**Week 2: Governance Framework Design**

**Target Environment:** Nigerian Government Healthcare Agency (Simulated via Metasploitable 2)

**1. Risk Management Policy**

**Policy Title**  
Risk Management Policy – To establish a structured approach to identifying, assessing, and mitigating cybersecurity risks across the healthcare agency.

**Scope**  
Applies to all IT systems, servers, applications, medical databases, and supporting infrastructure within the healthcare agency. Includes critical services discovered (FTP, SMB, MySQL, Apache, Tomcat, Telnet).

**Roles & Responsibilities**

* **Risk Manager** – Maintains enterprise risk register.
* **System Owners** – Ensure patching and remediation of vulnerabilities (e.g., CVE-2011-2523 vsFTPd backdoor, Samba RCE).
* **Chief Information Security Officer(CISO)** – Oversees cyber risk program and reports to governance board.
* **IT Security Team** – Conducts vulnerability scans and implements controls.

**Policy Statement**

* Cyber risks will be identified, assessed using CVSS and likelihood-impact scoring, and documented in the risk register.
* High/critical vulnerabilities must be remediated within defined timelines (Critical: 1 week, High: 2 weeks).
* Risk treatment strategies will be applied in the following ways:
* **Mitigation**: Implement security controls to reduce the likelihood or impact of a risk (role-based access control (RBAC), regular patch management).  
  Apply security patches to the hospital’s patient records system (Electronic Health Record) to prevent exploitation of a known SQL injection vulnerability.
* **Acceptance**: Formally acknowledge the risk and accept it without additional action, usually when the cost of mitigation outweighs the potential damage.  
  A legacy medical device connected to the network has a minor vulnerability, but fixing it requires replacing equipment worth millions. The organization accepts the risk while keeping it on the risk register.
* **Avoidance**: Eliminate the activity or process that introduces the risk.  
  Disable outdated file-sharing protocols (e.g SMB) on hospital servers to remove the risk of WannaCry-style ransomware attacks.
* **Transfer**: Shift the risk to a third party.  
  Purchase cyber liability insurance to cover potential fines for data breaches under GDPR, or outsource 24/7 threat monitoring to a managed security service provider.
* **Checklist Mapping:**
  + Personnel Security (Q5–Q6) → Mandatory background checks and offboarding controls eg account deactivation.
  + Physical Security (Q12, Q18–Q20) → Secure computing areas, annual emergency plan review eg test drills on fire, flood etc, and sealing procedures(server racks, doors).
  + Disaster Recovery (Q38–Q47) → Annual Business Continuity Plan/Disaster Recovery Plan(BCP/DRP) review and testing.

**Compliance Requirements**

* **NIST CSF:** ID.RA-1, PR.AC-1
* **ISO 27001:** A.8.8 (Management of Technical Vulnerabilities), A.8.20 (Network Security Controls)
* **GDPR:** Art. 32 (Security of Processing)
* **NDPR 2019:** Sec. 2.6 (Data Security & Patch Management)

**Enforcement & Review**

* Non-compliance reported to the Oversight Committee (Senior management, legal advisors, compliance officers, IT/security representatives) and escalated to executive leadership (CEO).
* Policy reviewed annually and after significant incidents.

**2. Auditing & Compliance Policy**

**Policy Title**  
Auditing & Compliance Policy – To ensure accountability and continuous regulatory compliance with Nigerian and international data protection frameworks.

**Scope**  
Covers all healthcare systems handling patient data, financial data, and medical record management platforms. Includes infrastructure supporting Metasploitable 2 simulated services.

**Roles & Responsibilities**

* **Internal Auditor** – Conducts quarterly compliance checks.
* **Data Protection Officer(DPO)** – Ensures GDPR/NDPR compliance audits.
* **Chief Information Security Officer(CISO)** – Oversees external certification audits (ISO 27001).

**Policy Statement**

* Internal audits shall be conducted quarterly to assess compliance with access control, encryption, and patching.
* External audits (ISO 27001 certification, GDPR readiness) shall be conducted annually.
* Non-compliance findings must be documented and corrective action plans implemented.
* **Checklist Mapping:**
  + Compliance & Audit (Q54–Q55) → Quarterly compliance audits.
  + Compliance & Audit (Q56–Q57) → Annual DRP testing and management review of access lists.
  + Compliance & Audit (Checklist items 54–57) → Document Non-compliance findings and corrective actions should be implemented.

