**Module Wise Importance**

**Honor’s -Cybersecurity (Security Information Management)**

**Module no 1:**

1. What is Information Security & Why do you need it?
2. Explain IT ACT 2000 and its IT ACT 2008.

**Module no 2:**

1. Explain Cloud computing issues and benefits related to information Security
2. Explain various standards of INFOSEC?
3. Write in details about ISO 27001 standard?

**Module no 3:**

1. Explain Threat Modelling?
2. Explain Risk Assessment and Analysis Framework in details?
3. Write a short -notes on: ISO 31010
4. Write a short -notes on: NIST-SP-800-30

**Module no 4:**

1. Explain Access Control Models?
2. Write a brief about Access control Techniques?
3. Explain difference types of Access Control Methods?
4. Explain Intrusion Detection System (IDS) and Intrusion Prevention system (IPS) in detail.
5. What is the significance of accountability in cybersecurity, and how does it relate to event monitoring and log reviews?

**Module no 5:**

1. Explain Business Continuity plan.
2. Explain the phases of Incident Response and Incident Management in detail.
3. Explain the phase of Disaster Recovery and its types?
4. What is the role of security policies and procedures in maintaining operational security?

**Module no 6:**

1. What are the key components and security measures used for conducting a server security audit in a Windows environment?
2. How can organizations ensure the integrity and security of Group Policy settings during audits?
3. What are the security implications of email communication in a Windows environment, and why are email audits important?
4. What are the signs and indicators that auditors typically look for when assessing malware infections and incidents?
5. What are some common compliance standards that organizations must adhere to when it comes to server security, Active Directory, antivirus, email, and malware protection?
6. What is endpoint protection, and why is it crucial in modern cybersecurity?
7. How do shadow password systems enhance password security compared to traditional password storage methods?
8. How can organizations effectively manage and audit SUDO users to enhance security and access control?
9. How can organizations implement a robust password management policy to enhance security, including the use of shadow passwords?

**Web Application security:**

1. What is cross-site request forgery (CSRF), and how can it be prevented in web applications?
2. What are the common security threats that web applications face, and how can they be mitigated?
3. How do SQL injection attacks work, and what measures can be taken to prevent them in web applications?
4. What is cross-site scripting (XSS), and how to protect against XSS attacks?
5. What role does access control play in web application security, and how can it be enforced effectively?
6. How do compliance standards like GDPR and HIPAA impact web application security, and what are the implications for data protection?