ISO 27001 Internal Audit – Healthcare Organization

As the designated Internal Auditor, I was tasked with evaluating the effectiveness and maturity of the organization's implementation of ISO/IEC 27001 controls. The organization operates within the healthcare sector, handling sensitive patient information and must adhere to strict regulatory and compliance obligations (such as HIPAA, GDPR, or national healthcare laws, depending on jurisdiction).

1. Reviewed Existing Security Controls Against ISO 27001 Requirements

Approach:

- Used an ISO 27001 audit checklist based on Clauses 4–10 and Annex A controls.
- Focus areas for healthcare:

  A.8 Asset Management – Proper inventory of patient record systems

  A.9 Access Control – Segregation of duties for doctors, nurses, admins

  A.13 Communications Security – Secure transmission of health data

  A.18 Compliance – HIPAA, local health privacy laws

Sample finding format:

Control	Status	Evidence	Comment
A.9.1.2 - user access provisioning	Partial	No formal approval process found	Medium risk of unauthorized access

2. Conducted Interviews with Key Personnel

Interview Targets:

- CISO / Security Manager
- IT Admins
- Clinical System Users
- HR (for onboarding/offboarding processes)
- Legal/Compliance Officer

Topics:

- Understanding of ISMS policies

- Role-specific security practices
- Awareness of incident response procedures
- Recent changes in data handling or systems

3. Evaluated Incident Response and Business Continuity Plans

Key Evaluation Criteria:

Area	Indicators of effectiveness
Incident Response	Incident log maintained, roles defined, post-incident reviews
BCP/DRP	Backup frequency, offsite storage, tested failover drills
Awareness	Staff can articulate what to do in an incident
Compliance	Aligned with ISO 27031 (ICT continuity) and ISO 22301 (BCM) where applicable

Red flag example:

Backup recovery not tested in the past 12 months → Risk of unverified recovery capability.

4. Identified Non-Conformities & Areas for Improvement

Types of non-conformities:

Major: Absence of formal access control policy

Minor: Incomplete user access reviews

Opportunities for Improvement (OFIs): Outdated AUP training content

Audit Report Table Example:

Finding	Type	Reference	Recommendation
No documented risk assessment	Major	Clause 6.1.2	Implement a formal risk assessment framework ASAP
Incident response plan untested	Minor	A.16.1.5	Schedule and document tabletop exercise quarterly

Weak access termination process	OFI	A.9.2.6	Automate deprovisioning via HR-IT sync

5. Provide Recommendations for Corrective Actions & Improvements

Corrective Action Plan Format:

Area	Action	Responsible party	Deadline	Follow-up date
Risk Assessment	Conduct full risk assessment workshop	CISO	May 15, 2025	June 15, 2025
DR Testing	Perform simulated outage test	IT Ops	June 1, 2025	July 1, 2025

General Improvement Suggestions:

- Implement a centralized GRC platform to manage risk & compliance.
- Introduce periodic internal security awareness campaigns.
- Update ISMS documentation annually and after major incidents.

Deliverables:

- ISO 27001 Internal Audit Report
- Non-conformity Register
- Corrective Action Plan (CAP)
- Executive Summary with Risk Heatmap (optional)
- Audit Presentation for Leadership