**Compliance Requirements**

* **NIST CSF:** RC.IM-1, PR.AA-1
* **ISO 27001:** A.18.2.3 (Technical Compliance Review), A.18.1.1 (Legal & Regulatory Compliance)
* **GDPR:** Art. 5(2) (Accountability), Art. 30 (Records of Processing)
* **NDPR 2019:** Sec. 2.6 (Data Security Compliance)

**Enforcement & Review**

* Non-compliance may result in disciplinary measures and escalation to regulators.
* Policy reviewed every 12 months or following audit findings.

**3. Data Security Policy**

**Policy Title**  
Data Security Policy – To safeguard the confidentiality, integrity, and availability of patient health data and agency information assets.

**Scope**  
Applies to all electronic health records (EHR), databases (MySQL, PostgreSQL), web applications, backup systems, and communication channels.

**Roles & Responsibilities**

* **DPO** – Ensures patient data handling aligns with GDPR/NDPR.(Art 4(15), Art 9(1) Art 9(2) )
* **IT Administrators** – Implement encryption, access controls, and secure disposal methods. GDPR (Art. 32(1))
* **All Staff** – Responsible for protecting patient data and following secure usage guidelines. Art 5(1)

**Policy Statement**

* Patient health data shall be classified as Restricted and encrypted at rest (AES-256) and in transit (TLS 1.3).
* Role-based access control (RBAC) must be enforced, and least privilege applied.
* Data retention shall follow healthcare regulations, with secure disposal of outdated records.
* Breach notifications must be reported within 72 hours of detection.
* **Checklist Mapping:**
  + Account & Password Mgmt (Q23–Q24) → Enforced password policy (complexity, rotation).
  + Confidentiality of Sensitive Data (Q28–Q29, Q36–Q37) → Encryption, retention, and secure disposal procedures.
  + Security Awareness (Q48–Q53) → Mandatory staff training on sensitive data handling, PCI, and NDPR compliance.

**Compliance Requirements**

* **NIST CSF:** PR.AA-3, PR.SV-1
* **ISO 27001:** A.8.2 (Data Classification), A.5.17 (Authentication Information)
* **GDPR:** Art. 25 (Data Protection by Design), Art. 32 (Security of Processing)
* **NDPR 2019:** Sec. 2.1 (Lawful Processing), Sec. 4.2 (Breach Notification)

**Enforcement & Review**

* Violations may result in disciplinary actions and breach reporting to NDPC/GDPR authorities. (Art 33&34)
* Policy reviewed annually or when new data handling regulations emerge(GDPR, ISO27001:2022,HIPPA).

| **Checklist Area** | **Example Checklist Control** | **Governance Policy Alignment** |
| --- | --- | --- |
| **Personnel Security** | Background checks for employees/contractors | Risk Management Policy |
|  | Termination access removal process | Risk Management Policy |
| **Physical Security** | Secure computing areas (locks, badges, logs) | Data Security & Privacy Policy |
|  | Escorting visitors into restricted areas | Data Security & Privacy Policy |
| **Account & Password Mgmt** | Enforce strong password policies | Data Security & Privacy Policy |
|  | Limit access to authorized users only | Risk Management Policy |
| **Confidentiality of Sensitive Data** | Data classification (sensitive vs non-sensitive) | Data Security & Privacy Policy |
|  | Encrypting sensitive data | Data Security & Privacy Policy |
|  | Secure disposal of old equipment/media | Data Security & Privacy Policy |
| **Disaster Recovery** | Maintain business continuity plan | Risk Management Policy |
|  | Backup and archival of critical data | Auditing & Monitoring Policy |
| **Security Awareness & Training** | Provide recurring security training | Auditing & Monitoring Policy |
|  | Teach password hygiene & phishing prevention | Risk Management Policy |
| **Compliance & Audit** | Review and update security policies | Auditing & Monitoring Policy |
|  | Test disaster recovery plans | Risk Management Policy |
|  | Management reviews access rights | Auditing & Monitoring Policy |