**Week 3: Implementation & Auditing Plan**

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

**1. Overview**

The primary compliance goal is to strengthen the cybersecurity posture of the government health agency by aligning its systems with **GDPR , NIST CSF, ISO 27001:2022, and NDPR (2019)** standards.  
This implementation ensures:

* Protection of sensitive health data (patient records, medical files).
* Identification and remediation of vulnerabilities demonstrated on Metasploitable 2.
* Establishment of a governance framework for monitoring, auditing, and continuous improvement.

**2. Key Milestones**

**Phase 1 – Preparation:**

* Identify critical assets (databases, patient records, network devices).
* Map vulnerabilities on Metasploitable 2 against compliance requirements.

**Phase 2 – Implementation:**

* Apply remediation strategies (patch management, access controls, secure communication).

(ISO27001:2022 Annex A.8.8, Annex A.5.15, Annex A.8.21), (GDPR Art.32) (NIST ID.RA-8)

* Deploy security controls aligned with NDPR & GDPR Art. 32.

**Phase 3 – Auditing & Monitoring Setup:**

* Establish auditing protocols (set up system logs from servers, database& others, implement intrusion detection systems, schedule vulnerability scans) (DE.CM-01, ID.RA-01).
* Define compliance KPIs for measuring effectiveness eg % of critical vulnerabilities patched within SLA (e.g. 14 days) (GV.OV-03).

**Phase 4 – Review & Reporting:**

* Document audit results.

Create structured reports (monthly/quarterly) showing:

* Findings from vulnerability scans.
* Anomalies detected in logs or IDS.
* Compliance status against frameworks (ISO 27001, GDPR, NDPR, NIST CSF).

Reports should highlight **gaps, risks, and trends**.

* Provide feedback loop for continuous improvement.
* Use audit results to adjust policies, update security controls, or retrain staff.
* Feed lessons learned into **future security strategy** eg If repeated failed login attempts are noticed, enforce stricter password policy or MFA.
* This aligns with the principle of **continuous improvement** in both ISO 27001:2022 A.10.2 and NIST CSF GV.RR-01.

| **Vulnerability (Metasploitable 2)** | **Compliance Requirement** | **Mapping Justification** |
| --- | --- | --- |
| **Anonymous FTP access** | GDPR Art. 32 (Security of Processing), NDPR Data Security Principles | Lack of access control violates the requirement for confidentiality & integrity of personal data. |
| **Outdated Apache server (with known exploits)** | ISO 27001 A.8.8 Technical Vulnerability Management | No patch management process in place. |
| **Weak MySQL root password** | NIST CSF PR.AA-1 (Identities & credentials managed), GDPR Art. 32 | Weak credentials expose EHR data to unauthorized access. |
| **No intrusion detection system (IDS)** | ISO 27001 A.8.16 (Logging and monitoring) | Failure to detect anomalies breaks compliance with monitoring requirements. |

**3. Action Plan**

**Tasks & Responsibilities:**

* **IT Security Team:** Conduct vulnerability scans on Metasploitable 2, apply patches to critical services (e.g., Apache, MySQL, OpenSSH, vsFTPd) and identify and configure all the misconfigurations in the system eg Disabling anonymous FTP access, Enforcing strong password policies, File permission changes etc.
* Deploy log monitoring using SIEM tools(Syslog/Splunk in lab environment) to enable detection of Failed/successful login attempts, Privilege escalation (e.g., sudo usage).
* **Compliance Officer:** Align remediation tasks with NDPR, GDPR, and ISO 27001 controls.
* **Oversight Committee:** Monitor adherence, review weekly reports, evaluate and approve proposed risk-related mitigation strategies.
* **System Admins:** Implement technical changes (encryption, authentication, patch deployment).
* Disable anonymous FTP and use Telnet services only for testing and validation (access control compliance). (ISO27001:2022 A.8.1), (NIST PR.DS-2)
* Patch outdated services (Apache, MySQL, OpenSSH) to meet ISO 27001 A.8.8 requirements.
* Implement data-in-transit protection (SSL/TLS enforcement).

**4. Risk Management**

**Potential Risks During Implementation:**

* Misconfiguration of patched services leading to downtime.
* Non-compliance due to incomplete patching.
* Insider threats from unauthorized system access.

**Mitigation Measures:**

* Before patch deployment, use rollback in case the system introduces system failure or unexpected incompatibility occurs and backup plans to ensure data and system states cannot be restored after roll back. (NIST 2.0 PR.IP-04, ISO27001:2022 Annex A 8.13, GDPR Art. 32(1))
* Conduct patch testing in lab before production. (NIST 2.0 GV.RM-05, ISO27001:2022 A.8.32, GDPR Art32(1))
* Implement least privilege access control. (ISO27001:2022 A.5.15, NIST 2.0 PR.AA-05, GDPR Art32(1))
* Train staff on compliance awareness. (NIST 2.0 PR.AT-01, ISO27001:2022 A.6.3, GDPR Art32(1))

**5. Monitoring & Auditing**

**Compliance Verification Activities:**

* Weekly vulnerability scans (Nmap, Nessus/OpenVAS).

This is essentially done to detect outdated software, open ports and misconfigurations. (ISO27001:2022 A.8.8, GDPR Art32(1))

* Monthly compliance audits mapped to NDPR, GDPR, ISO 27001 Annex A controls.

These are checks done to ensure that the organization is meeting regulatory and framework requirements (ISO27001:2022 A.5.36, GDPR Art 24)

* Log analysis for anomalies and unauthorized access attempts.

