**Information Assurance & Cybersecurity Basics**

* **CIA Triad:**
  + **Confidentiality:** Restricts access to sensitive data.
  + **Integrity:** Ensures data accuracy and reliability.
  + **Availability:** Guarantees system uptime and access.
* **System Resources:** Data, Hardware, Software, Networks.
* **Risk Equation:** Risk = Likelihood × Impact.
* **Types of Risks:**
  + **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  + **Technical:** Software vulnerabilities, outdated hardware.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 Treatment:** Avoidance, Mitigation, Transfer, Acceptance.
* **Security Policies:** Access Control, Network Security, Incident Response.

**Identity & Access Management (IAM)**

* **Authentication Methods:**
  + Knowledge-based (Passwords), Possession-based (Smart-cards), Biometric (Fingerprint, Iris scan).
* **Password Security:**
  + **Hashing & Salting:** Prevents rainbow table attacks.
  + **Multi-Factor Authentication (MFA):** Enhances security.
  + **One-Time Passwords (OTP):** Valid for single-use.
* **Access Control Models:**
  + **DAC (Owner-controlled), MAC (Central authority), RBAC (Role-based), ABAC (Attribute-based).**
* **Single Sign-On (SSO):** One login for multiple systems.
* **Denial of Service (DoS) Protection:** MFA, CAPTCHA

**Risk Assessment & Compliance**

* **Risk Assessment Process:**
  + Identify assets → Identify threats → Identify vulnerabilities → Assess risks → Prioritize → Implement controls → Monitor.
* **Compliance Frameworks:**
  + **ISO 27001:** Information security management.
  + **PCI DSS:** Payment security.
  + **HIPAA:** Healthcare data protection.
  + **GDPR:** EU personal data protection.
  + **SOX:** Financial reporting security.

**Security Auditing & Key Performance Indicators (KPIs)**

* **Security Auditing:** Examines security policies, network configurations, and access controls.
* **Key KPIs:**
  + **Incident Response:** Mean Time to Detect (MTTD), Mean Time to Respond (MTTR).
  + **Patch Compliance Rate:** Percentage of updated systems.
  + **Phishing Click-through Rate:** Employee resilience to phishing.
  + **Endpoint Security Effectiveness:** Malware detection success.
  + **Regulatory Compliance Status:** Adherence to security regulations.

**Countermeasures & Security Practices**

* **Firewalls:** Filter incoming/outgoing traffic.
* **Intrusion Detection Systems (IDS):** Detect threats.
* **Antivirus Software:** Identifies & removes malware.
* **Encryption:** Secures sensitive data.
* **Security Awareness Training:** Educates employees.
* **Incident Response Plan:** Outlines actions for security breaches.

**Risk Management Frameworks**

* **NIST Risk Management Framework (RMF):**
  1. Categorize Systems
  2. Select Controls
  3. Implement Controls
  4. Assess Controls
  5. Authorize Systems
  6. Monitor Security Continuously