4.3 Security, IS Vulnerability, Disaster Management

4.3.1 Security:

Information security, sometimes shortened to Info Sec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)

4.3.2 Need for Information Security:

Information security is essential for protecting sensitive and valuable data from unauthorized access, use, disclosure, disruption, modification, or destruction. Here are some of the key reasons why information security is important:

Protecting Confidential Information: Confidential information, such as personal data, financial records, trade secrets, and intellectual property, must be kept secure to prevent it from falling into the wrong hands. This type of information is valuable and can be used for identity theft, fraud, or other malicious purposes.

Complying with Regulations: Many industries, such as healthcare, finance, and government, are subject to strict regulations and laws that require them to protect sensitive data. Failure to comply with these regulations can result in legal and financial penalties, as well as damage to the organization's reputation.

Maintaining Business Continuity: Information security helps ensure that critical business operations can continue in the event of a disaster, such as a cyber-attack or natural disaster. Without proper security measures in place, an organization's data and systems could be compromised, leading to significant downtime and lost revenue.

Protecting Customer Trust: Customers expect organizations to keep their data safe and secure. Breaches or data leaks can erode customer trust, leading to a loss of business and damage to the organization's reputation.

Preventing Cyber-attacks: Cyber-attacks, such as viruses, malware, phishing, and ransomware, are becoming increasingly sophisticated and frequent. Information security helps prevent these attacks and minimizes their impact if they do occur.

Protecting Employee Information: Organizations also have a responsibility to protect employee data, such as payroll records, health information, and personal details. This information is often targeted by cybercriminals, and its theft can lead to identity theft and financial fraud.

4.3.3 Definition

1. "Preservation of confidentiality, integrity and availability of information.
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)."
4. "Information Security is the process of protecting the intellectual property of an organization."
5. "Information security is a risk management discipline; whose job is to manage the cost of information risk to the business."

4.3.4 Principles of Security:

The CIA triad of confidentiality, integrity, and availability is at the heart of information security. (The members of the classic Info Sec triad -confidentiality, integrity and availability - are interchangeably referred to in the literature as security attributes properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) There is continuous debate about extending

this classic trio. Other principles such as Accountability have sometimes been proposed for addition it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer systems has increased (particularly amongst the Western nations) Legality is becoming a key consideration for practical security installations.

In 1992 and revised in 2002 the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

4.3.4.1 Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity

in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

4.3.4.2 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

4.3.4.3 Authenticity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

4.3.5 Risk management

The Certified Information Systems Auditor (CISA) Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk analysis and risk evaluation processes have their limitations since, when security incidents occur, they emerge in a context, and their rarity and even their uniqueness give rise to unpredictable threats.

The analysis of these phenomena which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach which is able to examine and interpret subjectively the detail of each incident.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed.

The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human The ISO/IEC 27002:2005

Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security
- physical and environmental security,
- communications and operations management, access control,
- information systems acquisition, development and maintenance,
- information security incident management,
- business continuity management, and
- Regulatory compliance.

In broad terms, the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, and other), and supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost-effective protection without discernible loss of productivity.

4.3.6 IS Vulnerability :

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three

elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.
In this frame, vulnerability is also known as the attack surface.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

A security risk may be classified as vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is tied to the potential of a significant loss. Then there are vulnerabilities without risk: for example when the affected asset has no value. Vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability a vulnerability for which can exploit exists. The window of vulnerability is the time from when the security hole was introduced or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attackers was disabled see zero-day attack.

A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.

1. **Software Vulnerabilities**:

   These are weaknesses in software code that can be exploited to compromise the security of a system. Common examples include bugs, coding errors, or design flaws in applications and operating systems.

2. **Hardware Vulnerabilities**:

   Weaknesses in hardware components can expose systems to security risks. This might include vulnerabilities in computer processors, memory, or other hardware devices.

3. **Configuration Vulnerabilities**:

Insecure or misconfigured settings in software, servers, network devices, or other components can create vulnerabilities. This may include default passwords, unnecessary services, or open ports.

4. **Human-Related Vulnerabilities**:

Human factors, such as poor security awareness, lack of training, and social engineering attacks, can introduce vulnerabilities. For example, employees falling victim to phishing emails may compromise the security of an organization.

5. **Outdated Software and Patching:**

Failure to update and patch software regularly can leave systems vulnerable to known security issues. Hackers often exploit unpatched vulnerabilities to gain unauthorized access.

