# TRAINING DAY 5 REPORT:

- ## Risk Management & Methodology

Today, I learned about **Risk Management**, which helps organizations **identify, analyze, and handle potential risks** to minimize negative impacts.

### What is Risk Management?

**Risk Management** is the process of **identifying, assessing, and controlling threats** to an organization's assets, operations, or reputation. These threats could come from cyberattacks, natural disasters, human error, or other sources.

### Why is it Important?

- Protects **business continuity**.

- Reduces **financial losses**.

- Improves **decision-making** and organizational resilience.

- Ensures **legal and regulatory compliance**.

### Risk Management Methodology :

The risk management process includes these key steps

1. *Establish Context*

   - Define the **scope, objectives, and environment** of risk management.

   - *Understand the* **internal and external factors** *affecting the organization.*

2. *Risk Identification*

   - Identify all **possible risks** that could affect the organization's goals, operations, assets, or reputation.

   - *Use methods like brainstorming, checklists, interviews, or historical data.*

3. *Risk Analysis*

   - Analyze identified risks to determine **likelihood (probability) and potential impact**.

   - *Tools like risk matrices or quantitative methods help prioritize risks.*

4. *Risk Assessment and Evaluation*

**- Compare analyzed risks with risk criteria** set during context establishment.

*- Decide which risks need treatment, acceptance, or monitoring.*

5. *Risk Mitigation (Treatment)*

   - Develop strategies to **reduce, transfer, accept, or avoid risks**.

   *- Implement security controls, policies, insurance, or contingency plans.*

6. *Risk Monitoring*

   - Continuously **track identified risks and detect new ones**.

   *- Assess effectiveness of risk controls and update strategies as needed.*

7. *Communicate and Consult*

   - Keep **stakeholders informed** throughout the risk management process.

   - Engage with relevant teams to gather feedback and ensure everyone understands the risks and controls.

- ## Software and Hardware Requirements

### Hardware Requirements

These are the **physical components of a computer system**, which determine how well it can perform tasks:

1. *Processor (CPU)*

   - A modern multi-core processor (e.g., Intel i5/i7, AMD Ryzen 5/7) for faster performance.

   *- Higher clock speeds improve system responsiveness.*

2. *RAM (Memory)*

   - Minimum **8 GB RAM** recommended.

   **- 16 GB or more** preferred for tasks like virtual machines, pentesting tools, and running multiple applications.

3. *GPU (Graphics Processing Unit)*

   *- Not always required for ethical hacking, but a dedicated GPU (e.g., NVIDIA/AMD) is useful for tasks like password cracking or GPU-based computations.*

4. *Hard Disk / Storage*

   - Minimum **250 GB SSD or HDD** recommended.

   **- SSD preferred** for faster boot times and data access.

   - *More storage needed for large datasets, logs, and virtual machines.*

5. *Network Adapters*

   - Integrated Ethernet/Wi-Fi adapter for connectivity.

   **- External USB Wi-Fi adapters** supporting monitor mode and packet injection (e.g., Alfa AWUS036NHA) for wireless pentesting.

## Software Requirements

These include **operating systems, tools, and applications** needed for the work:

1. *Operating System*

   - Linux distributions like **Kali Linux, Parrot Security, or BlackArch** for pentesting.

   - *Windows (10/11) or macOS for compatibility with general tools.*

**2.** *Virtualization Software*

   **- VMware Workstation, VirtualBox, or Hyper-V** *to run virtual machines for safe testing.*

*3.* *Pentesting Tools*

   - *Tools like* **Nmap, Metasploit, Wireshark, Burp Suite, John the Ripper**, *etc.*

**4.** *Programming Languages*

   **- Python, Bash, or Perl** *interpreters for scripting and automation.*

**5.** *Text Editors/IDEs*

   **-VS Code, Sublime Text, Atom**, *or any code editor.*

6. *Other Utilities*

   - Web browsers with extensions for testing, password managers, and encryption tools.

- ## Dual Boot vs. Virtual Machine

### Dual Boot

- Dual booting means **installing two (or more) operating systems on separate partitions** of your hard drive.

- At startup, you choose which OS to load (e.g., Windows or Linux).

- Both OSs have **full access to the system's hardware**, giving **better performance**.

- Best when you need **maximum speed** or use resource-heavy apps.

- Example: Installing **Kali Linux alongside Windows** for pentesting.

**Advantages**

1. Full hardware performance
2. Good for gaming, graphics work, or heavy tasks
3. Stable and reliable

**Disadvantages**

1. Requires restarting to switch OS
2. Risk of accidentally deleting data or corrupting bootloader
3. Harder to share files live between OSs

## Virtual Machine (VM)

- A VM lets you **run an OS inside another OS**, like a computer within a computer.

- Uses **virtualization software** (e.g., VMware, VirtualBox) to create virtual systems.

- Easier to **run multiple OSs simultaneously** (e.g., using Windows while testing Linux in a VM).

- Great for **testing, ethical hacking, development, or learning**.

### Advantages

1. Run multiple OSs at the same time

2. Easy snapshots & backups
3. Safer testing of malware or exploits
4. Easy to delete or recreate VMs

### Disadvantages

1. Requires **more RAM and CPU power**
2. Performance not as fast as native install
3. Relies on host OS stability

## • Downloading VMware

### How to Download VMware Workstation Player

**-** VMware Workstation Player is a **free virtualization software** you install on your computer to create and run virtual machines.

- To download:

- Go to the official VMware website:
  Download VMware Workstation Player
- Choose the version for your operating system (Windows or Linux).
- Click **Download Now**.
- Once downloaded, **install it like any other software**:

  Open the installer → Click **Next** through the steps → Accept license → Finish installation.

### Downloading a Virtual Machine (ISO)

- The **ISO file** is like the installation disk of the operating system you want to run inside VMware.

- Examples of popular Linux ISOs for ethical hacking or learning:

**Kali Linux ISO** (for pentesting):
- Download Kali Linux ISO

**Ubuntu ISO** (for general Linux use):

Steps:

- Open the download link.
- Choose the right version (usually the latest stable release).
- Download the ISO file and **save it to your computer** (remember the folder location).