national security interests of the United States, arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems.
* Organizations conduct risk assessments to determine risks that are common to the organization’s core missions/business functions, mission/business processes, mission/business segments, common infrastructure/support services, or information systems.
* Risk assessments can support a wide variety of risk-based decisions and activities by organizational officials across all three tiers in the risk management hierarchy including, but not limited to, the following:

• Development of information security architecture;

• Definition of interconnection requirements for information systems (including systems supporting mission/business processes and common infrastructure/support services);

• Design of security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers/supply chain, and contractors;

• Authorization (or denial of authorization) to operate information systems or to use security controls inherited by those systems (i.e., common controls);

• Modification of missions/business functions and/or mission/business processes permanently, or for a specific time frame (e.g., until a newly discovered threat or vulnerability is addressed, until a compensating control is replaced);

• Implementation of security solutions (e.g., whether specific information technology products or configurations for those products meet established requirements); and

• Operation and maintenance of security solutions (e.g., continuous monitoring strategies and programs, ongoing authorizations).

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

**Ans:**

Preparing for a risk assessment includes the following tasks:

• Identify the purpose of the assessment;

• Identify the scope of the assessment;

• Identify the assumptions and constraints associated with the assessment;

• Identify the sources of information to be used as inputs to the assessment; and

• Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

**1.IDENTIFY PURPOSE:**

**TASK 1-1:** Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

* The purpose of the risk assessment is explicitly stated in sufficient detail to ensure that the assessment produces the appropriate information and supports the intended decisions.
* Organizations can provide guidance on how to capture and present information produced during the risk assessment (e.g., using a defined organizational template).

The purpose of the risk assessment is influenced by whether the assessment is:

(i) an initial assessment; or

(ii) a subsequent assessment initiated from the risk response or monitoring steps in the risk management process.

**2.IDENTIFY SCOPE:**

**TASK 1-2:** Identify the scope of the risk assessment in terms of organizational applicability, time frame supported and architectural/technology considerations.

* The scope of the risk assessment determines what will be considered in the assessment.
* Risk assessment scope affects the range of information available to make risk-based decisions and is determined by the organizational official requesting the assessment and the risk management strategy.

Establishing the scope of the risk assessment helps organizations to determine:

(i) what tiers are addressed in the assessment;

(ii) what parts of organizations are affected by the assessment and how they are affected;

(iii) what decisions the assessment results support;

(iv) how long assessment results are relevant; and

(v) what influences the need to update the assessment.

* Establishing the scope of the risk assessment helps to determine the form and content of the risk assessment report, as well as the information to be shared as a result of conducting the assessment.

**3.IDENTIFY ASSUMPTIONS AND CONSTRAINTS:**

**TASK 1-3:** Identify the specific assumptions and constraints under which the risk assessment is conducted.

* As part of the risk framing step in the risk management process, organizations make explicit the specific assumptions, constraints, risk tolerance, and priorities/trade-offs used within organizations to make investment and operational decisions. This information guides and informs organizational risk assessments.
* When an organizational risk management strategy cannot be cited, risk assessments identify and document assumptions and constraints.
* Assumptions and constraints identified by organizations during the risk framing step and included as part of the organizational risk management strategy need not be repeated in each individual risk assessment.
* By making assumptions and constraints explicit, there is greater clarity in the risk model selected for the risk assessment, increased reproducibility/repeatability of assessment results, and an increased opportunity for reciprocity among organizations.
* Organizations identify assumptions in key areas relevant to the risk assessment including, for example:

(i) threat sources;

(ii) threat events;

(iii) vulnerabilities and predisposing conditions;

(iv) potential impacts;

(v) assessment and analysis approaches; and

(vi) which missions/business functions are primary.

**4.IDENTIFY INFORMATION SOURCES:**

**TASK 1-4:** Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.

* Descriptive information enables organizations to be able to determine the relevance of threat and vulnerability information. Sources of information can be either internal or external to organizations.
* Internal sources of information that can provide insights into both threats and vulnerabilities can include, for example, risk assessment reports, incident reports, security logs, trouble tickets, and monitoring results.

**5.IDENTIFY RISK MODEL AND ANALYTIC APPROACH:**

**TASK 1-5:** Identify the risk model and analytic approach to be used in the risk assessment.

* Organizations define one or more risk models for use in conducting risk assessments and identify which model is to be used for the risk assessment.
* To facilitate reciprocity of assessment results, organization-specific risk models include, or can be translated into, the risk factors (i.e., threat, vulnerability, impact, likelihood, and predisposing condition) defined in the appendices.
* Organizations also identify the specific analytic approach to be used for the risk assessment including the assessment approach (i.e., quantitative, qualitative, semi-quantitative) and the analysis approach (i.e., threat-oriented, asset/impact-oriented, vulnerability-oriented).

**Q.4. What are the different risk assessment approaches?**

**Ans:**

**Different Risk Assessment Approaches are as follows:**

1. **Quantitative:**

* *Quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
* This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action. However, the meaning of the quantitative results may not always be clear and may require interpretation and explanation—particularly to explain the assumptions and constraints on using 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.
* Additionally, the rigor of quantification is significantly lessened when subjective determinations are buried within the quantitative assessments, or when significant uncertainty surrounds the determination of values.
* The benefits of quantitative assessments (in terms of the rigor, repeatability, and reproducibility of assessment results) can, in some cases, be outweighed by the costs (in terms of the expert time and effort and the possible deployment and use of tools required to make such assessments).

1. **Qualitative:**

* *Qualitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high).
* This type of assessment supports communicating risk results to decision makers. However, the range of values in qualitative assessments is comparatively small in most cases, making the relative prioritization or comparison within the set of reported risks difficult.
* Additionally, unless each value is very clearly defined or is characterized by meaningful examples, different experts relying on their individual experiences could produce significantly different assessment results.
* The repeatability and reproducibility of qualitative assessments are increased by the annotation of assessed values (e.g., this value is high because of the following reasons) and by the use of tables or other well-defined functions to combine qualitative values.

1. **Semi-Quantitative:**

* *Semi-Quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers.
* This type of assessment can provide the benefits of quantitative and qualitative assessments.
* The bins (e.g., 0-15, 16-35, 36-70, 71-85, 86-100) or scales (e.g., 1-10) translate easily into qualitative terms that support risk communications for decision makers (e.g., a score of 95 can be interpreted as very high), while also allowing relative comparisons between values in different bins or even within the same bin (e.g., the difference between risks scored 70 and 71 respectively is relatively insignificant, while the difference between risks scored 36 and 70 is relatively significant).
* The role of expert judgment in assigning values is more evident than in a purely quantitative approach.
* Moreover, if the scales or sets of bins provide sufficient granularity, relative prioritization among results is better supported than in a purely qualitative approach.
* As in a quantitative approach, rigor is significantly lessened when subjective determinations are buried within assessments, or when significant uncertainty surrounds a determination of value.
* As with the non-numeric categories or levels used in a well-founded qualitative approach, each bin or range of values needs to be clearly defined and/or characterized by meaningful examples.

**Q.5. What are the different risk analysis approaches?**

**Ans:**

Analysis approaches differ with respect to the orientation or 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*:**

A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent.

**(ii)** ***asset/impact-oriented*:**

An asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences.

**(iii)** ***vulnerability oriented*:**

A vulnerability-oriented approach starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised.

* Each analysis approach takes into consideration the same risk factors, and thus entails the same set of risk assessment activities, albeit in different order. Differences in the starting point of the risk assessment can potentially bias the results, causing some risks not to be identified.
* Therefore, identification of risks from a second orientation (e.g., complementing a threat-oriented analysis approach with an asset/impact-oriented analysis approach) can improve the rigor and effectiveness of the analysis.