6. **Zero-Day Vulnerabilities:**

These are vulnerabilities that are unknown to the software vendor or the public. Cybercriminals often seek to exploit zero-day vulnerabilities because there are no patches or defenses available.

7. **Web Application Vulnerabilities**:

Web applications may have vulnerabilities such as SQL injection, cross-site scripting (XSS), or insecure file uploads. These can be exploited to compromise data or gain unauthorized access.

8. **Insufficient Authentication and Authorization**:

Weaknesses in authentication and authorization mechanisms can lead to unauthorized access. This might include weak passwords, lack of multi-factor authentication, or improper access controls.

9. **Supply Chain Vulnerabilities**:

Threats can exploit vulnerabilities in the supply chain, including compromised hardware or software components introduced during the manufacturing or distribution process.

10. **Environmental Vulnerabilities**:

Factors such as physical security, power supply, and environmental conditions can impact the overall security of information systems.

11. Denial of Service (DoS) Vulnerabilities:

Systems may be vulnerable to DoS attacks, where attackers flood a network, system, or service with traffic to disrupt normal operation.

To mitigate information security vulnerabilities, organizations implement strategies such as regular security assessments, vulnerability scanning, penetration testing, and the prompt application of security patches. A proactive and layered approach to security helps minimize the risks associated with vulnerabilities.

4.3.7 Disaster Management

4.3.7.1 Objectives

1. To overcome limitation of existing system.
2. Effective utilizations of natural resources database in event of disaster.
3. Building decision support system for better district administration
4. Providing vital information related to pre-disaster and post-disaster at fingertips.
5. Facilitating users for easy data integration.
6. Editing, updating of spatial and non-spatial data at ease.
7. To assist in post disaster damage assessment analysis.
8. Provide centralized system that would be time & cost effective and maintenance free. o Development of user friendly customized DMIS software.

"Disaster management" means a continuous and integrated process of planning, organizing, coordinating and implementing measures which are necessary or expedient for prevention of danger or threat of any disaster, mitigation or reduction of risk of any disaster or its severity or consequences, capacity-building, preparedness to deal with any disaster, prompt response to any threatening disaster situation or disaster, assessing the severity or magnitude of effects of any disaster, evacuation,

rescue and relief, rehabilitation and reconstruction. Disaster Management comprises all forms of activities including structural and non-structural measures to avoid (i.e. prevention) or to limit (i.e. mitigation and preparedness) adverse effects of disasters in the pre-disaster phase and post disaster stage like Response, Relief, Recovery, & Reconstruction.

As per the directives laid under GOI-UNDP program, the Government of Maharashtra (GOM) has a Disaster Management Unit (DMU), which prepares action plan to support and strengthen the efforts of district administration for overall disaster vigilance of the State. In view of preparedness, each district has evolved its own district disaster management action plan (DDMAP). It is anticipated that these multi-hazard response plans would increase the effectiveness of administrative intervention.

The DDMAP addresses the districts 'response to disaster situations such as earthquakes, floods, cyclones, epidemics, off-site industrial disasters, roads accidents and fires. Some of these disasters such as floods and earthquakes affect widespread area causing extensive damage to life, property and environment while disaster like epidemics only affect populations. Anyhow, the management of these disasters requires far-reaching resources and manpower for containment by remedial action.

As a part of said project, Government of Maharashtra (GOM) entrusted the development of Disaster Management Information System (DMIS) to Maharashtra Remote Sensing Applications Centre (MRSAC) at the initiative of Relief and Rehabilitation Department. The project thrusts on requirements of the user department viz., Relief & Rehabilitation Department and District Administrations in Maharashtra State.

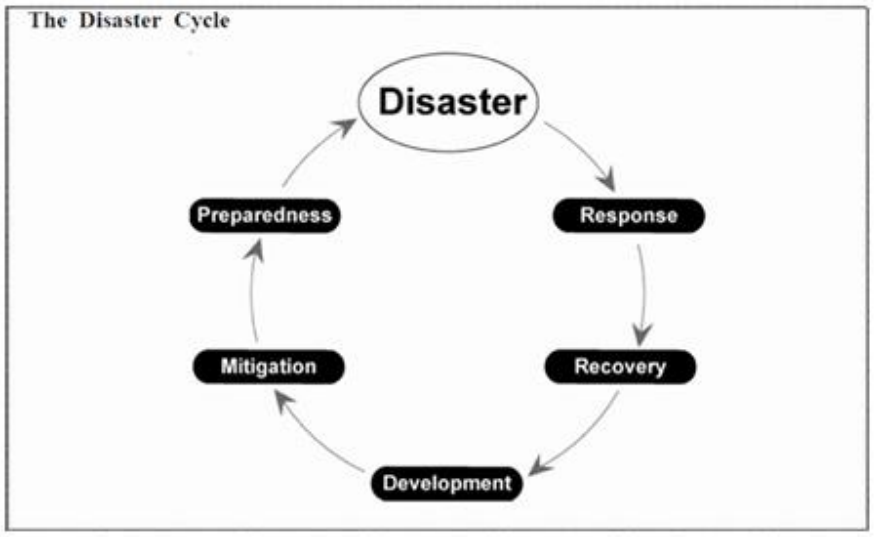
Methodology:

