INFO7374
Cybersecurity Audit & Compliance

Project Report: Designing a Compliance Framework for a startup

GROUP 2 - MEMBERS	
NAME	**NU ID**
Krisha Lakhani	002334794
Nisarg Sheth	002308269
Siqi Yang	002772876
Emmanuel Frimpong	002062148

TABLE OF CONTENTS

MediCore AI Solutions

1. Executive Summary

A healthcare technology business called MediCore AI Solutions focuses on AI-powered diagnostics and small clinic patient record management. HIPAA, SOC 2, ISO 27001, and NIST CSF are just a few of the compliance requirements the organization must meet as a cloud-based service provider and handler of Protected Health Information (PHI).Additionally, as the company plans for potential growth into public markets, SOX compliance considerations have been incorporated into the framework design.

In order to simplify compliance efforts across many regulatory requirements, this study offers a thorough compliance framework created utilizing the Common Controls Framework (CCF) methodology. In order to accomplish compliance within a 12-month period, the framework identifies overlapping control objectives, evaluates important organizational risks, suggests customized controls to close identified gaps, and provides a systematic implementation plan.

MediCore AI Solutions will provide robust security procedures, guarantee regulatory compliance, foster customer trust, and lay the groundwork for future expansion by combining various compliance needs into a single framework.

2. Company Profile

2.1 Company Overview

Startup Name: MediCore AI Solutions
Industry: Healthcare Technology
Services: AI-powered diagnostics tools and cloud-based electronic health records (EHRs)
Target Market: Small to medium healthcare clinics
Company Size: 25 employees (5 executive team, 12 development staff, 8 operations/support)

2.2 Compliance Requirements:

- **HIPAA**: Required for handling Protected Health Information (PHI). *(U.S. Department of Health & Human Services [HHS], n.d.)*
- **SOC 2**: Needed for cloud-based service offerings and customer assurance. (American Institute of Certified Public Accountants [AICPA], 2017)
- **ISO 27001**: Adopted for global security best practices and international credibility. (International Organization for Standardization [ISO], 2013)
- **SOX**: Preparation for future financial reporting requirements as the company grows. *(U.S. Congress, 2002)*
- **NIST CSF**: Used as the foundational cybersecurity framework. (National Institute of Standards and Technology [NIST], 2018)

2.3 Approach: Implementation of a Common Controls Framework (CCF) to streamline overlapping requirements across multiple compliance frameworks.

3. Objective 1

3.1 Understanding Framework Overlap and CCF Benefits

These overlapping controls are addressed by major frameworks such as ISO 27001, SOC 2, HIPAA, SOX, and NIST CSF *(ISO, 2013; AICPA, 2017; HHS, n.d.; U.S. Congress, 2002; NIST, 2018)*.

By identifying overlapping requirements and putting in place unified controls, the Common Controls Framework (CCF) assists enterprises in maintaining compliance with various regulatory frameworks. This method creates uniform security procedures, drastically cuts down on redundancy, and lowers compliance expenses.
For MediCore AI Solutions, we identified several critical areas where requirements overlap across frameworks:

1. **Access Control**: According to the least privilege principle, all frameworks mandate limiting access to sensitive information and systems.
2. **Audit Logging and Monitoring**: uniform specifications for monitoring system events and identifying illegal activity.
3. **Risk Management**: standardized criteria for recognizing, assessing, and reducing security threats.
4. **Data Protection**: Complementing laws requiring the use of encryption and other security measures to safeguard private data.
5. **Incident Response**: Similar specifications apply to security incident detection, response, and recovery.

3.2 Comprehensive Compliance Mapping Table

The following table maps control objectives across different compliance frameworks using CCF categories: Control objectives were mapped based on authoritative frameworks *(ISO, 2013; AICPA, 2017; HHS, n.d.; U.S. Congress, 2002; NIST, 2018)*.

CCF Category	**Control Objective**	**ISO 27001**	**SOC 2**	**HIPAA**	**SOX**	**NIST CSF**
Access Control	Restrict access to data and systems by role, authentication, and need-to-know	A.9.1.1 -- A.9.4	CC6.1, CC6.2	§164.312(a)(1), §164.308(a)	Sec. 404	PR.AC-1 to PR.AC-6
Audit Logging & Monitoring	Audit and track system events for anomalies	A.12.4, A.15.2	CC7.2, CC7.3	§164.312(b), §164.308(a)(1)	Sec. 404	DE.CM-1 to DE.CM-8
Risk Management	Discover, evaluate, and respond to risk	A.6.1, A.18.2	CC3.3, CC4.1	§164.308(a)(1)(ii)(A)	Sec. 302	ID.RA-1 to ID.RA-6

