I. **Identification of Threats:**

-External Threats: These come from outside the organization and may include malicious actors such as hackers, cybercriminals, or state-sponsored entities.

-Internal Threats: These arise from within the organization and can involve employees, contractors, or other individuals with access to the network.

II. **Vulnerability Assessment:**
III. **Risk Assessment:**
IV. **Asset Valuation:**

Identify and prioritize the critical assets within the organization, such as sensitive data, intellectual property, or critical infrastructure.

Assess the potential impact on these assets in the event of a security breach.

V. **Likelihood Assessment:**

Evaluate the likelihood of each threat occurring based on historical data, threat intelligence, and the organization's specific context.

VI. **Prioritization:**

Prioritize identified threats based on the level of risk they pose to the organization.

This helps allocate resources effectively, focusing on addressing the most significant threats first.

VII. **Mitigation Strategies:**
VIII. **Continuous Monitoring:**
IX. **Incident Response Planning:**