1. GIS is a powerful technology that can assist decision-making in all phases of the disaster management cycle. GIS tools are used for integrating the geographic (i.e. location) and the associated attribute data pertaining to the location and its spatial relationship with numerous other parameters, to carry out effective spatial planning, minimize the possible damage, ensure immediate action when required and prioritize actions for long-term risk reduction.

2. Resources database on various themes obtained through Remote Sensing data has been compiled for all the districts of Maharashtra. Similarly attribute data on Demography & Census, government core sectors, and past disaster have been integrated in the DMIS. Spatial and non-spatial database has been generated in GIS environment.
3. A customized system has been developed for each district for prioritizing hazards for use in developing Mitigation Strategies, Risk Estimation and Hazard and Vulnerability Mapping.
4. A user-friendly menu driven software has been developed in Arc GIS using Arc Objects with Visual Basic 6.0. It has been designed and customized keeping in mind the skill level of the expected users at the district level. The methodology and database has been customized for easy implementation.
5. High resolution satellite data for the study area are analyzed for generation of base map as well as DEM. Slopes (or Contours) generated from DEM is used for locating shelter camps in event of disaster.
6. The themes like Slope, Landuse, and Geology are amalgamated so as to calculate weighted ranks that indicate vulnerability index. For example, Slope (0-1%) + Landuse (River, Reservoir, Double Cropped) + Geology (water body mask, deep alluvial plain) = Rank 1. This index will decide the sensitivity of the flood prone area i.e. very high-risk area, high-risk area, moderate risk area, low risk area and no risk area.
7. The software has been thoroughly tested before its packaging and deployment. Each district user is authenticated for accessing data in DMIS software.
8. Standard DMIS software has been developed using prototyping model of Software Development Life Cycle (SDLC). The final software has been installed and implemented in Relief and Rehabilitation Cell at Mantralaya, Mumbai, Maharashtra State.
9. The DMIS is installed and implemented in all districts of Maharashtra State followed by demonstration to District Collector and training to concerned officials. The User Guide Manuals are provided to users for further guidance and operating software at ease. Detail requirement analysis of the user had been done with

respect to the standard procedures followed during disaster and effort is taken to incorporate the same in the software.

Disaster Cycle:



To effectively coordinate this cycle, disaster-management leaders must develop a number of critical skills. The skills necessary for each stage of the cycle are as follows:

Prevention

During the prevention stage, strong analytical skills help leaders identify potential threats, hazards and high-risk areas. Problem-solving abilities are also invaluable in identifying the best ways to avoid or diminish the likelihood of catastrophic events.

Mitigation

Planning is an important skill during the mitigation stage; the disaster-management leader will need to develop strategies and structural changes that can help mediate potential threats. Spreading awareness is also critical, as community members must be made aware of the steps they can take to prepare for all contingencies.

“Of the five stages, mitigation is the most crucial because, if done correctly, it can reduce the impact of the next emergency or crisis,” explains Claire Connolly Knox, associate professor and emergency and crisis management academic program coordinator at the University of Central Florida. “As per the National Institute of Building Science, for every $1 spent on mitigation, there is a $6 savings post-disaster. Mitigation can include changes to building codes as seen following Hurricane Andrew in 1992 or reinforcing infrastructure as seen in coastal communities in response to sea-level rise and climate change.”

Preparedness

During the preparedness stage, it’s important to be skilled in training people to respond to disasters. It’s important to stay organized, which is the best way to ensure readiness. Oral and written communication skills prepare laypeople and emergency-response personnel for action in worst-case scenarios.

Response

The ability to quickly make decisions is crucial here, as the response stage is time-sensitive. Another valuable skill is delegating essential tasks to other volunteers or emergency responders.

Recovery

As disaster-management leaders help their communities recover, the most essential skills are empathy, understanding and relationship building; indeed, without earning the trust of the community, any recovery efforts are likely to come up short.

****