Information Assurance Program Design (NIST-Aligned)

Overview

This project presents a comprehensive Information Assurance Plan designed to protect organizational information assets against modern cyber threats. The plan applies industry-recognized frameworks to assess risk, define security responsibilities, and establish enforceable policies that support confidentiality, integrity, and availability (CIA).

The objective was to move beyond checklist compliance and design a practical, sustainable security program aligned with real-world enterprise environments.

Problem Statement

Organizations face increasing exposure to ransomware, credential compromise, and exploitation of unpatched systems. Inconsistent enforcement of security controls, limited centralized monitoring, and infrequent testing of incident and disaster recovery plans significantly increase organizational risk.

- Identify and prioritize security risks
- Align controls with recognized standards
- Define clear roles and accountability
- Improve incident preparedness and resilience

My Approach

1. Information Assurance Assessment

- Confidentiality: Role-based access controls and limited MFA, but inconsistent enforcement
- Integrity: Patch management and monitoring existed but were applied unevenly
- Availability: Basic backups were present, but disaster recovery testing was limited

2. Risk Assessment (NIST SP 800-30)

- Threat likelihood evaluation
- Business impact analysis

- Identification of existing control gaps
- High-risk threats: unpatched vulnerabilities, ransomware, credential compromise via phishing

3. Policy & Control Design

- Incident response
- Disaster recovery and business continuity
- Access control and MFA enforcement
- Logging, monitoring, and continuous improvement

Key Deliverables

- Information Assurance Plan
- Risk matrix with likelihood and impact ratings
- Defined security roles and responsibilities
- Incident response and disaster recovery policies
- Access control standards aligned with least privilege
- Continuous review and maintenance strategy

Frameworks & Standards Used

- NIST SP 800-30 – Risk Assessment
- NIST SP 800-53 – Security & Privacy Controls
- NIST SP 800-61 – Incident Response
- NIST SP 800-34 – Contingency & Disaster Recovery
- CIA Triad (Confidentiality, Integrity, Availability)

Skills Demonstrated

- Information assurance program design
- Risk assessment and prioritization
- Incident and disaster response planning
- Security policy development
- Governance and accountability modeling
- Translating technical risk into business impact

Outcome & Impact

This plan establishes a repeatable, defensible security posture that reduces dwell time through improved detection and response, strengthens accountability through defined roles, improves resilience against ransomware and system outages, and aligns organizational security with industry best practices.

What I Would Improve Next

- Integrate centralized SIEM tooling for real-time monitoring
- Automate patch management and configuration baselines
- Conduct tabletop and live incident response exercises
- Expand security awareness training with phishing simulations