CCF Category	**Control Objective**	**ISO 27001**	**SOC 2**	**HIPAA**	**SOX**	**NIST CSF**
Encryption & Data Protection	Protect sensitive data in transit and at rest	A.10.1, A.13.2	CC6.6, CC6.7	§164.312(a)(2)(iv), (e)(2)(ii)	N/A	PR.DS-1 to PR.DS-5
Incident Response	Detect, respond, and recover from an incident	A.16.1	CC7.4	§164.308(a)(6)	N/A	RS.RP-1 to RS.CO-5
Vendor Management	Confirm third-party service providers are secure and compliant	A.15.1.1 -- A.15.2	CC9.2	§164.308(b)(1)	Sec. 404	ID.SC-1 to ID.SC-5
Change Management	Approve, test, and monitor system changes	A.12.1.2	CC8.1	N/A	Sec. 404	PR.IP-3
Asset Management	Discover, categorize, and protect information assets	A.8.1 -- A.8.3	CC1.1	§164.310(d)(1)	N/A	ID.AM-1 to ID.AM-6
Business Continuity	Maintain availability and continuity during disruptions	A.17.1 -- A.17.2	CC9.1	§164.308(a)(7)	Sec. 404	PR.IP-9, RC.RP-1
Security Awareness & Training	Train workforce in information security best practices	A.7.2.2, A.18.1.3	CC1.2	§164.308(a)(5)	N/A	PR.AT-1 to PR.AT-5
Physical Security	Protect facilities and equipment	A.11.1 -- A.11.2	CC6.4, CC6.5	§164.310	N/A	PR.AC-2
Data Governance	Manage data throughout its lifecycle	A.8.2, A.18.1.3	CC6.3, CC6.7	§164.308(a)(4), §164.312(c)	Sec. 404	PR.DS-1, PR.DS-2

This mapping demonstrates how MediCore AI Solutions can efficiently address multiple compliance requirements through an integrated control approach. By implementing controls that satisfy multiple frameworks simultaneously, the company can minimize duplication of effort while maintaining comprehensive compliance coverage.

4. Objective 2

4.1 Key Risk Identification

The following 10 key risks were identified for MediCore AI Solutions:

1. Unauthorized access to PHI due to insufficient RBAC – could lead to data breaches, penalties, and patient harm.
2. Cloud misconfigurations exposing patient data – risks include breaches, compliance violations, and customer distrust.
3. Inadequate logging and monitoring – leads to delayed breach detection and weak forensic capabilities.
4. No incident response plan – results in poor breach handling and amplified damage.
5. Third-party vendors not assessed – creates supply chain vulnerabilities and potential breaches.
6. Lack of formal security training – increases risk of insider threats and social engineering.
7. No central risk register – limits visibility into emerging and cumulative risks.
8. No formal change management process – causes instability and introduces unvetted vulnerabilities.
9. Untested business continuity/disaster recovery plans – could lead to prolonged outages or data loss.
10. No encryption in transit – makes sensitive data interceptable, violating HIPAA.

4.2 Detailed Gap Analysis Based on Frameworks

The identified compliance gaps were benchmarked against ISO 27001, SOC 2, HIPAA, SOX, and NIST CSF *(ISO, 2013; AICPA, 2017; HHS, n.d.; U.S. Congress, 2002; NIST, 2018)*

Risk	**Affected Frameworks**	**Current Status**	**Gap Summary**	**Compliance Impact**
Access Control Weakness	ISO 27001, HIPAA, SOC 2, NIST	MFA implemented but no role-based controls	No RBAC, weak session management, no access reviews	Direct violation of HIPAA §164.312(a)(1) and SOC 2 CC6.1
Cloud Misconfigurations	NIST, SOC 2	Basic access setup only	No configuration audits, logging, or security hardening	Fails SOC 2 CC6.6 and NIST CSF PR.DS requirements
Audit Logging Gaps	ISO 27001, SOC 2, HIPAA, NIST	Application-level logs only	No central logging system, no real-time alerting, limited retention	Non-compliance with HIPAA §164.312(b) and ISO A.12.4

