Gap Assessment Report for FitZone Health & Wellness Pvt. Ltd.

Executive Summary

This Gap Assessment Report evaluates FitZone Health & Wellness Pvt. Ltd.'s current information security posture against ISO 27001:2022 requirements. The assessment identifies critical gaps in security controls, policies, and procedures that must be addressed to achieve certification within the 10-month timeline.

Key Findings:

- **7 Critical Gaps** requiring immediate attention
- **Overall Compliance Level:** ~25% (Low)
- **Highest Risk Areas:** Access control, network security, vendor management, cryptography
- **Timeline Risk:** High (significant effort required in limited timeframe)

Gap Assessment Matrix

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
Clause 6.1.2	Information Security Risk Assessment	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria (risk acceptance, risk analysis methods); b) ensures risk assessments produce consistent, valid and comparable results; c) identifies information security risks (asset identification, threat identification,	No formal risk assessment process exists. Risks are handled reactively when incidents occur. No documented risk criteria, risk register, or risk analysis methodology. Management is unaware of current risk exposure.	**Critical Gap:** Absence of systematic risk assessment process prevents informed decision-making and is a fundamental requirement for ISO 27001 compliance. Without risk assessment, the organization cannot demonstrate it understands its security risks or has appropriate controls.	**Immediate Action Required:** 1) Establish risk assessment methodology document defining criteria for likelihood, impact, and risk acceptance levels. 2) Create comprehensive risk register identifying assets, threats, vulnerabilities, and controls (initial register provided as starting point). 3) Conduct facilitated risk workshops with stakeholders from IT, operations, and management. 4) Obtain management approval for risk treatment plan. 5) Schedule quarterly

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
		vulnerability identification, impact identification); d) analyzes information security risks (likelihood and consequences assessment); e) evaluates information security risks (comparison with risk criteria, prioritization).			risk assessment reviews. **Timeline:** Complete within 6 weeks.
Control 5.15	Access Control	Management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. Rules for handling and protecting authentication information shall be established according to its classification.	Front desk staff have admin-level access to membership management system with shared credentials in some cases. No role-based access control (RBAC) implemented. No password policy exists. Authentication information (passwords) are written on sticky notes near workstations. No periodic access reviews.	**Critical Gap:** Lack of access control policy and RBAC creates significant risk of unauthorized access to sensitive member data (personal info, health records, payment details). This violates principle of least privilege and increases insider threat risk, especially with high staff turnover.	**Immediate Action Required:** 1) Draft and implement Access Control Policy defining roles, responsibilities, and approval processes. 2) Implement role-based access control in membership system - define roles: Admin, Manager, Front Desk, Trainer, Read-Only. 3) Conduct immediate access rights review and remove excessive privileges. 4) Implement password policy (minimum 12 characters, complexity requirements, 90-day rotation, no reuse of last 5 passwords). 5) Deploy password manager for staff. 6) Implement multi-factor

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
					authentication (MFA) for admin accounts. 7) Schedule quarterly access rights reviews. **Timeline:** Complete RBAC implementation within 8 weeks.
Control 5.24	Information Security Incident Management Planning and Preparation	The organization shall plan and prepare for managing information security incidents by: a) establishing information security incident management processes, procedures and responsibilities; b) establishing and maintaining an information security incident response plan; c) providing awareness training on incident reporting and response; d) implementing mechanisms for timely detection, reporting, and escalation.	Last year's ransomware attempt went unreported for 3 days. No documented incident response plan exists. Staff are unaware of what constitutes a security incident or how to report it. No incident response team or defined roles. Incidents are handled ad-hoc by IT staff when they become aware of issues. No incident log or post-incident review process.	**Critical Gap:** Inadequate incident management capabilities resulted in delayed response to ransomware, potentially increasing damage and exposing organization to regulatory penalties. Without formal incident response procedures, future incidents will continue to be mishandled, causing operational disruption and reputational damage.	**Immediate Action Required:** 1) Draft Incident Response Policy defining incident categories (security, privacy, operational), severity levels, and escalation matrix. 2) Establish Incident Response Team with defined roles: Incident Manager (IT Manager), Security Analyst (IT Security), Communications Lead (Marketing Manager), Legal Advisor (Legal Team), Management Representative (COO). 3) Create incident response procedures covering: detection and reporting (24/7 reporting mechanism), initial assessment and triage, containment strategies, eradication and recovery, evidence preservation, post-incident review. 4) Deploy incident ticketing system for logging and tracking. 5) Conduct tabletop

