**Information Assurance & Cybersecurity Basics**

* **Computer Security (NIST Definition):** Measures ensuring **Confidentiality, Integrity, and Availability (CIA Triad)**.
  + **Confidentiality:** Restricts access to sensitive information.
  + **Integrity:** Ensures data accuracy and prevents unauthorized modifications.
  + **Availability:** Ensures system accessibility and uptime.
* **System Resources:** Assets requiring protection.
  + **Data, Hardware, Software, Networks**
* **Vulnerability:** A weakness in a system that can be exploited.
* **Threat:** Potential danger exploiting vulnerabilities.
* **Attack:** A malicious action exploiting vulnerabilities.
* **Risk:** Likelihood and impact of threats exploiting vulnerabilities.
  + **Risk Score = Likelihood x Impact**

**Risk Management & Assessment**

* **Types of Risk:**
  + **Operational:** System failures, human errors.
  + **Strategic:** Poor cybersecurity investment.
  + **Technical:** Software vulnerabilities, outdated hardware.
  + **Compliance:** Failure to follow regulations (GDPR, HIPAA).
  + **Human:** Phishing, insider threats.
  + **Environmental:** Natural disasters, power outages.
* **Risk Assessment Process:**
  1. Identify Assets
  2. Identify Threats
  3. Identify Vulnerabilities
  4. Assess Risks (Likelihood & Impact)
  5. Prioritize Risks
  6. Implement Controls
  7. Monitor and Review
* **Risk Treatment Strategies:**
  + **Avoidance:** Eliminate risky activities.
  + **Mitigation:** Reduce risk impact or likelihood.
  + **Transfer:** Shift risk responsibility (e.g., insurance).
  + **Acceptance:** Accept risks if manageable.
* **Risk Monitoring & Contingency Planning:** Continuous review to adapt to emerging threats.
* **Inherent vs. Residual Risk:**
  + **Inherent:** Risk before controls are applied.
  + **Residual:** Remaining risk after mitigation measures.

**Identity & Access Management (IAM)**

* **IAM:** Policies & technologies managing digital identities & access rights.
* **Authentication Methods:**
  + **Knowledge-based:** Passwords.
  + **Possession-based:** Smart cards.
  + **Biometric:** Fingerprints, facial recognition.
* **Password Security:**
  + **Hashing & Salting:** Prevents rainbow table attacks.
  + **Multi-Factor Authentication (MFA):** Combines multiple authentication factors.
* **Access Control Models:**
  + **Discretionary Access Control (DAC):** Owner controls permissions.
  + **Mandatory Access Control (MAC):** Central authority assigns access.
  + **Role-Based Access Control (RBAC):** Access based on job roles.
  + **Attribute-Based Access Control (ABAC):** Dynamic, rule-based access.

**Security Policies & Countermeasures**

* **Security Policy:** Rules for securing information systems.
  + **Examples:** Access control policies, network security policies, incident response policies.
* **Countermeasures:** Techniques to mitigate threats.
  + **Firewalls:** Regulate network traffic.
  + **Intrusion Detection Systems (IDS):** Detect malicious activities.
  + **Antivirus Software:** Identifies and removes malware.
  + **Encryption:** Secures data.
  + **Security Awareness Training:** Educates users on best practices.

**Access Control & Threat Protection**

* **Single Sign-On (SSO):** Access multiple services with one login.
* **Denial-of-Service (DoS) Protection:** MFA, CAPTCHA prevent authentication abuse.
* **Replay Attack Prevention:** Time-stamps & challenge-response mechanisms.
* **Biometric Authentication:** Uses unique human characteristics.

**Risk Assessment Frameworks**

* **NIST Risk Management Framework (RMF):**
  1. Categorize Information Systems
  2. Select Security Controls (NIST SP 800-53)
  3. Implement Controls
  4. Assess Controls
  5. Authorize Systems
  6. Monitor Security Continuously
* **Other Frameworks:**
  1. **OCTAVE:** Risk assessment method focusing on assets & threats.
  2. **FAIR:** Risk quantification model.