System logs, firewall logs, and application logs are reviewed to detect suspicious activity like unauthorized login attempts, this is usually done using SIEM tools like Splunk (ISO 27001:2022 A.8.15&16, NIST 2.0 DE.CM-1)

* Penetration testing simulations on Metasploitable 2 every quarter.

A practical security test is done where ethical hackers simulate real-world cyberattacks on the vulnerable test environment (Metasploitable 2). (ISO 27001:2022 A.8.29, ID.RA-05, GDPR Art32&33)

**Audit Review Frequency:**

* **Weekly:** Technical vulnerability scans, new vulnerabilities emerge daily so weekly scanning reduces the window of exposure.
* **Monthly:** Internal compliance audit.
* **Quarterly:** Oversight committee review & management report. Reviews are done quarterly to give opportunity for strategic visibility.

**6. Final Steps**

**Continuous Improvement Strategies:**

* Adopt a **continuous monitoring program** with automated alerts for vulnerabilities instead of waiting for monthly/quarterly scans. Tools like Splunk , OpenVAS can do this.
* Establish **compliance KPIs (Key Performance Indicators)**, including:
  + % of vulnerabilities patched within SLA eg if critical patches must be applied within 14days and only 50% is patched, then compliance is weak.
  + % of systems aligned with encryption and access control policies eg if 90% of systems use encryption but 10% still run unencrypted services, then that is a gap. Compliance should be 100%.
  + Number of non-compliance findings per audit cycle. If audits keep flagging the same issues, it shows lack of execution.

These KPIs help management to measure, report and improve security.

* Conduct **annual compliance training** for all staff handling health data.
* Staff are often the weakest target (phishing, mishandling personal data, weak passwords).
* Annual training ensures employees understand:
* GDPR obligations (handling health data properly).
* Security best practices (no sharing accounts, phishing awareness, reporting incidents).
* Local laws (NDPR for Nigeria, HIPAA if in US context).

This reduces insider risks and ensures legal compliance.

* Benchmark compliance posture against updated standards (GDPR, ISO).
* ISO 27001 standards and GDPR regulations are not static, they get updated. Benchmark is comparing your current security program with the latest versions to see if any gap exists. This ensures the organization is not “stuck in old compliance”.

| **Section** | **Details** | **Owner/Responsibility** | **Timeline** |
| --- | --- | --- | --- |
| **1. Overview** | Goal: Strengthen cybersecurity posture & protect patient health data. Align with NDPR, GDPR, ISO 27001:2022, NIST CSF. | Oversight Committee | Kickoff |
| **2. Key Milestones** |  |  |  |
| Phase 1 – Preparation | Identify critical assets (databases, patient records). Map vulnerabilities in Metasploitable 2. | IT Security Team | (Day 1–2) |
| Phase 2 – Implementation | Apply remediation: patch outdated services, disable anonymous FTP/Telnet, enforce encryption. | System Admins / Compliance Officer | (Day 3–5) |
| Phase 3 – Auditing Setup | Establish auditing protocols (system logs, scans, intrusion detection). Define KPIs. | Compliance Officer / Oversight Committee | (Day 6–7) |
| Phase 4 – Review & Report | Submit audit findings, update compliance status, recommend improvements. | Oversight Committee | End |
| **3. Action Plan** |  |  |  |
| Vulnerability Scan | Run Nmap/Nessus/OpenVAS scan on Metasploitable 2. | IT Security Team | Weekly |
| Patch Deployment | Fix Apache, MySQL, OpenSSH vulnerabilities. Test patches before rollout ie secondary validation for verification by another team, most likely the IT Security Team. | System Admins | Weekly |
| Access Control | Implement least privilege. Disable anonymous accounts. | IT Security Team | Ongoing |
| Encryption | Enforce SSL/TLS for data-in-transit protection. | System Admins | Weekly |
| Log Monitoring | Enable Syslog/Splunk in lab environment. | IT Security Team | Ongoing |
| **4. Risk Management** |  |  |  |
| Service Downtime | Patch testing in lab before rollout. Maintain rollback plan. | System Admins | Pre-deployment |
| Insider Threats | Enforce least privilege & multi-factor authentication. | Compliance Officer | Ongoing |
| Policy Gaps | Conduct weekly compliance review vs. NDPR & GDPR requirements. | Oversight Committee | Monthly |
| **5. Monitoring & Auditing** |  |  |  |
| Vulnerability Scans | Weekly scans with nmap,Nessus/OpenVAS. | IT Security Team | Weekly |
| Compliance Audits | Map results against GDPR (Art. 32), NDPR & ISO 27001 Annex A. | Compliance Officer | Monthly |
| Log Reviews | Detect anomalies in system logs. | Security Analysts | Weekly |
| Penetration Testing | Controlled tests on Metasploitable 2. | IT Security Team | Quarterly |
| **6. Final Steps** |  |  |  |
| KPIs Tracking | % vulnerabilities patched, % systems encrypted,number audit findings per cycle. | Compliance Officer | Monthly Report |
| Training | Annual compliance training for all staff handling patient health data. | HR & Compliance | Bi-Annual |
| Continuous Monitoring | Automated alerts for vulnerabilities & misconfigurations. | IT Security Team | Continuous |
| Benchmarking | Compare compliance posture with new NIST, GDPR & ISO 27001 updates. | Compliance Officer | Annual Review |