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
					exercises simulating ransomware, data breach, and DDoS scenarios. 6) Develop incident communication templates for internal and external stakeholders. 7) Establish relationships with external incident response consultants and cyber insurance provider. **Timeline:** Complete within 10 weeks.
Control 8.20	Networks Security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. Security measures shall include: a) controls to protect information within networks; b) security mechanisms on networks; c) procedures to manage network devices; d) logical separation of networks.	Members and staff share the same Wi-Fi network without any segmentation. No network security policy exists. Guest Wi-Fi has no bandwidth limitations or content filtering. No network monitoring or intrusion detection system (IDS) in place. Network devices (routers, switches) use default credentials in some locations. Network diagrams are outdated or non-existent.	**Critical Gap:** Shared network infrastructure creates multiple attack vectors. Malicious members or guests could perform man-in-the-middle attacks, intercept sensitive data (including payment card information during transactions), or gain unauthorized access to internal systems. This violates PCI-DSS requirements for payment card handling.	**Immediate Action Required:** 1) Implement network segmentation across all 5 locations: Corporate network (management, finance, HR), Staff network (trainers, front desk systems), Guest Wi-Fi (members), IoT network (biometric scanners, CCTV), Payment network (PCI-DSS compliant segment for payment terminals). 2) Configure VLANs and firewall rules to restrict inter-network communication. 3) Deploy WPA3-Enterprise for staff network with RADIUS authentication. 4) Configure guest Wi-Fi with captive

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
					portal, bandwidth limits, and device isolation. 5) Implement network monitoring solution with IDS/IPS capabilities. 6) Change all default credentials on network devices and implement secure management practices. 7) Conduct network penetration testing after implementation. **Timeline:** Complete within 12 weeks.
Control 8.24	Use of Cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. Considerations shall include: a) cryptographic controls for data at rest; b) cryptographic controls for data in transit; c) key lifecycle management; d) legal and regulatory requirements related to cryptography.	Sensitive health data (medical history, fitness assessments, body metrics) is stored in the membership database without encryption at rest. Data in transit over shared Wi-Fi network has no additional encryption layer beyond application-level TLS (which may be misconfigured). Payment data encryption status is unknown. No cryptographic policy or key management procedures exist.	**Critical Gap:** Absence of encryption for health data violates data protection principles and creates severe risk of data breach. If database is compromised (via SQL injection, insider threat, or vendor breach), all member health information would be exposed in plaintext. This creates regulatory non-compliance risk under DPDP Act 2023 and potential liability for breach notification and penalties.	**Immediate Action Required:** 1) Draft Cryptography Policy defining: encryption standards (AES-256 for data at rest, TLS 1.3 for data in transit), key management procedures, approved algorithms, and responsibilities. 2) Implement database encryption at rest for membership system: Full database encryption using Transparent Data Encryption (TDE), Column-level encryption for sensitive fields (medical history, health assessments, payment tokens). 3) Configure TLS 1.3 on all web

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
					services and APIs; disable TLS 1.0/1.1 and weak ciphers. 4) Implement VPN for staff accessing systems remotely. 5) Verify payment data encryption with payment gateway provider and ensure PCI-DSS compliance. 6) Establish key management procedures including secure key generation, storage in hardware security module (HSM) or cloud key management service, rotation schedules, and access controls. 7) Conduct encryption verification testing. **Timeline:** Complete within 10 weeks.
Control 5.19 & 5.20	Information Security in Supplier Relationships & Addressing Security within Supplier Agreements	The organization shall define and implement processes to manage information security risks associated with supplier relationships. Requirements: a) identify and document supplier relationships and information security risks; b) define types of supplier relationships and corresponding security requirements; c) include information	Third-party vendor (GymTech Solutions) has full administrative access to member database but: No security assessment or due diligence performed before engagement, No data processing agreement (DPA) in place, Contract does not specify security requirements, SLAs, or breach	**Critical Gap:** Vendor GymTech Solutions represents a significant third-party risk. If their systems are breached, all FitZone member data could be compromised without FitZone's knowledge. Lack of contractual security obligations means FitZone has no legal recourse and may be held	**Immediate Action Required:** 1) Conduct urgent third-party risk assessment for GymTech Solutions: Request security questionnaire (SOC 2 report, ISO 27001 certificate, security policies), Review data processing activities and sub-processor list, Assess backup and disaster recovery capabilities, Verify incident response and breach notification procedures. 2) Negotiate and execute Data Processing