In addition to the orientation of the analysis approach, organizations can apply more rigorous analysis techniques (e.g., graph-based analyses) to provide an effective way to account for the 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);

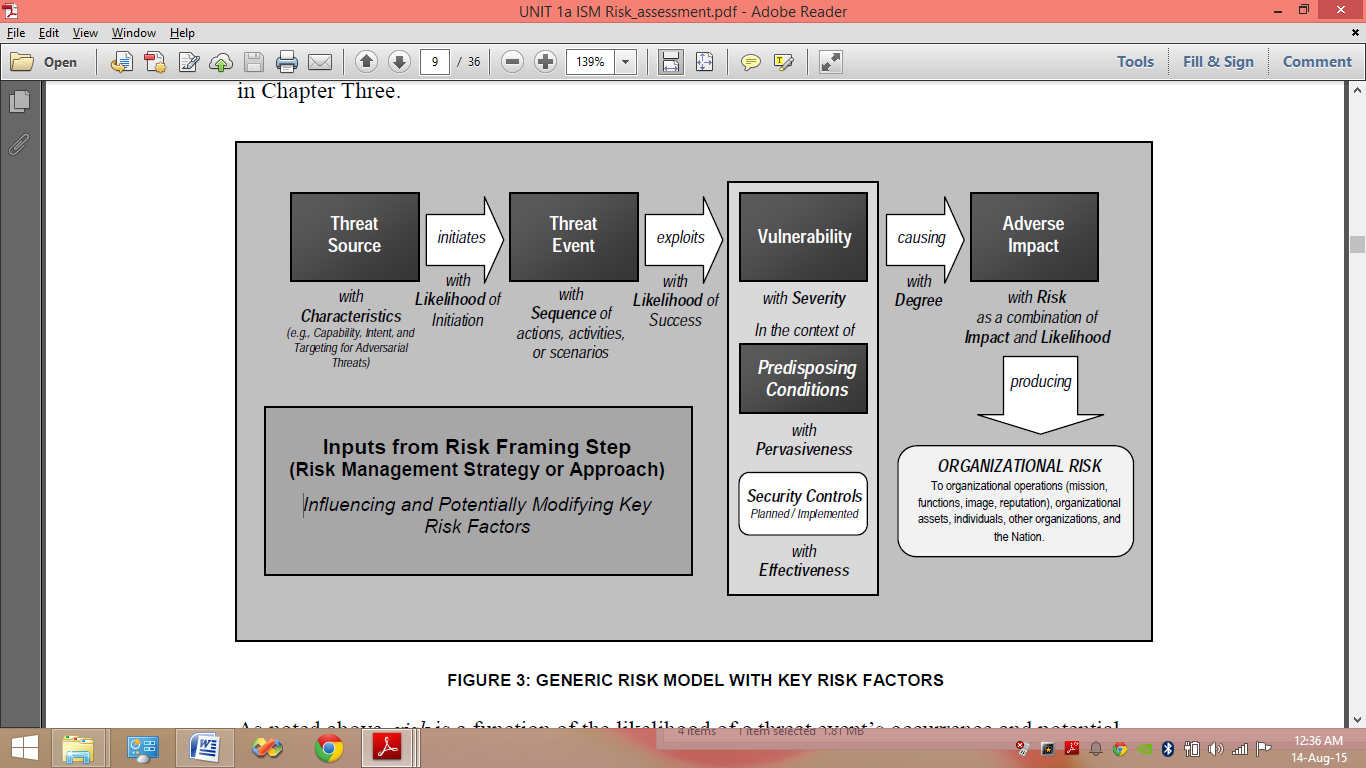
(iii) threat events and impacts/assets (i.e., a single threat event can affect multiple assets or have multiple impacts, and a single asset can be affected by multiple threat events).

* Rigorous analysis approaches also provide a way to account for whether, in the time frame for which risks are assessed, a specific adverse impact could occur (or a specific asset could be harmed) at most once, or perhaps repeatedly, depending on the nature of the impacts and on how organizations (including mission/business processes or information systems) recover from such adverse impacts.

**Q.6. Explain generic risk model in detail.**

**Ans:**

* *Risk models* define the *risk factors* to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments.
* Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition.



**Threat:**

* A ***threat***is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Threat events are caused by threat sources.

**Threat source** :

A ***threat source***is characterized as:

(i) the intent and method targeted at the exploitation of a vulnerability; or

(ii) a situation and method that may accidentally exploit a vulnerability.

In general, types of threat sources include:

(i) hostile cyber or physical attacks;

(ii) human errors of omission or commission;

(iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and

(iv) natural and man-made disasters, accidents, and failures beyond the control of the organization.

**Threat events:**

* ***Threat events*** for cyber or physical attacks are characterized by the tactics, techniques, and procedures (TTPs) employed by adversaries.

**Threat shifting*:***

* ***Threat shifting***is the response of adversaries to perceived safeguards and/or countermeasures (i.e., security controls), in which adversaries change some characteristic of their intent/targeting in order to avoid and/or overcome those safeguards/countermeasures.

**Vulnerabilities and Predisposing Conditions:**

* A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness.
* 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 affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation.

**Likelihood:**

* The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
* The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

For adversarial threats, an assessment of likelihood of occurrence is typically based on:

(i) adversary *intent*;

(ii) adversary *capability*; and

(iii) adversary *targeting*.

**Impact:**

* The level of *impact* from a threat event is the magnitude of harm that can be expected to 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.
* Such harm can be experienced by a variety of organizational and non-organizational stakeholders including, for example, heads of agencies, mission and business owners, information owners/stewards, mission/business process owners, information system owners, or individuals/groups in the public or private sectors relying on the organization—in essence, anyone with a vested interest in the organization’s operations, assets, or individuals, including other organizations in partnership with the organization, or the Nation.

**Risk:**

* Figure 3 illustrates an example of a risk model and the relationship among the factors. Each of the risk factors is used in the risk assessment process. R*isk* is a function of the likelihood of a threat event’s occurrence and potential adverse impact should the event occur.

**Aggregation:**

* Organizations may use risk *aggregation* to roll up several discrete or lower-level risks into a more general or higher-level risk.
* Organizations may also use risk aggregation to efficiently manage the scope and scale of risk assessments involving multiple information systems and multiple mission/business processes with specified relationships and dependencies among those systems and processes.

**Uncertainty:**

*Uncertainty* is inherent in the evaluation of risk, due to such considerations as:

(i) limitations on the extent to which the future will resemble the past;

(ii) imperfect or incomplete knowledge of the threat (e.g., characteristics of

adversaries including tactics, techniques, and procedures);

(iii) undiscovered vulnerabilities in technologies or products; and

(iv) unrecognized dependencies, which can lead to unforeseen impacts.

**Q.7. What are the key characteristics of OCTAVE approach?**

**Ans:**

* OCTAVE is self directed, requiring an organization to manage the evaluation process and make information-protection decisions.
* An interdisciplinary team, called the analysis team, leads the evaluation. The team includes people from both the business units and the IT department, because both perspectives are important when characterizing the global, organizational view of information security risk.

OCTAVE is an asset-driven evaluation approach. Analysis teams

* identify information-related assets (e.g., information and systems) that are important to the organization
* focus risk analysis activities on those assets judged to be most critical to the organization
* consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats
* evaluate risks in an operational context - how they are used to conduct an organization’s business and how those assets are at risk due to security threats
* create a practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization’s critical assets
* The organizational, technological, and analysis aspects of an information security risk evaluation are complemented by a three-phased approach. OCTAVE is organized around these three basic aspects (illustrated in Figure 2), enabling organizational personnel to assemble a comprehensive picture of the organization’s information security needs.
* The phases are :

**• *Phase 1: Build Asset-Based Threat Profiles*** –

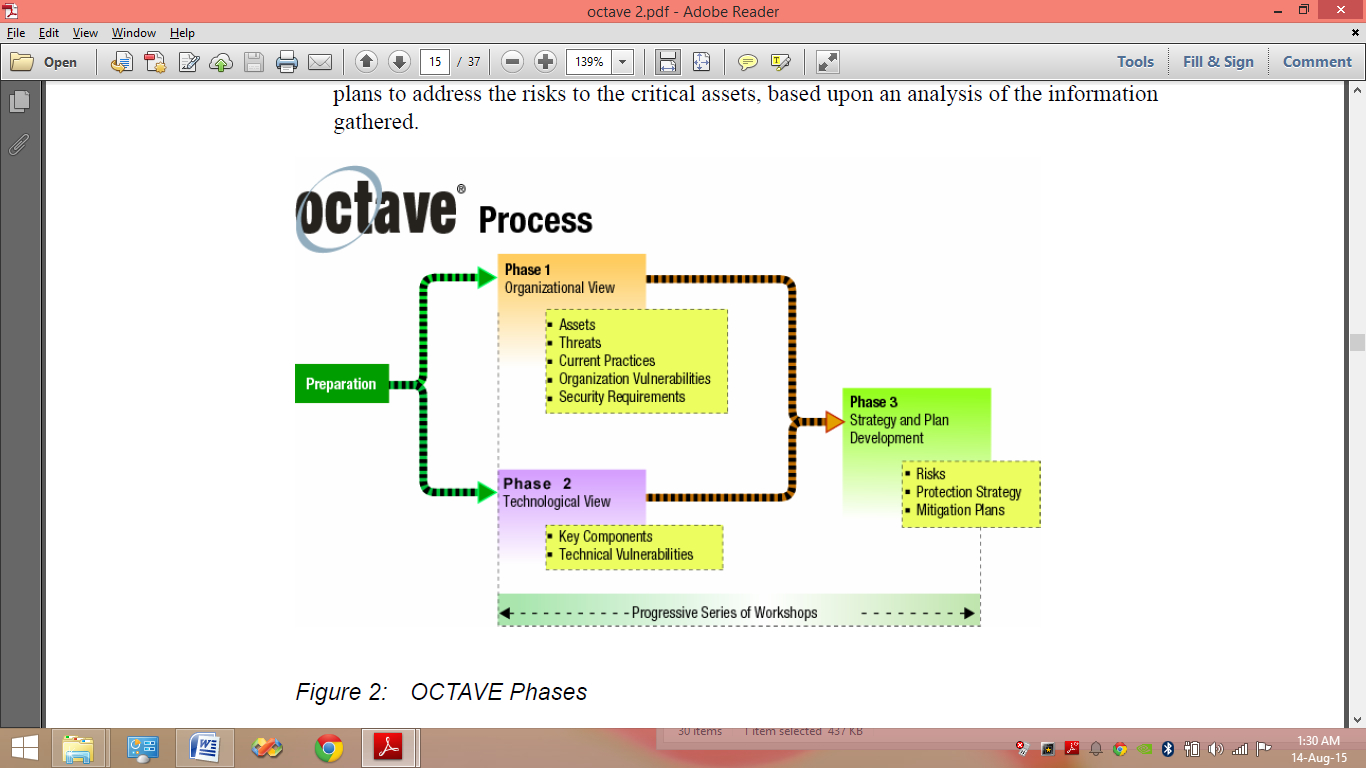
* This is an organizational evaluation. The analysis team determines what is important to the organization (information-related assets) and what is currently being done to protect those assets. The team then selects those assets that are most important to the organization (critical assets) and describes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

