**The Basis of Security Testing**: This topic can cover the basics of security testing, including its definition, objectives, and types. You can also discuss the importance of security testing in today’s digital world and the challenges associated with it.

**1.Security Risks**: This topic can cover the various types of security risks that organizations face, including cyber-attacks, data breaches, and insider threats. You can also discuss the impact of security risks on businesses and the steps that organizations can take to mitigate them.

Here is a presentation topic that you can consider for **Security Risks**:

1. **Security Risks and Threats**: This topic can cover the various types of security risks and threats that organizations face, including cyber attacks, data breaches, and insider threats. You can also discuss the impact of security risks on businesses and the steps that organizations can take to mitigate them.

Here is a brief outline of the presentation:

* Introduction
  + Definition of security risks and threats
  + Importance of security risks and threats
* Types of Security Risks and Threats
  + Cyber attacks
  + Data breaches
  + Insider threats
  + Social engineering attacks
  + Malware and viruses
* Impact of Security Risks and Threats
  + Financial losses
  + Reputation damage
  + Legal and regulatory consequences
* Mitigating Security Risks and Threats
  + Risk assessment and management
  + Security policies and procedures
  + Employee training and awareness
  + Security technologies and tools

1. **The Role of Risk Assessment in Security Testing**: This topic can cover the importance of risk assessment in security testing, including its objectives, benefits, and limitations. You can also discuss the various risk assessment techniques that are commonly used in security testing.
2. **Asset Identification**: This topic can cover the process of identifying and classifying assets in an organization, including hardware, software, and data. You can also discuss the importance of asset identification in security testing and the challenges associated with it.
3. **Analysis of Risk Assessment Techniques**: This topic can cover the various risk assessment techniques that are commonly used in security testing, including qualitative and quantitative methods. You can also discuss the strengths and weaknesses of each technique and the factors that influence their effectiveness.
4. **Information Security Policies and Procedures**: This topic can cover the importance of information security policies and procedures in an organization, including their objectives, scope, and implementation. You can also discuss the various types of policies and procedures that are commonly used in security testing.
5. **Understanding Security Policies and Procedures**: This topic can cover the key concepts and principles of security policies and procedures, including confidentiality, integrity, and availability. You can also discuss the importance of security policies and procedures in maintaining the security of an organization’s assets.
6. **Analysis of Security Policies and Procedures**: This topic can cover the various security policies and procedures that are commonly used in security testing, including access control, authentication, and authorization. You can also discuss the strengths and weaknesses of each policy and procedure and the factors that influence their effectiveness.
7. **Security Auditing and Its Role in Security Testing**: This topic can cover the importance of security auditing in security testing, including its objectives, benefits, and limitations. You can also discuss the various types of security audits that are commonly used in security testing.
8. **Purpose of a Security Audit**: This topic can cover the key objectives and principles of security audits, including their scope, methodology, and reporting. You can also discuss the importance of security audits in maintaining the security of an organization’s assets.
9. **Risk Identification, Assessment and Mitigation**: This topic can cover the process of identifying, assessing, and mitigating risks in an organization, including the various techniques and tools that are commonly used. You can also discuss the importance of risk management in security testing and the challenges associated with it.
10. **People, Process and Technology**: This topic can cover the three key components of security testing, including the people, processes, and technology involved. You can also discuss the importance of each component and the challenges associated with managing them effectively.