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
		security requirements in supplier agreements addressing: access controls, data protection obligations, incident notification, right to audit, data return/destruction, liability and indemnification; d) monitor and review supplier security performance.	notification obligations, No monitoring of vendor security practices, No right to audit vendor security controls, Unknown if vendor has sub-processors accessing data. Mobile app development agency was engaged 2 years ago without security requirements; current security posture unknown. Payment gateway integration with Razorpay/Paytm lacks security oversight.	liable for vendor-caused breaches under DPDP Act. This creates existential risk to business reputation and regulatory compliance.	Agreement (DPA) with GymTech including: Data protection obligations aligned with DPDP Act, Security control requirements (encryption, access control, logging), Incident notification within 24 hours, Right to audit annually or upon security event, Data return/destruction upon contract termination, Liability and indemnification clauses. 3) Establish vendor security requirements template for all new suppliers. 4) Conduct security assessment of mobile app development agency and payment gateway providers. 5) Implement vendor monitoring program with quarterly security reviews. 6) Maintain vendor risk register tracking all supplier relationships. **Timeline:** Complete DPA negotiation within 8 weeks.
Control 8.8	Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained in a timely	Payment terminals are outdated (potentially running unsupported firmware	**Critical Gap:** Outdated payment terminals pose severe PCI-DSS compliance risk	**Immediate Action Required:** 1) Create comprehensive IT asset inventory documenting: All payment terminals (make, model,

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
		manner, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures shall be taken. Requirements include: a) establishing processes to identify and track vulnerabilities; b) defining timelines for vulnerability remediation based on risk; c) conducting regular vulnerability assessments; d) maintaining inventory of assets and software versions.	versions). Mobile application has not undergone security testing (penetration testing or vulnerability scanning) for 2 years. No vulnerability management process exists. No asset inventory documenting software versions, patch levels, or end-of-life status. IT staff manually patch systems when they remember, with no tracking. Critical vulnerabilities may remain unpatched for months.	and could expose payment card data to known exploits (e.g., memory scraping malware). The mobile app's unknown security posture puts 8,500 members at risk when using the app for payments and accessing sensitive data. Without vulnerability management, the organization is operating blind to its technical exposure.	firmware version, location), Servers and network equipment, Workstations and tablets, Mobile applications and APIs, Third-party SaaS platforms, Software licenses and versions. 2) Assess payment terminal security: Verify PCI-DSS PA-DSS compliance status, Check for available firmware updates, Determine if terminals support current security standards, Plan replacement if end-of-life. 3) Conduct immediate penetration testing and vulnerability assessment of: Mobile application (iOS and Android), Web application/member portal, APIs, Network infrastructure (all 5 locations). 4) Implement vulnerability management process: Subscribe to vulnerability intelligence feeds, Deploy automated vulnerability scanning tools (quarterly scans), Establish remediation timelines (Critical: 7 days, High: 30 days, Medium: 60 days, Low: 90 days), Create patch management

Clause/Control Number	Clause/Control	Requirement (as per ISO 27001:2022)	Current State	Gap Identified	Recommendation
					procedure with testing and rollback plans. 5) Remediate all critical and high vulnerabilities identified in initial assessment. 6) Schedule annual penetration testing for mobile app. **Timeline:** Complete initial assessment within 10 weeks; ongoing process.

Additional Gaps Identified (Quick Reference)

Gap Area	Current State	Required State	Priority
Clause 5 (Leadership & Commitment)	No ISMS policy document. Management has not formally assigned information security roles and responsibilities.	Top management must demonstrate leadership by establishing ISMS policy, assigning roles, and allocating resources.	High
Clause 7.2 (Competence)	No documented competency requirements for security-sensitive roles. High staff turnover with no security training for new hires.	Define competency requirements and ensure personnel receive appropriate training and possess necessary skills.	Medium
Clause 9.2 (Internal Audit)	No internal audits have been conducted. No audit program established.	Conduct internal audits at planned intervals to verify ISMS conformity and effectiveness. Schedule first internal audit 2 months before certification audit.	High
Control 5.33 (Protection of Records)	No data retention policy. Member data retained indefinitely after membership expiry.	Establish retention schedule based on legal/regulatory requirements (DPDP Act requires data minimization). Implement secure disposal procedures.	High
Control 6.3 (Security Awareness Training)	No documented security awareness program. New employees receive no security training during onboarding.	Develop comprehensive security awareness program covering: phishing, password security, physical security, incident reporting, acceptable use. Conduct training during onboarding and annual refreshers. Track attendance.	Medium

Implementation Roadmap

Phase 1: Foundation (Weeks 1-12) - Critical Priority

Objective: Address critical gaps and establish ISMS foundation

1. **Week 1-2:** Establish ISMS scope, policy, and governance structure

2. **Week 3-6:** Complete risk assessment and obtain management approval
3. **Week 6-8:** Implement access control policy and RBAC
4. **Week 8-10:** Implement network segmentation across all locations
5. **Week 10-12:** Deploy encryption for health data and complete cryptography policy