**• *Phase 2: Identify Infrastructure Vulnerabilities* –**

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

**• *Phase 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 what to do about them. The team creates a protection strategy for the organization and mitigation 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, imposing a small degree of rigor to the reactive approach can help organizations of all types to better use their resources.

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 in the long run.
* 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.
* If you determine that there will be no adverse effects, or that they would be outweighed by the positive benefits of activity, containment should begin as quickly as possible during a security incident by disconnecting from the network the systems known to be affected.
* If you cannot contain the damage by isolating the servers, ensure that you actively monitor the attacker’s actions in order to be able to remedy the damage as soon as possible.
* And in any event, ensure that all log files are saved before shutting off any server, in order to preserve the information contained in those files as evidence if you (or your lawyers) need it later.

3. **Assess the damage**:

* Immediately make a duplicate of the hard disks in any servers that were attacked and put those aside for forensic use later. Then assess the damage.
* You should begin to determine the extent of the damage that the attack caused as soon as possible, right after you contain the situation and duplicate the hard disks. This 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.
* If it is not possible to assess the damage in a timely manner, you should implement a contingency plan so that normal business operations and productivity can continue.
* It is at this point that organizations may want to engage law enforcement regarding the incident; however, you should establish and maintain working relationships with law enforcement agencies that have jurisdiction over your organization's business before an incident occurs so that when a serious problem arises you know whom to contact and how to work with them.
* You should also advise your company’s legal department immediately, so that they can determine whether a civil lawsuit can be brought against anyone as a result of the damage.

4. **Determine the cause of the damage**:

* In order to ascertain the origin of the assault, 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. You should conduct this activity on the computer systems in place and not on the backed up drives created in step 3.
* Those drives must be preserved intact for forensic purposes so that law enforcement or your lawyers can use them to trace the perpetrators of the attack and bring them to justice.
* If you need to create a backup for testing purposes to determine the cause of the damage, create a second backup from your original system and leave the drives created in step 3 unused.

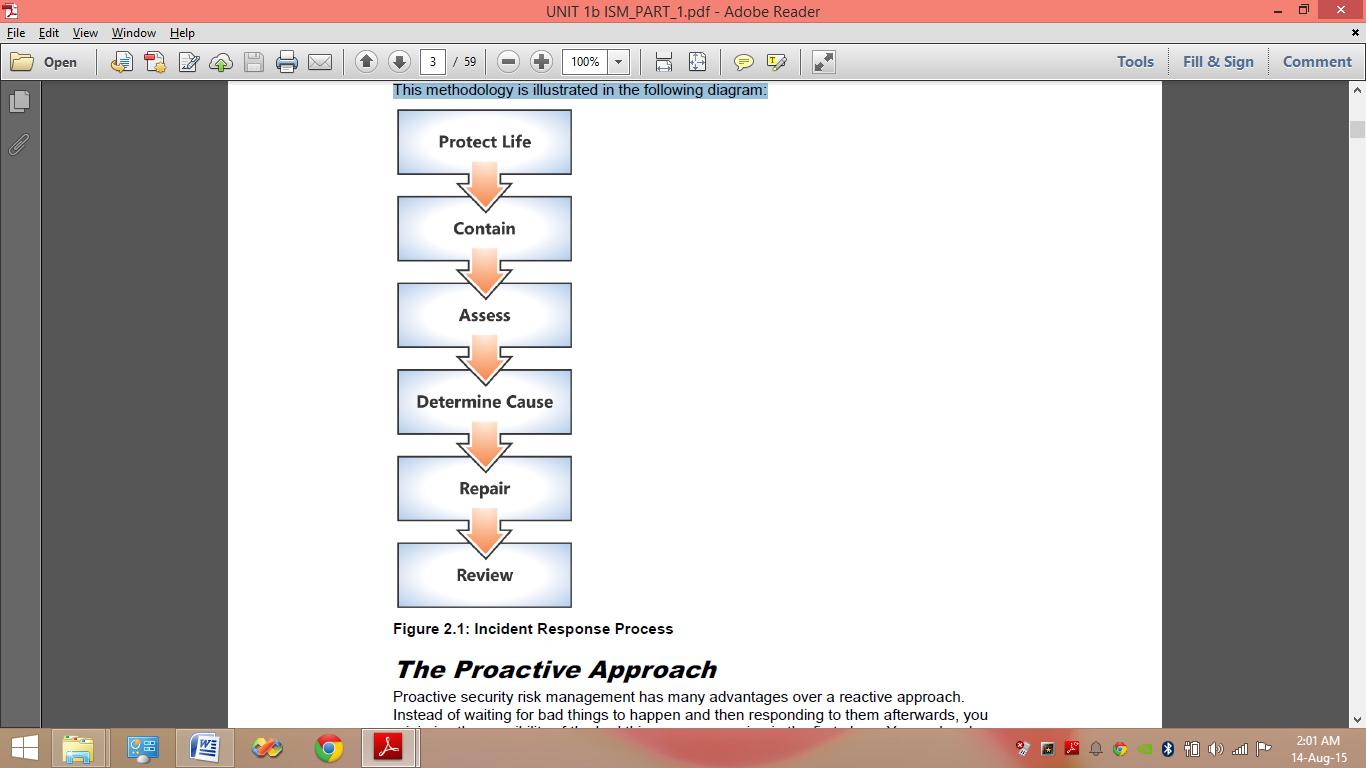
5. **Repair the damage**:

* In most cases, 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 or to provide guidance on the process to the responsible team.
* During recovery, contingency procedures are executed to limit the spread of the damage and isolate it.
* Before returning repaired systems to service be careful that they are not reinfected immediately by ensuring that you have mitigated whatever vulnerabilities were exploited during the incident.

6. **Review response and update policies**:

* After the documentation and recovery phases are complete, you should review the process thoroughly.
* Determine with your team the steps that were executed successfully and what mistakes were made.
* In almost all cases, you will find that your processes need to be modified to allow you to handle incidents better in the future.
* You will inevitably find weaknesses in your incident response plan. This is the point of this after-the-fact exercise—you are looking for opportunities for improvement.
* Any flaws should prompt another round of the incident-response planning process so that you can handle future incidents more smoothly.

This methodology is illustrated in the following diagram:



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

**Ans:**

* Proactive security risk management has many advantages over a reactive approach. 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 analogy may help to illustrate this idea.
* Influenza is a deadly respiratory disease that infects millions of people in the United States alone each year. Of those, over 100,000 must be treated in hospitals, and about 36,000 die.
* You could choose to deal with the threat of the disease by waiting to see if you get infected and then taking medicine to treat the symptoms if you do become ill.
* Alternatively, you could choose to get vaccinated before the influenza season begins. Organizations should not, of course, completely forsake incident response.
* 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.

Each of the 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.