Risk	Affected Frameworks	Current Status	Gap Summary	Compliance Impact
No Incident Response Plan	ISO 27001, HIPAA, NIST	Verbal processes only, no documentation	No formal IR plan, no assigned roles, no testing procedures	Violates HIPAA §164.308(a)(6) and ISO A.16.1
Vendor Risk	HIPAA, SOC 2, ISO	Basic contracts signed	No vendor risk assessments, no ongoing monitoring, no SLA reviews	Fails HIPAA §164.308(b)(1) and SOC 2 CC9.2
Training Deficiency	ISO 27001, HIPAA, SOC 2	One-time onboarding only	No recurring training, no testing, no role-specific security education	Non-compliance with HIPAA §164.308(a)(5)
No Risk Register	ISO 27001, NIST	Not implemented	No systematic risk management, no periodic assessments	Violates ISO 27001 A.6.1 core requirements
Lack of Change Mgmt	ISO 27001, SOX	Informal email approvals only	No formalized change process, no testing requirements, no documentation	Fails SOC 2 CC8.1 and SOX Sec. 404 control requirements
No BCP/DRP	HIPAA, ISO, SOC 2	Basic backups only	No recovery time objectives, no testing, no documented procedures	Non-compliance with HIPAA §164.308(a)(7)
Inconsistent Encryption	HIPAA, ISO, NIST	AES encryption at rest only	No TLS enforcement, no key management, incomplete coverage	Violates HIPAA §164.312(e)(2)(ii) requirements

4.3 Risk Matrix (Likelihood × Impact)

Risk	Likelihood (L)	Impact (I)	Risk Score (L×I)	Existing Controls	Missing Controls	Priority
Unauthorized Access	High (3)	High (3)	9	MFA enabled	RBAC, access reviews, privileged access management	Critical
Cloud Misconfigurations	Medium (2)	High (3)	6	Basic permissions	Config audit, security hardening, automated scanning	High
Logging Deficiency	High (3)	Medium (2)	6	Basic logs present	SIEM solution, alerting system, log retention policy	High
Incident Response Gap	Medium (2)	High (3)	6	None	IR policy, team training, incident playbooks	High
Vendor Risk	Medium (2)	High (3)	6	BAAs signed	Vendor assessment process, ongoing monitoring, SLAs	High
No Security Training	Medium (2)	Medium (2)	4	Onboarding briefing	Recurring training program, phishing tests, role-specific education	Medium
No Risk Register	Medium (2)	High (3)	6	None	Risk management system, regular reviews, mitigation tracking	High
Change Mgmt Gaps	Medium (2)	High (3)	6	Email approvals	Change process, test procedures, approval workflows	High
No BCP/DRP	Low (1)	High (3)	3	Daily backups	Recovery test plans, documented procedures, assigned roles	Medium
Encryption Gaps	Medium (2)	High (3)	6	AES in storage	TLS enforcement, key management policy, comprehensive coverage	High

5. Objective 3

5.1 Developed Controls Addressing Identified Compliance Gaps

Based on the risk assessment, the following controls address MediCore AI Solutions' compliance gaps while aligning with HIPAA, ISO 27001, SOC 2, SOX, and NIST CSF.
All frameworks referenced align with standards outlined in their respective documents *(ISO, 2013; AICPA, 2017; HHS, n.d.; U.S. Congress, 2002; NIST, 2018)*.

1. Access Control System
Implement RBAC for PHI systems, with quarterly access reviews and PAM for admin accounts. Session timeouts enhance security.
Frameworks: ISO 27001 (A.9), HIPAA (§164.312(a)(1)), SOC 2 (CC6.1–6.2), NIST CSF (PR.AC)
Key Actions: Identity system integration, role matrix, approval workflow.

---

2. Encryption and Data Protection
Apply AES-256 encryption at rest and TLS 1.3 for data in transit. Establish data classification, key management, and DLP policies.
Frameworks: HIPAA (§164.312), ISO 27001 (A.10.1, A.13.2), NIST CSF (PR.DS)
Key Actions: Encryption rollout, cert management, data discovery.

---

3. Audit Logging & Monitoring
Deploy a centralized SIEM with real-time alerts, anomaly detection, and 6-year retention for HIPAA.
Frameworks: ISO 27001 (A.12.4), HIPAA (§164.312(b)), SOC 2 (CC7.2–7.3), NIST CSF (DE.CM)
Key Actions: Log integration, alerting, monitoring dashboard.

---

4. Incident Response Program
Develop a formal IR plan with defined roles, playbooks, and scenario-based training.
Frameworks: ISO 27001 (A.16.1), HIPAA (§164.308(a)(6)), NIST CSF (RS.RP, RS.CO)
Key Actions: Plan documentation, IR team setup, tabletop exercises.