Deliverables: ISMS Policy, Risk Register, Access Control Policy, Network Security Implementation, Cryptography Policy

---

Phase 2: Control Implementation (Weeks 13-24) - High Priority

Objective: Implement key ISO 27001 controls and policies

1. **Week 13-16:** Establish incident response capabilities and procedures
2. **Week 16-20:** Conduct vendor security assessments and execute DPAs
3. **Week 20-22:** Implement vulnerability management program and conduct security testing
4. **Week 22-24:** Develop and deliver security awareness training program

Deliverables: Incident Response Policy, Vendor Management Framework, Vulnerability Management Process, Security Training Program

---

Phase 3: Documentation & Continuous Improvement (Weeks 25-36) - Medium Priority

Objective: Complete documentation and prepare for certification audit

1. **Week 25-28:** Document all ISMS procedures and work instructions
2. **Week 28-30:** Establish data retention policy and implement disposal procedures
3. **Week 30-32:** Complete Statement of Applicability and control evidence
4. **Week 32-34:** Conduct first internal audit and address findings
5. **Week 34-36:** Management review and readiness assessment

Deliverables: Complete ISMS documentation, Data Retention Policy, Internal Audit Report, Management Review Minutes

---

Phase 4: Certification Preparation (Weeks 37-40)

Objective: Final preparation and Stage 1 audit

1. **Week 37-38:** Second internal audit focusing on certification readiness
2. **Week 38-39:** Address any remaining non-conformities
3. **Week 39-40:** Stage 1 certification audit (documentation review)
4. **Week 40+:** Stage 2 certification audit (implementation verification)

Resource Requirements

Personnel:

- ISO 27001 Lead Implementer (Full-time, 10 months)
- IT Manager (50% allocation)

- IT Security Specialist (Hire or contract, Full-time for 6 months)
- Network Engineer (Contract for network segmentation, 3 months)
- Part-time involvement: HR Manager, Facility Manager, Legal Advisor, Operations Managers

Technology Investments:

- Network segmentation equipment (managed switches, firewalls): ₹8-12 lakhs
- Network monitoring/IDS solution: ₹3-5 lakhs annually
- Vulnerability scanning tools: ₹2-3 lakhs annually
- Encryption implementation (TDE licensing if needed): ₹2-4 lakhs
- Incident management ticketing system: ₹1-2 lakhs annually
- Password manager enterprise licenses: ₹50,000 annually
- Payment terminal upgrades/replacements: ₹5-8 lakhs (if required)

External Services:

- Penetration testing (mobile app, network): ₹4-6 lakhs
- Vendor security assessments: ₹2-3 lakhs
- Legal review of DPAs and policies: ₹1-2 lakhs
- ISO 27001 certification audit fees: ₹3-5 lakhs
- Security awareness training platform: ₹1-2 lakhs annually

Total Estimated Budget: ₹30-50 lakhs over 10 months

Risk to Timeline

Assessment: HIGH RISK to achieving certification in 10 months

Challenges:

1. **Scope:** 13 critical controls not implemented
2. **Infrastructure changes:** Network segmentation across 5 locations requires significant effort
3. **Vendor dependency:** GymTech Solutions negotiations may be time-consuming
4. **Resource constraints:** Small IT team with limited security expertise
5. **Cultural change:** High staff turnover requires ongoing training efforts

Mitigation Strategies:

- Hire/contract dedicated security resources immediately
- Prioritize critical controls using risk-based approach
- Consider staged certification (initial scope limited to head office, expand later)
- Engage experienced ISO 27001 consultant for accelerated implementation
- Obtain strong management commitment and resource allocation

---

Compliance Status Summary

ISO 27001:2022 Clause	Compliance Level	Key Gaps
Clause 4 (Context)	30%	ISMS scope not formally defined; stakeholder needs not documented
Clause 5 (Leadership)	20%	No ISMS policy; roles and responsibilities not assigned
Clause 6 (Planning)	15%	No risk assessment process; no risk treatment plan; no objectives
Clause 7 (Support)	35%	Limited documentation; no training program; inadequate resources
Clause 8 (Operation)	25%	Critical controls missing (access, encryption, incident response, vendor)
Clause 9 (Performance Evaluation)	10%	No internal audits; no monitoring; no management review
Clause 10 (Improvement)	20%	No non-conformity process; no continuous improvement mechanism
Overall ISMS Maturity	**~25%**	**Significant implementation work required across all clauses**

Document Version: 1.0

Prepared By: ISO 27001 Lead Implementer

Date: October 15, 2025

Next Review: November 15, 2025

Approved By: Chief Executive Officer