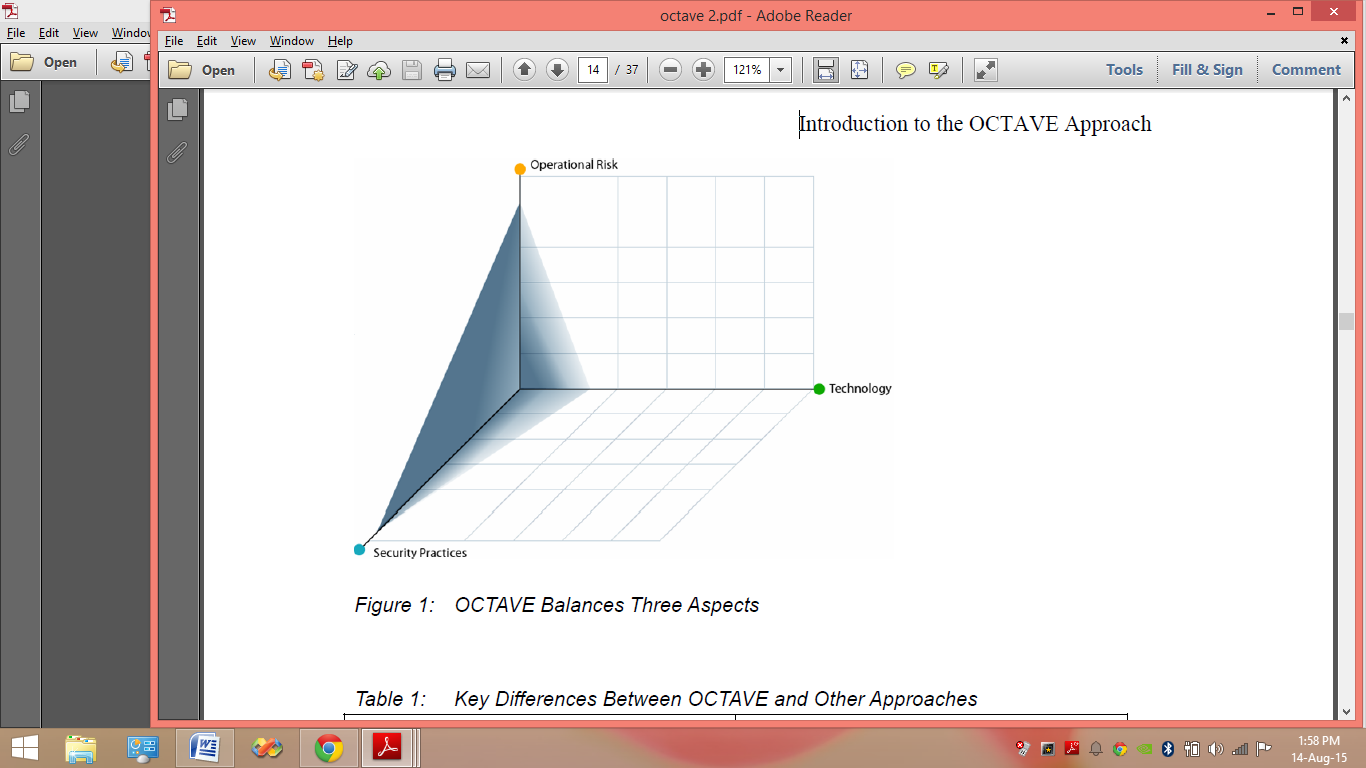
*Proactive Risk Management’s*unique approach provides:

* A model of risk that is scalable to any size project or program and easily deployable as the risk management approach built into any product development or project management life cycle.
* Methods for identifying drivers (causes) of risks so you can manage root causes rather than the symptoms of risks.
* An appropriate quantification of the key factors of a risk that allows you to prioritize risks without introducing errors that render your numbers meaningless.
* A clear distinction between a risk and an issue and the different types of management they require.
* A vast array of supporting tools and strategies that support implementation of an effective project risk management program.
* Guidance on identifying and overcoming the organizational and cultural impediments that can block implementation of your risk management program.

**Q.10. Write a short note on OCTAVE.**

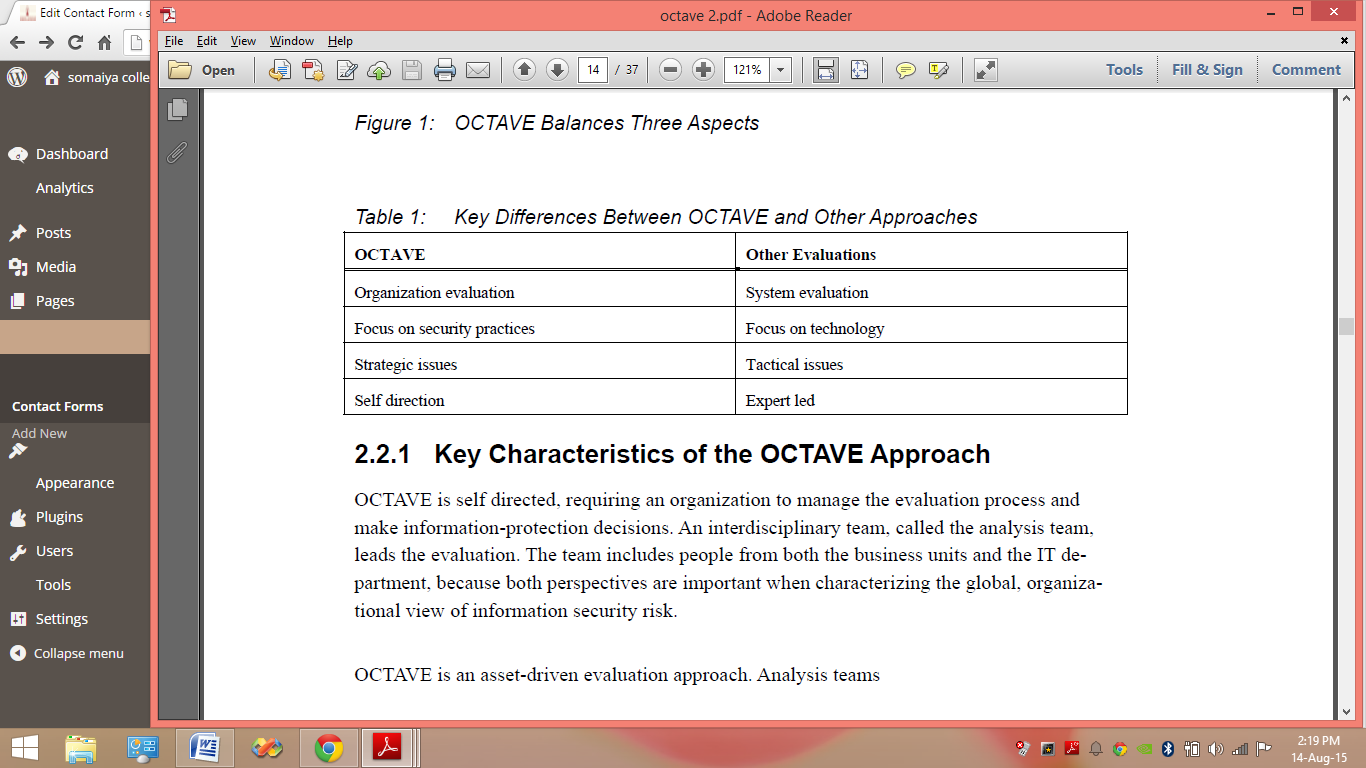
**Ans:**

* OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a security framework for determining risk level and planning defenses against cyber assaults.
* The framework defines a methodology to help organizations minimize exposure to likely threats, determine the likely consequences of an attack and deal with attacks that succeed.
* OCTAVE is designed to leverage the experience and expertise of people within the organization. The first step is to construct profiles of threats based on the relative risk that they pose.
* The process goes on to conduct a [vulnerability assessment](http://searchmidmarketsecurity.techtarget.com/definition/vulnerability-analysis) specific to the organization.
* OCTAVE defines three phases:
* Phase 1: Build Asset-Based Threat Profiles
* Phase 2: Identify Infrastructure Vulnerabilities
* Phase 3: Develop Security Strategy and Plans
* OCTAVE is a risk-based strategic assessment and planning technique for security. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization’s security strategy.
* The technique leverages people’s knowledge of their organization’s security- related practices and processes to capture the current state of security practice within the organization.
* Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization.
* Unlike the typical technology-focused assessment, which is targeted at technological risk and focused on tactical issues, 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, balancing the three key aspects illustrated in Figure 1: operational risk, security practices, and technology.



* The OCTAVE approach is driven by two of the aspects: operational risk and security practices.
* Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices.
* By using the OCTAVE approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets.
* All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are factored into decision making, enabling an organization to match a practice-based protection *strategy* to its security risks.

Table 1 summarizes key differences between OCTAVE and other evaluations.



