INFO 7374 - Cybersecurity Audit and Compliance
Week 6 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Question 1: Control Implementation

1. Three NIST 800-53 Controls to Prioritize

INFO-7374 Solutions should prioritize the following controls to address ransomware attacks and data loss:

1) SI-3: Malicious Code Protection
- Deployment of anti-malware tools and endpoint protection software.
- Regular updates of virus definitions; regular notification of system scans.

2) CP-9: System Backup
- Perform the backup of data in an automated, encrypted, and outsourced manner.
- Regular testing of data restoration for sure reliability.

3) IR-4: Incident Handling
- Prepare a written plan for incident response.
- Train employees to recognize different types of security incidents and respond to them accordingly.

2. Ensuring Cost-Effectiveness

To align with limited resources:

- **Risk-Based Prioritization**: Focus on high-impact threats like ransomware.
- **Open-Source & Cloud Solutions**: Use cost-effective security tools like Microsoft Defender, AWS Backup, or open-source IDS/IPS.
- **Outsourcing & MSSPs**: Engage a Managed Security Service Provider (MSSP) for 24/7 monitoring at a lower cost.

INFO 7374 - Cybersecurity Audit and Compliance
Week 6 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Question 2: NIST CSF 2.0 Implementation

1. Framework Alignment

INFO-7374 Solutions can use NIST CSF 2.0 to align cybersecurity efforts with business objectives by:

- Mapping security initiatives against the requirements of business risks and compliance;
- Using a risk-based approach to balance security investments.

High-Level Plan to Implement NIST CSF 2.0 Core Functions

1) Govern:
- Create cybersecurity policies aligned with business goals.
- Assign roles and responsibilities to manage security.

2) Identify:
- Conduct a risk assessment for identification of vulnerabilities and critical assets.
- Compile and maintain an inventory of IT assets and sensitive data.

3) Protect:
- Implement Multi-Factor Authentication (MFA) and access controls.
- Training employees in cybersecurity awareness.

4) Detect:
- Deploy Intrusion Detection System (IDS) and log monitoring.
- Enable real-time alert and anomaly detection.

5) Respond:
- Form incident response teams.
- Prepare a ransomware response playbook.

6) Recover:
- Implement disaster recovery (DR) plans.
- Frequent testing of backup recovery and business continuity plans.

INFO 7374 - Cybersecurity Audit and Compliance
Week 6 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

2. Cybersecurity Maturity

1) Recommended Tier: Risk-Informed (Tier 2)

- Information-7374, with their limited resources, should be able to achieve Tier 2 (Risk-Informed) with documented security policies that are not yet fully optimized.

2) Using NIST CSF Profile to

- Document the Current State: limited monitoring capabilities, basic security controls.
- Target State: proactive, automated monitoring.
- Lay down the roadmap to reduce the gap step by step.

Question 3: Integration of NIST 800-53 and NIST CSF 2.0

1. Synergy Between Frameworks

The INFO-7374 can integrate NIST 800-53 with NIST CSF 2.0 in the following ways:

- Map NIST 800-53 controls to CSF core functions to build a structured security approach.
- Example mappings:
  - Identify → RA-3 (Risk Assessment)
  - Protect → AC-2 (Access Control)
  - Detect → SI-4 (System Monitoring)
  - Respond → IR-4 (Incident Handling)
  - Recover → CP-10 (Recovery Procedures)
  - Continuous Monitoring and Improvement

2. Continuous Monitoring and Improvement

- Security Information and Event Management (SIEM) that automates analysis of logs.
- Regular penetration testing: to seek out vulnerabilities before they are exploited.
- Security metrics and KPIs:
  - Incident response time
  - Successful attempts blocking for ransomware attacks
  - Rate of recovery from backups

With these actions, INFO-7374 may prepare an NIST 800-53 and CSF 2.0-based cost-effective and scalable cybersecurity program.