Name: M. Taimoor

Registration No: FA22-BSE-072

Course: CSC232 Information Security

Instructor: Ma'am Shumaila

Instructor: _____

Date: 3 June 2025

1. Certification & Accreditation Analysis

a. Technical Distinction between Certification and Accreditation:

Certification is the comprehensive evaluation of a system's technical and non-technical security controls to determine their effectiveness. It verifies that the system meets specified security requirements. Accreditation, on the other hand, is the formal declaration by a Designated Approving Authority (DAA) that a system is approved to operate with a defined level of risk. It is a risk management decision based on the certification results.

b. Application of NIST RMF (SP 800-37 Rev. 1):

NCIA followed the NIST Risk Management Framework in certifying the HSOP platform. The steps included:

1. Categorizing HSOP based on impact levels.

2. Selecting security controls aligned with FIPS 200 and NIST SP 800-53.

3. Implementing selected controls on HSOP.

4. Assessing the controls to determine effectiveness.

5. Authorizing the system for operation by the DAA.

6. Continuous monitoring post-deployment to track changes and emerging threats.

c. NIACAP Phases Ensuring HSOP Security:

NIACAP consists of four key phases:

1. Definition: Established mission needs, security requirements, and DAA roles.

2. Verification: Evaluated system architecture and performed initial risk assessment.

3. Validation: Conducted system testing and reviewed security documentation.

4. Post Accreditation: Ensured continuous monitoring and compliance through scheduled reviews and incident handling.

These phases ensured a robust security posture and operational readiness for HSOP.

d. Role of ISO 27001/27002 Standards:

ISO 27001 provided the framework for establishing an Information Security Management System (ISMS), and ISO 27002 offered detailed control objectives. NCIA used these standards to implement structured policies, conduct risk assessments, and enforce access controls, helping align HSOP with international best practices and facilitating systematic certification.

2. Security Maintenance Lifecycle Execution

a. Role of NIST SP 800-100:

NIST SP 800-100 supports ongoing operational security through guidelines on governance, policy development, awareness, and security performance. It ensures that NCIA maintains and improves security practices post-certification, focusing on strategic planning and integration with business goals.

b. Step-by-step Compliance Maintenance:

1. Continuous Monitoring:

- Internal: Log reviews, anomaly detection systems, and staff activity audits.
- External: Third-party vulnerability scans and penetration testing.

2. Scheduled Risk Assessments:

- Quarterly assessments with documentation and risk mitigation planning.

3. Vulnerability Detection and Patching:

- Weekly scans, automated patch deployment, pre-deployment testing, and rollback strategies to minimize disruption.

3. Digital Forensics Methodology Application

a. Roles and Responsibilities:

The digital forensics team at NCIA includes forensic analysts, legal advisors, and incident responders. Their responsibilities include identifying breaches, preserving digital evidence, conducting analysis, and supporting legal processes.

b. Legal and Procedural Considerations:

- Affidavits and Search Warrants: Legal advisors draft affidavits to obtain search warrants for digital evidence.

- Evidence Collection and Chain of Custody: Forensic analysts use write-blockers and imaging tools, documenting all handling steps.

- Documentation and Presentation: Analysts compile reports, timelines, and visual evidence, presenting findings in court or audit environments with expert testimony.