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

**Ans:**

COBIT stands for “Control Objectives for Information and related Technology”. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

COBIT uses a maturity model as a means of assessing the maturity of the processes described in the domains. The model encompasses the following levels:

1) non-existent

2) initial / ad hoc

3) repeatable but intuitive

4) defined process

5) managed and measurable

6) optimised

COBIT is made up of a number of „domains‟, „processes‟ & „activities‟. Here they are:

**DOMAIN:**

**1) Plan & Organise (PO):**

**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

**DOMAIN:**

**2) Acquire & Implement (AI):**

**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)

**DOMAIN:**

**3) Deliver & Support (DS):**

**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

**DOMAIN:**

**4) Monitor & Evaluate (ME):**

**PROCESSES:**

ME1 Monitor and Evaluate IT Processes

ME2 Monitor and Evaluate Internal Control

ME3 Ensure Regulatory Compliance

ME4 Provide IT Governance

**Q.12. Explain any 2 methods of quantitative risk assessment.**

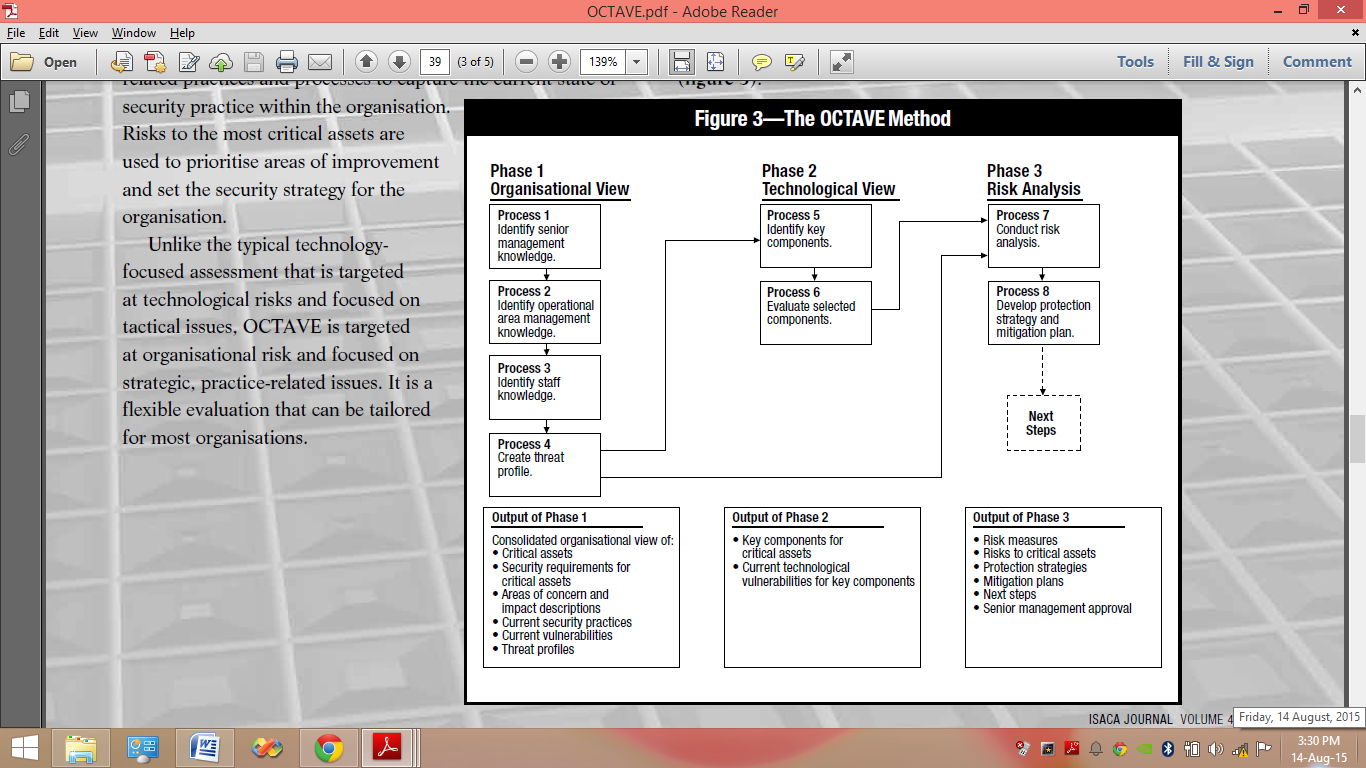
**Ans:**

**Q.13. Explain with diagram OCTAVE method.**

**Ans:**

**The OCTAVE Method:**

* The OCTAVE Method has been designed for large organizations having multi-layered hierarchy and maintaining their own computing infrastructure.
* The organisational, technological and analysis aspects of an information security risk evaluation are undertaken by a three-phased approach with eight processes (**figure 3**):

****

• **Phase 1: Build asset-based threat profiles (organizational evaluation)** —

The analysis team determines critical assets and what is currently being done to protect them. The security requirements for each critical asset are then identified. Finally, the organisational vulnerabilities with the existing practices and the threat profile for each critical asset are established.

• **Phase 2: Identify infrastructure vulnerabilities (technological evaluation)**—

The analysis team identifies network access paths and the classes of IT components

related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks and establishes the technological

vulnerabilities that expose the critical assets.

• **Phase 3: Develop security strategy and mitigation plans (strategy and plan development)**—

The analysis team establishes risks to the organisation’s critical assets based on analysis of the information gathered and decides what to do about them. The team creates a protection strategy for the organisation and mitigation plans to address identified risks. The team also determines the ‘next steps’ required for

implementation and gains senior management’s approval on the outcome of the whole process.

**Q.14. Explain with diagram OCTAVE allegro.**

**Ans:**

* OCTAVE Allegro is focused on risk assessment in an organisational context, but offers an alternative approach and attempts to improve an organisation’s ability to perform risk assessment in a more efficient and effective manner.
* One of the insights acquired from earlier experiences has been the need to move to a more information-centric risk assessment.
* One of the guiding philosophies of Allegro has been that when information assets are the focus of the security risk assessment, all other related assets are considered ‘information containers’, storing, processing or transporting the information assets.
* Information containers can be people (since people access information and gain knowledge), objects (piece of paper) or technology (database). Thus, threats to information assets are analysed by considering where they live and effectively limiting the number and types of assets brought into the process.

Some key drivers that led SEI to formulating this new methodology include:

• Improving ease of use

• Refining the definition of assessment scope by introducing the container concept

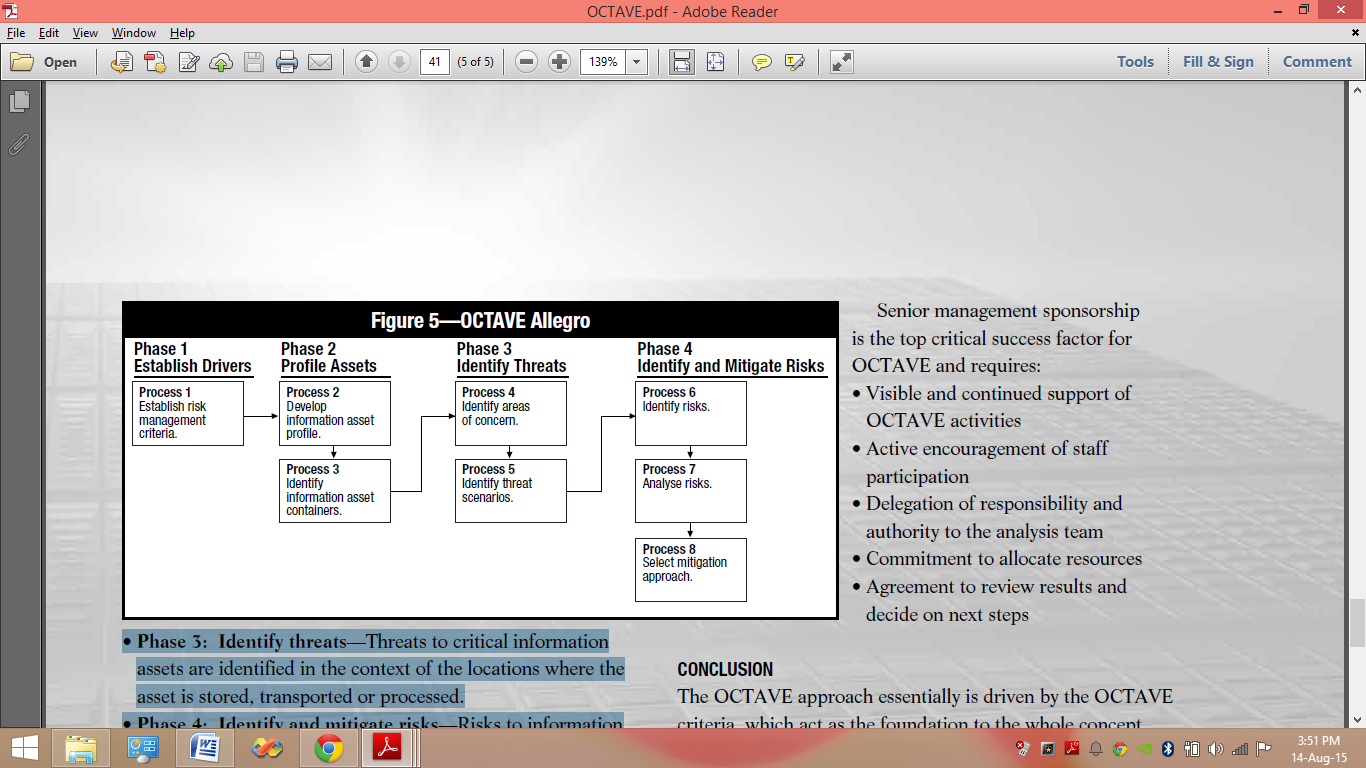
• Streamlining data collection and threat identification processes

• Reducing training and knowledge requirements

• Improving institutionalisation and repeatability

• Reducing the technology view

The OCTAVE Allegro approach comprises eight processes and is organised into four phases (**figure 5**):



• **Phase 1: Establish drivers**—

The organisation develops risk measurement criteria consistent with organisational 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 analysed and the development of mitigation approaches commences.