---

5. Vendor Risk Management
Assess third-party vendors using tiered questionnaires. Include SLAs/BAAs and monitor compliance.
Frameworks: ISO 27001 (A.15), HIPAA (§164.308(b)(1)), SOC 2 (CC9.2), NIST CSF (ID.SC)
Key Actions: Vendor inventory, security clauses, reassessment.

---

6. Risk Management Program
Maintain a live risk register with scheduled reviews. Align assessments with change management.
Frameworks: ISO 27001 (A.6.1, A.8.2), SOC 2 (CC3.3, CC4.1), HIPAA (§164.308(a)(1)), NIST CSF (ID.RA)
Key Actions: Register tools, risk treatment planning, reporting.

---

7. Change Management System

Establish workflows with classification, testing, and CAB review for major changes.
Frameworks: ISO 27001 (A.12.1.2), SOC 2 (CC8.1), SOX (Sec. 404), NIST CSF (PR.IP-3)
Key Actions: Change system, testing protocols, approval matrix.

---

8. Security Awareness & Training
Deliver ongoing security training with phishing simulations and role-specific modules.
Frameworks: ISO 27001 (A.7.2.2), HIPAA (§164.308(a)(5)), SOC 2 (CC1.2), NIST CSF (PR.AT)
Key Actions: Curriculum rollout, LMS, tracking tests and updates.

---

9. Business Continuity & Disaster Recovery
Document BCP/DRP with defined RTOs/RPOs and perform regular recovery drills.
Frameworks: ISO 27001 (A.17), HIPAA (§164.308(a)(7)), SOC 2 (CC9.1), NIST CSF (PR.IP-9, RC.RP)
Key Actions: Backup infra, recovery playbooks, test schedules.

5.2 Mapping Controls to CCF Categories

The following table maps the proposed controls to CCF categories, demonstrating the integrated approach to compliance:

CCF Category	Control Implementation	Primary Compliance Frameworks	Business Benefit
Identity & Access Management	Role-based access control, privileged account management, access reviews	ISO 27001, HIPAA, SOC 2, NIST CSF	Prevents unauthorized access to sensitive data, demonstrates proper PHI protection
Data Protection	Encryption (AES-256 at rest, TLS 1.3 in transit), data classification, DLP	HIPAA, ISO 27001, NIST CSF	Protects patient data from unauthorized access, meets explicit HIPAA requirements
Threat & Vulnerability Management	SIEM implementation, security monitoring, vulnerability scanning	SOC 2, NIST CSF, ISO 27001	Enables early detection of potential security incidents, demonstrates due care
Third-Party Risk Management	Vendor assessments, continuous monitoring, contractual requirements	HIPAA, SOC 2, ISO 27001	Reduces supply chain risk, ensures vendor compliance with security requirements
Risk Management	Risk register, assessment methodology, treatment plans	ISO 27001, NIST CSF, HIPAA	Creates systematic approach to identifying and addressing security risks

CCF Category	Control Implementation	Primary Compliance Frameworks	Business Benefit
Business Resilience	BCP/DRP development, testing procedures, recovery objectives	HIPAA, ISO 27001, SOC 2	Ensures service continuity and data preservation during disruptions
Security Governance	Security policies, standards, and procedures development	All frameworks	Creates foundation for security program and demonstrates management commitment
Security Training & Awareness	Training program, phishing simulations, role-specific education	HIPAA, ISO 27001, NIST CSF	Reduces human error risk, increases security awareness organization-wide
Change & Configuration Management	Change control process, secure configuration baselines	SOX, ISO 27001, SOC 2	Prevents unauthorized system changes, maintains secure configurations
Incident Management	Response plan, team development, testing exercises	ISO 27001, HIPAA, NIST CSF	Minimizes impact of security incidents through prompt, effective response

5.3 High-Level Implementation Roadmap (12 Months)

Based on the risk assessment and compliance requirements, the following implementation roadmap prioritizes critical controls while establishing a systematic approach to achieving comprehensive compliance:

The roadmap phases are designed to meet regulatory benchmarks set by key frameworks *(ISO, 2013; AICPA, 2017; HHS, n.d.; U.S. Congress, 2002; NIST, 2018)*.