**Compliance & Security Auditing**

1. **Compliance**
   * Adhering to security rules, regulations, and standards.
   * Protects sensitive data, ensures legal adherence, and maintains trust.
   * Compliance is demonstrated through audits, assessments, and documentation.
2. **Common Compliance Frameworks**
   * **ISO/IEC 27001**: Information security management system standard.
   * **PCI DSS**: Payment security standards for handling credit card data.
   * **HIPAA**: Protects health information in the U.S.
   * **GDPR**: EU regulation for data protection and privacy.
   * **SOX**: Ensures financial reporting integrity in the U.S.
3. **Security Auditing**
   * Systematic review of security policies, processes, and controls.
   * Evaluates compliance, identifies vulnerabilities, and mitigates risks.
4. **Key Performance Indicators (KPIs)**
   * **Incident Response Time** (MTTD, MTTR)
   * **Vulnerability Management** (# of unresolved vulnerabilities)
   * **Patch Management** (Patch compliance rate)
   * **Phishing Resilience** (Click-through rate on phishing tests)
   * **Access Control** (Access review completion rate)
   * **Encryption Effectiveness** (% of encrypted data)
   * **Security Incident Trends** (# of incidents over time)

**Identity & Access Management (IAM)**

1. **Definition**
   * Ensures the right people have the right access at the right time.
   * Manages user identities, roles, and permissions.
2. **Authentication Methods**
   * **Knowledge-based** (Passwords)
   * **Possession-based** (Smart Cards)
   * **Biometric** (Fingerprint, Iris scan)
   * **Multi-Factor Authentication (MFA)** (Combining two or more factors)
3. **Password Security**
   * Hashing passwords prevents easy retrieval.
   * **Salting**: Adds unique values to hashed passwords to prevent rainbow table attacks.
   * **Brute force protection**: Using CAPTCHA, account lockout policies.
4. **One-Time Password (OTP)**
   * Single-use passwords for enhanced security.
   * Delivered via SMS, email, or authentication apps.
5. **Access Control Models**
   * **Discretionary Access Control (DAC)**: Owner determines access.
   * **Mandatory Access Control (MAC)**: Central authority enforces access based on security labels.
   * **Role-Based Access Control (RBAC)**: Access is assigned based on roles within an organization.
   * **Attribute-Based Access Control (ABAC)**: Access is determined dynamically using attributes.
6. **Single Sign-On (SSO)**
   * Allows access to multiple services with a single login.
   * Improves user experience but poses security risks if compromised.
7. **Denial of Service (DoS) in Authentication**
   * Overloading authentication systems with repeated requests.
   * Prevented using MFA and lockout mechanisms.
8. **Level of Assurance (LOA)**
   * **LOA1**: Basic username/password authentication.
   * **LOA2**: Password + OTP authentication.
   * **LOA3**: Password + OTP + biometric authentication.

**CIA Triad**

* **Confidentiality**: Restricts access to sensitive data.
* **Integrity**: Prevents unauthorized data modification.
* **Availability**: Ensures system uptime.

**Risk Management**

* **Risk = Likelihood x Impact**
* **Types**: Operational, Strategic, Technical, Compliance, Human, Environmental.
* **Risk Treatment**: Avoid, Mitigate, Transfer, Accept.

**Identity & Access Management (IAM)**

* **Authentication Methods**:
  + Knowledge-based (Password)
  + Possession-based (Smart Card)
  + Biometric (Fingerprint, Facial Recognition)
  + **Multi-Factor Authentication (MFA)**: Combines multiple factors.
* **Access Control Models**:
  + **DAC**: Owner controls access.
  + **MAC**: Central authority assigns access.
  + **RBAC**: Role-based access.
  + **ABAC**: Attribute-based, dynamic.
* **SSO (Single Sign-On)**: One login for multiple services (security risk if compromised).

**Password Security**

* **Hashing & Salting**: Prevents password attacks.
* **Brute Force Protection**: CAPTCHA, Account Lockouts.
* **One-Time Password (OTP)**: Single-use authentication code.

**Security Auditing & Compliance**

* **Frameworks**: ISO 27001, PCI DSS, HIPAA, GDPR, SOX.
* **Auditing**: Evaluates compliance, identifies vulnerabilities.
* **KPIs**:
  + Incident Response (MTTD, MTTR)
  + Vulnerability Management
  + Patch Compliance Rate
  + Phishing Click-through Rate
  + Access Review Completion Rate
  + Encryption Effectiveness

**Threat Protection & Countermeasures**

* **Firewalls**: Regulate network traffic.
* **IDS/IPS**: Detect and prevent intrusions.
* **Antivirus & Encryption**: Protect data integrity.
* **Security Awareness Training**: Reduces human risks.
* **DoS Attack Protection**: MFA, CAPTCHA, Lockouts.
* **Replay Attack Prevention**: Timestamps, Challenge-Response.

**Risk Assessment Frameworks**

* **NIST RMF**:
  1. Categorize Systems
  2. Select Security Controls
  3. Implement & Assess Controls
  4. Authorize & Monitor Systems
* **OCTAVE & FAIR**: Alternative risk assessment methods.

**Level of Assurance (LOA)**

* **LOA1**: Username + Password.
* **LOA2**: Password + OTP.
* **LOA3**: Password + OTP + Biometric.