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

**Ans:**

A *risk assessment methodology* typically includes:

(i) a risk assessment process;

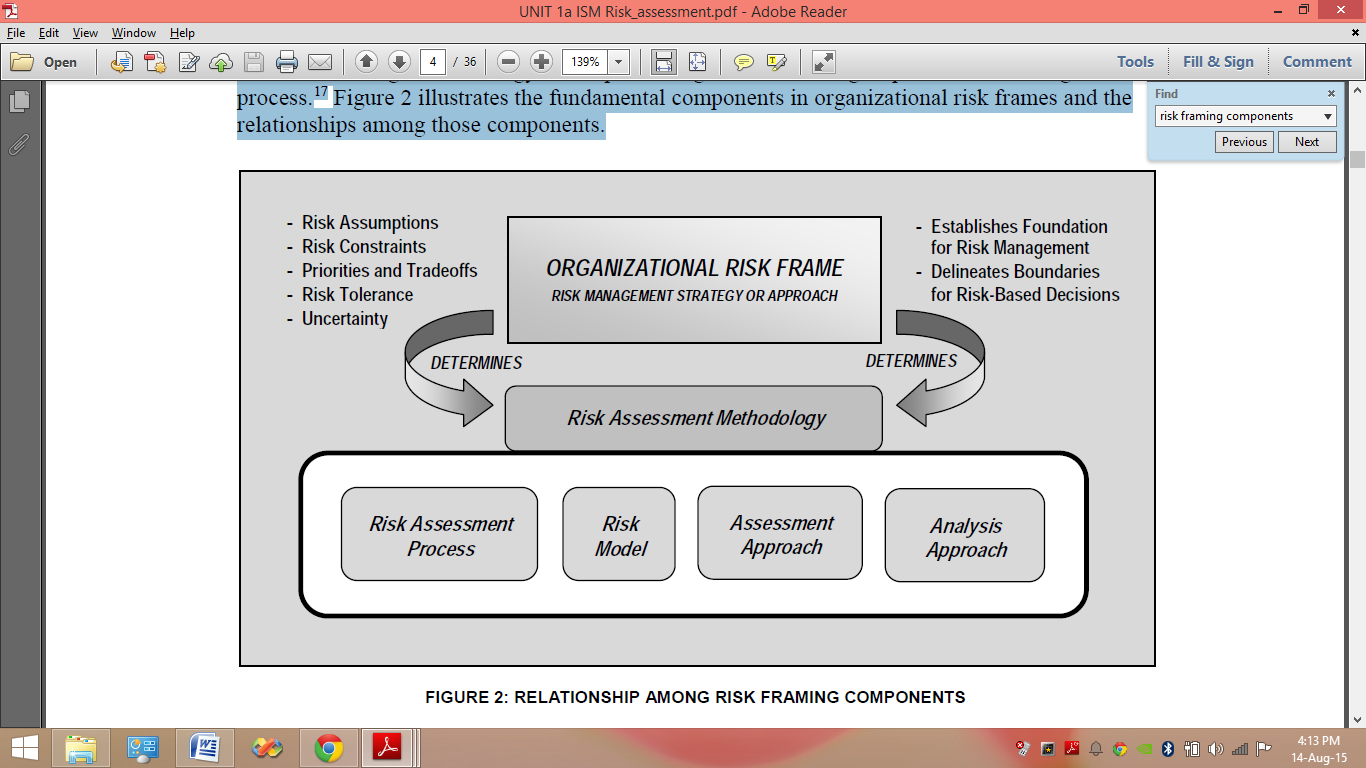
(ii) an explicit *risk model*, defining key terms and assessable risk factors and the relationships among the factors;

(iii) an *assessment approach* (e.g., quantitative, qualitative, or semi-qualitative), specifying the range of values those risk factors can assume during the risk assessment and how combinations of risk factors are identified/analyzed so that values of those factors can be functionally combined to evaluate risk; and

(iv) an *analysis approach* (e.g., threat-oriented, asset/impact-oriented, or vulnerability-oriented), describing how combinations of risk factors are identified/analyzed to ensure adequate coverage of the problem space at a consistent level of detail.

* Risk assessment methodologies are defined by organizations and are a component of the risk management strategy developed during the risk framing step of the risk management process.

Figure 2 illustrates the fundamental components in organizational risk frames and the relationships among those components.



**1.Risk Assessment Process:**

* 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; and

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

**2. Risk Models:**

* *Risk models* define the *risk factors* to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments.
* Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition.

**3.Assessment approach:**

* 1. **Quantitative:**

*Quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

* 1. **Qualitative:**

*Qualitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high).

**4.Analysis approach:**

* Analysis approaches differ with respect to the orientation or 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

(iii) vulnerability oriented

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

**Ans:**

**Valuing Assets:**

* Determining the monetary value of an asset is an important part of security risk

management. Business managers often rely on the value of an asset to guide them in determining how much money and time they should spend securing it.

* Many organizations maintain a list of asset values (AVs) as part of their business continuity plans.
* Note how the numbers calculated are actually subjective estimates, though: No

objective tools or methods for determining the value of an asset exist. To assign a value to an asset, calculate the following three primary factors:

**1.The overall value of the asset to your organization**.

* Calculate or estimate the asset’s value in direct financial terms.
* Consider a simplified example of 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.

2.**The immediate financial impact of losing the asset**.

* If you deliberately simplify the 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.
* In reality, most e-commerce Web sites generate revenue at a wide range of rates depending upon the time of day, the day of the week, the season, marketing campaigns, and other factors.
* Additionally, some customers may find an alternative Web site that they prefer to the original, so the Web site may have some permanent loss of users.
* Calculating the revenue loss is actually quite complex if you want to be precise and consider all potential types of loss.

**3.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:**

**Same as Q.6.**

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

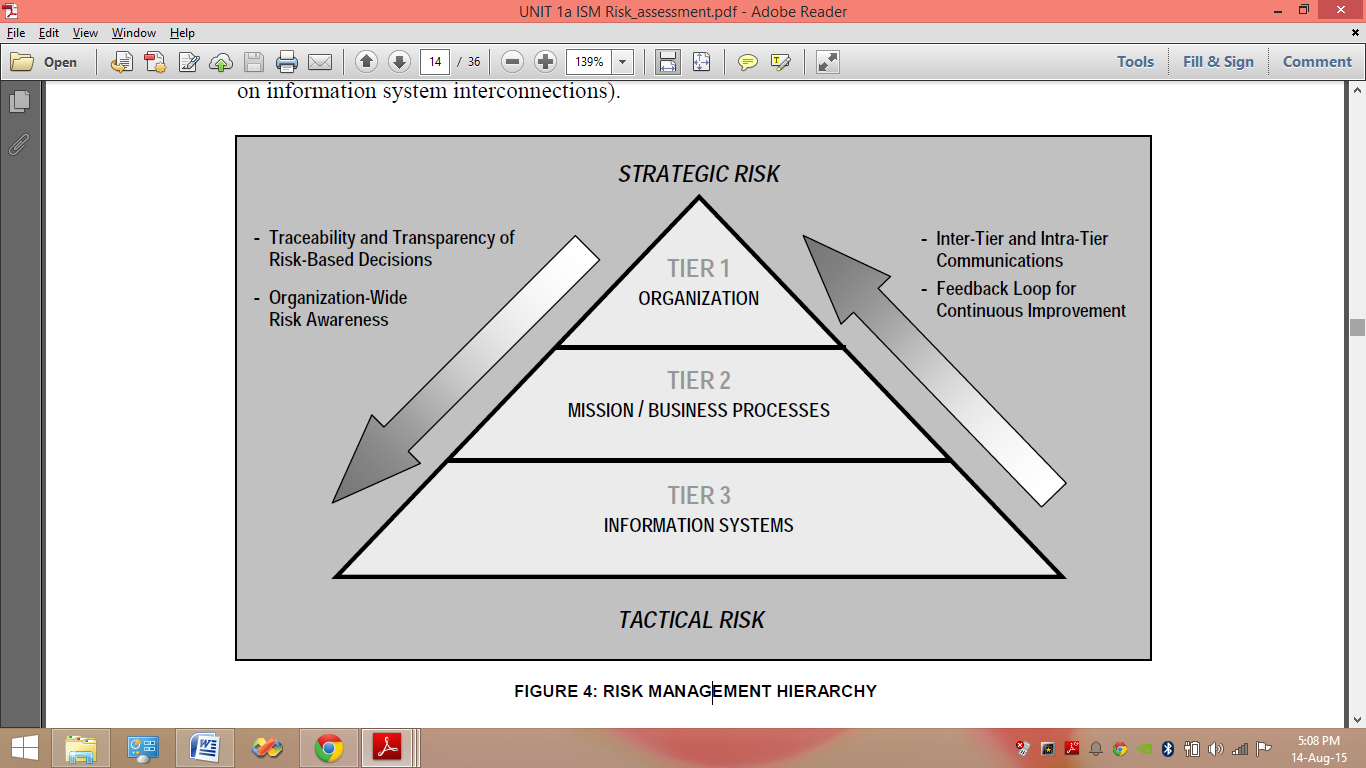
**Ans:**

**Refer Q.6.**

**Q.19. With neat diagram explain the risk management hierarchy.**

**Ans:**

* Risk assessments can be conducted at all three tiers in the risk management hierarchy—*organization level*, *mission/business process level*, and *information system level*.
* Figure 4 illustrates the risk management hierarchy, which provides multiple risk perspectives from the strategic level to the tactical level.
* Traditional risk assessments generally focus at the Tier 3 level (i.e., information system level) and as a result, tend to overlook other significant risk factors that may be more appropriately assessed at the Tier 1 or Tier 2 levels (e.g., exposure of a core mission/business function to an adversarial threat based on information system interconnections).