Phase	Timeline	Key Activities	Deliverables	Success Metrics
1: Foundation	**Month 1-2**	• Complete detailed risk assessment • Develop security governance structure • Establish security policies • Create project team and governance	• Security policy framework • Risk assessment report • Project charter • Executive brief	• Security policy approval • Project team established • Executive sponsorship secured

Phase	Timeline	Key Activities	Deliverables	Success Metrics
2: Critical Controls	**Month 3-4**	• Implement access control system • Deploy encryption for PHI • Develop incident response plan • Establish vendor assessment process	• RBAC implementation • Encryption deployment • IR plan and team • Vendor questionnaires	• 100% PHI under access controls • All PHI encrypted at rest • IR team established • Top vendors assessed
3: Monitoring & Detection	**Month 5-6**	• Deploy SIEM solution • Implement security monitoring • Establish vulnerability management • Develop change management process	• SIEM deployment • Security dashboards • Vulnerability scans • Change control process	• Log sources integrated • Alert mechanisms tested • Initial vulnerability remediation • Change process followed
4: Operational Controls	**Month 7-8**	• Launch security awareness program • Implement business continuity planning • Develop audit processes • Establish risk management program	• Training curriculum • BCP/DRP documentation • Audit schedule • Risk register	• All staff trained • Recovery objectives defined • Audit capability established • Risks documented and assessed
5: Testing & Validation	**Month 9-10**	• Conduct security testing • Run tabletop exercises • Perform BCP/DRP testing • Validate control effectiveness	• Penetration test results • IR exercise reports • BCP test outcomes • Control validation report	• Critical vulnerabilities remediated • Successful IR exercises • Recovery capabilities validated • Control effectiveness demonstrated
6: Preparation & Documentation	**Month 11-12**	• Prepare for external audits • Finalize documentation• Conduct final gap remediation • Complete compliance readiness assessment	• Compliance documentation • Evidence repository • Remediation report • Readiness assessment	• SOC 2 readiness confirmed • HIPAA compliance validated • ISO 27001 gaps closed • Continuous compliance approach established

5.4 Implementation Considerations and Critical Success Factors

For successful implementation, MediCore AI Solutions should consider the following factors:

1. **Resource Allocation**: Dedicated security personnel and budget for tools/technologies
2. **Executive Sponsorship**: Clear leadership support and accountability for the program
3. **Phased Approach**: Prioritizing high-risk areas while building toward comprehensive compliance
4. **Integration with Development**: Incorporating security into the software development lifecycle
5. **Metrics and Monitoring**: Establishing KPIs to track implementation progress and effectiveness
6. **Technology Enablement**: Selecting appropriate tools to automate and scale compliance efforts
7. **Cultural Alignment**: Fostering a security-minded culture throughout the organization

6. Conclusion and Recommendations

The comprehensive compliance framework presented in this report provides MediCore AI Solutions with a strategic approach to addressing multiple regulatory requirements while establishing strong security practices. By implementing the Common Controls Framework methodology, the company can efficiently meet compliance obligations while minimizing redundancy and operational burden.

Key recommendations for successful implementation include:

1. **Prioritize Critical Risks**: Focus initial implementation efforts on addressing the highest-risk areas identified in the risk assessment, particularly access control and data protection.
2. **Establish Security Governance**: Develop a formal security governance structure with clear roles, responsibilities, and executive sponsorship.
3. **Leverage Automation**: Invest in security automation tools to scale compliance efforts efficiently, particularly for monitoring, detection, and access management.
4. **Build Security Culture**: Integrate security awareness into the organizational culture through comprehensive training and regular communication.
5. **Prepare for Growth**: Design the compliance framework with scalability in mind to accommodate future business expansion and evolving regulatory requirements.

Through systematic implementation of this framework, MediCore AI Solutions will establish a strong security posture, demonstrate regulatory compliance, build customer trust, and create a sustainable foundation for secure business operations and growth.

7. References

1. **International Organization for Standardization.** (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. https://www.iso.org/standard/54534.html
2. **American Institute of Certified Public Accountants (AICPA).** (2017). *SOC 2® – SOC for Service Organizations: Trust Services Criteria*. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html
3. **U.S. Department of Health & Human Services.** (2006). *The HIPAA Security Rule (45 CFR Parts 160 and 164)*. https://www.hhs.gov/hipaa/for-professionals/security/index.html
4. **U.S. Congress.** (2002). *Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745*. https://www.congress.gov/bill/107th-congress/house-bill/3763
5. **National Institute of Standards and Technology (NIST).** (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://www.nist.gov/cyberframework
6. **Unified Compliance.** (n.d.). *Common Controls Framework (CCF)*. https://www.unifiedcompliance.com/ccf/
7. **HITRUST Alliance.** (n.d.). *HITRUST CSF: A certifiable framework to manage risk (HITRUST Alliance, n.d.)*. https://hitrustalliance.net/hitrust-csf/
8. **National Institute of Standards and Technology (NIST).** (2020). *Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final