****

Risk assessments support risk response decisions at the different tiers of the risk management hierarchy.

**Tier 1:**

At Tier 1, risk assessments can affect, for example:

1. organization-wide information security programs, policies, procedures, and

guidance;

1. the types of appropriate risk responses (i.e., risk acceptance, avoidance,

mitigation, sharing, or transfer);

1. investment decisions for information technologies/systems;

(iv) procurements;

(v) minimum organization-wide security controls;

(vi) conformance to enterprise/security architectures; and

(vii) monitoring strategies and ongoing authorizations of information systems and

**Tier 2:**

At Tier 2, risk assessments can affect, for example:

1. enterprise architecture/security architecture design decisions;
2. the selection of common controls;
3. the selection of suppliers, services, and contractors to support organizational missions/business functions;
4. the development of risk-aware mission/business processes; and
5. the interpretation of information security policies with respect to organizational information systems and environments in which those systems operate.

**Tier 3:**

Finally, at Tier 3, risk assessments can affect, for example:

1. design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems);
2. implementation decisions (including whether specific information technology products or product configurations meet security control requirements); and
3. operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

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

**Ans:**

* At Tier 1, risk assessments support organizational strategies, policies, guidance, and processes for

managing risk. Risk assessments conducted at Tier 1 focus on organizational operations, assets, and individuals—comprehensive assessments across mission/business lines.

For example, Tier 1 risk assessments may address:

* 1. the specific types of threats directed at organizations that may be different from other organizations and how those threats affect policy decisions;
  2. systemic weaknesses or deficiencies discovered in multiple organizational information systems capable of being exploited by adversaries;
  3. the potential adverse impact on organizations from the loss or compromise of organizational information (either intentionally or unintentionally); and
  4. 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.
* Organization-wide assessments of risk can be based solely on the assumptions, constraints, risk tolerances, priorities, and trade-offs established in the risk framing step (i.e., derived primarily from Tier 1 activities).
* However, more realistic and meaningful risk assessments are based on assessments conducted across multiple mission/business lines (i.e., derived primarily from Tier 2 activities).
* The ability of organizations to effectively use Tier 2 risk assessments as inputs to Tier 1 risk assessments is shaped by such considerations as:
  + the similarity of organizational missions/business functions and mission/business processes; and
  + the degree of autonomy that organizational entities or subcomponents have with respect to parent organizations.
* 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 (COOP) 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:**

* The Tier 2 context and the system development life cycle determine the purpose and define the scope of risk assessment activities at Tier 3.
* While initial risk assessments (i.e., risk assessments performed for the first time, rather than updating prior risk assessments) can be performed at any phase in the system development life cycle, ideally these assessments should be performed in the Initiation phase.
* In the Initiation phase, risk assessments evaluate the anticipated vulnerabilities and predisposing conditions affecting the confidentiality, integrity, and availability of information systems in the context of the planned environments of operation.
* Such assessments inform risk response, enabling information system owners/program managers, together with mission/business owners to make the final decisions about the security controls necessary based on the security categorization and the environment of operation.
* Risk assessments are also conducted at later phases in the system development life cycle, updating risk assessment results from earlier phases.
* These risk assessment results for as-built or as-deployed information systems typically include descriptions of vulnerabilities in the systems, an assessment of the risks associated with each vulnerability (thereby updating the assessment of vulnerability severity), and corrective actions that can be taken to mitigate the risks.
* The risk assessment results also include an assessment of the overall risk to the organization and the information contained in the information systems by operating the systems as evaluated.
* Risk assessment results at Tier 3 are communicated to organizational entities at Tier 1 and Tier 2.
* Risk assessment activities can be integrated with the steps in the Risk Management Framework (RMF).

***RMF Step 1 – Categorize:***

* Organizations can use initial risk assessments to make security categorization decisions consistent with the risk management strategy provided by the risk executive (function) and as a preparatory step to security control selection.

***RMF Step 2 – Select:***

* Organizations can use risk assessments to inform and guide the selection of security controls for organizational information systems and environments of operation.

***RMF Step 3 – Implement:***

* Organizations can use risk assessment results to identify alternative implementations of selected security controls (e.g., considering vulnerabilities inherent in one security control implementation versus another).

***RMF Step 4 – Assess:***

* Organizations can use the results from security control assessments to inform risk assessments. Security control assessments (documented in security assessment reports) identify vulnerabilities in organizational information systems and the environments in which those systems operate.

***RMF Step 5 – Authorize:***

* Organizations can use risk assessment results to provide risk-related information to authorizing officials. The risk responses carried out by organizations based on the risk assessments result in a known security posture of organizational information systems and environments of operation.

***RMF Step 6 – Monitor:***

* Organizations can update risk assessments on an ongoing basis using security-related information from organizational continuous monitoring processes.

**Q.22. Explain the quantitative risk assessment.**

**Ans:**

* 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.
* You endeavor to use the same objectivity when computing asset exposure, cost of

controls, and all of the other values that you identify during the risk management process.

There are some significant weaknesses inherent in this approach that are not easily

overcome.

* First, there is no formal and rigorous way to effectively calculate values for

assets and controls. In other words, while it may appear to give you more detail, the financial values actually obscure the fact that the numbers are based on estimates. How can you precisely and accurately calculate the impact that a highly public security incident might have on your brand? If it is available you can examine historical data, but quite often it is not.

* Second, organizations that have tried to meticulously apply all aspects of quantitative risk management have found the process to be extremely costly. Such projects usually take a very long time to complete their first full cycle, and they usually involve a lot of staff members arguing over the details of how specific fiscal values were calculated.
* Third, for organizations with high value assets, the cost of exposure may be so high that you would spend an exceedingly large amount of money to mitigate any risks to which you were exposed. This is not realistic, though; an organization would not spend its entire budget to protect a single asset, or even its top five assets.

Some of the factors and values that are typically evaluated during a quantitative risk assessment such as asset valuation; costing controls; determining Return On Security Investment (ROSI); and calculating values for Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), and Annual Loss Expectancy (ALE).

**Valuing Assets:**

Determining the monetary value of an asset is an important part of security risk

management. Business managers often rely on the value of an asset to guide them in

determining how much money and time they should spend securing it.

**Determining the ARO:**

The ARO is the number of times that you reasonably expect the risk to occur during one year. Making these estimates is very difficult; there is very little actuarial data available. What has been gathered so far appears to be private information held by a few property insurance firms.

**Determining the ALE:**

The ALE is the total amount of money that your organization will lose in one year if

nothing is done to mitigate the risk. Calculate this value by multiplying the SLE by the ARO. The ALE is similar to the relative rank of a qualitative risk analysis.

**Determining Cost of Controls:**

Determining the cost of controls requires accurate estimates on how much acquiring,

testing, deploying, operating, and maintaining each control would cost. Such costs would include buying or developing the control solution; deploying and configuring the control solution; maintaining the control solution; communicating new policies or procedures related to the new control to users; training users and IT staff on how to use and support the control; monitoring the control; and contending with the loss of convenience or productivity that the control might impose.

**ROSI:**

Estimate the cost of controls by using the following equation:

(ALE before control) – (ALE after control) – (annual cost of control) = ROSI

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

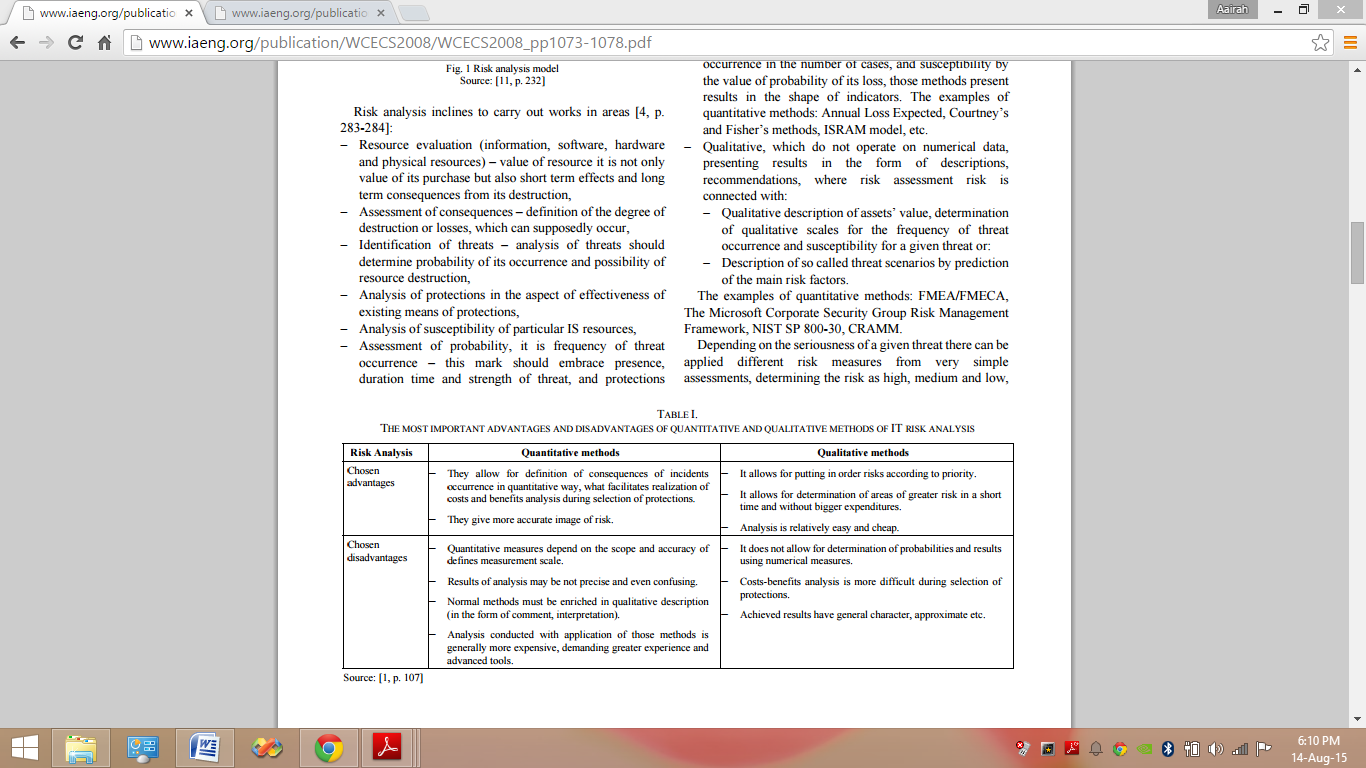
**Ans:**

**Quantitative Risk:**

* Quantitative Risk Analyses assign fixed numerical values (within a margin of error) to both the probability and utility (business impact) of an outcome.
* A quantitative risk analysis is a further analysis of the highest priority risks during a which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project.
* Quantitative Risk Analysis maps a cost, a monetary loss, to a particular risk exposure.
* Quantitative risk analysis deals with a lot of probabilities and more mathematical tools, such as Monte Carlo simulation and such, in order to have answer like we have a 30% chance for a delay in a shipment, or a loss of a supplier.
* project-level.
* probabilistic estimates of time and cost.
* time consuming.
* may require specialized tools.

**Qualitative Risk:**

* Qualitative Risk Analysesdon’t. Instead, they represent both the probability and utility of an outcome using an interval scale, where each interval includes a range of numerical values (beyond the margin of error) and each interval is typically represented by a non-numerical label (such as the words “High”, “Medium”, “Low”), not the ranges of values those labels represent.
* A qualitative risk analysis prioritizes the identified project risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurring and the impact on project objectives should they occur.
* Qualitative risk is a rank for risks during any project where it tasks a number or letter as per the category approved by risk team and project management.
* Qualitative risk analysis will provide you with the nature of risk and uncertainty you are dealing with, you can label them in a way that in a graph you'll see the treaths such as construction accidents or the absentiesm of workers.
* risk-level.
* subjective evaluation of probability and impact.
* quick and easy to perform.
* no special software or tools required.



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

**Ans:**

The risk assessment process43 is composed of four steps:

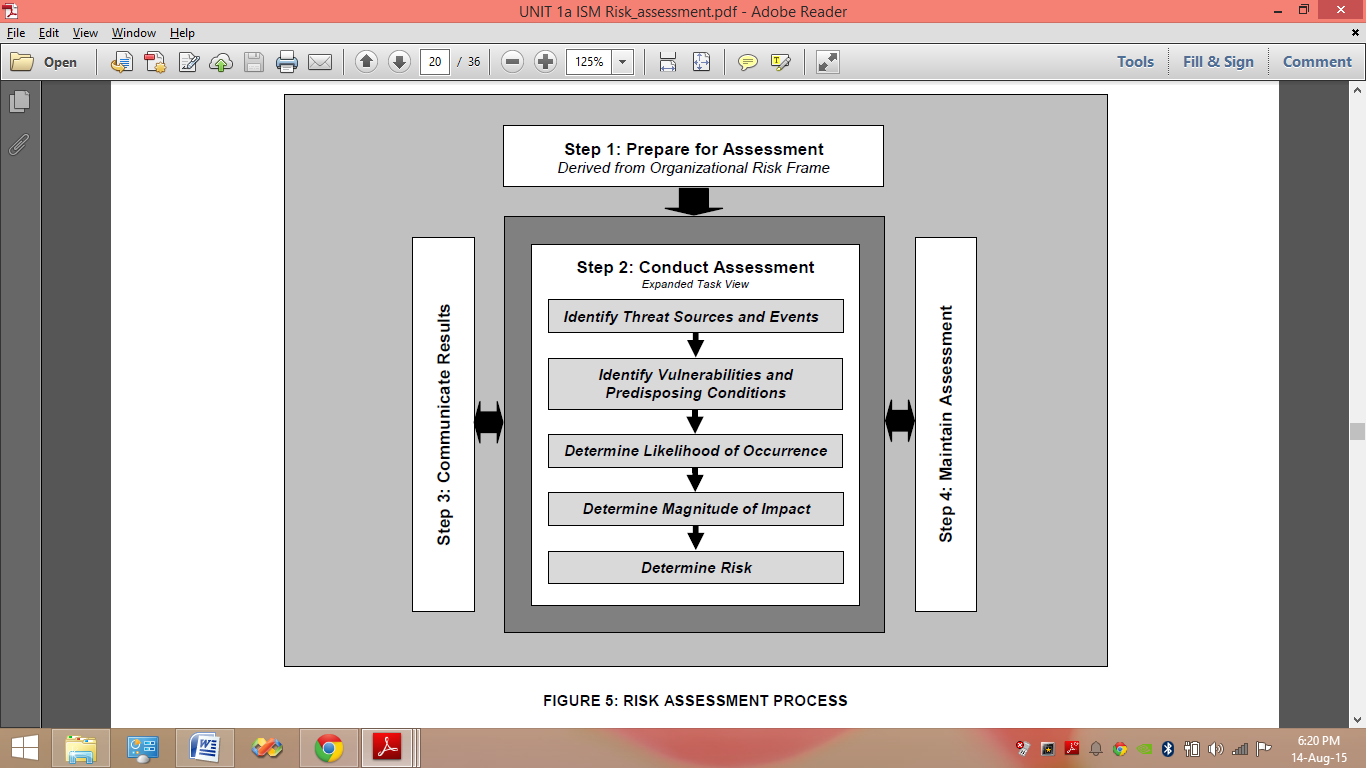
(i) *prepare* for the assessment;

(ii) *conduct* the assessment;

(iii) *communicate* assessment results; and

(iv) *maintain* the assessment.

Figure 5 illustrates the basic steps in the risk assessment process and highlights the specific tasks for conducting the assessment.



**1.PREPARING FOR THE RISK 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:

• Identify the purpose of the assessment;

• Identify the scope of the assessment;

• Identify the assumptions and constraints associated with the assessment;

• Identify the sources of information to be used as inputs to the assessment; and

• Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

**2.CONDUCTING THE RISK 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:

• Identify threat sources that are relevant to organizations;

• Identify threat events that could be produced by those sources;

• Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;

• Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;

• Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and

• Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

**3.COMMUNICATING AND SHARING RISK ASSESSMENT INFORMATION:**

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 theorganization have the appropriate risk-related information needed to inform and guide risk decisions.

Communicating and sharing information consists of the following specific tasks:

• Communicate the risk assessment results; and

• Share information developed in the execution of the risk assessment, to support other risk management activities

**4.MAINTAINING THE RISK 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. The results of risk assessments inform risk management decisions and guide risk responses.

Maintaining risk assessments includes the following specific tasks:

• Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors; and

• Update the components of risk assessments reflecting the monitoring activities carried out by organizations.