HAACrypt

Methodology Document

INDEX

INTRODUCTION

In today's increasingly complex and interconnected digital landscape, cybersecurity is not just a necessity—it is a strategic imperative. HAACRYPT LLP stands at the forefront of this mission, dedicated to building robust defenses that secure your organization's most critical assets while enabling seamless, confident operations.

Our services are designed to establish and maintain a **digital line of control**—a clear, enforceable boundary that shields your digital infrastructure from evolving threats. Whether it's safeguarding sensitive data, ensuring business continuity, or meeting regulatory compliance, we provide tailored security solutions that adapt to your unique operational needs.

At HAACRYPT, we don't believe in one-size-fits-all security. Our approach combines **deep technical expertise**, **precision-driven methodology**, and a **client-first mindset** to deliver outcomes that matter. We engage with you as strategic partners—understanding your environment, assessing risk, and crafting end-to-end protection frameworks that enhance both resilience and agility.

From proactive threat detection to advanced incident response, we empower your business to operate with **trust, clarity, and control** in a world where cyber risks are constantly evolving. With HAACRYPT, security isn't just about defense—it's about enabling your growth, maintaining trust, and preserving your digital future.

WHO ARE WE

We are a team of cybersecurity experts forged from **real-world experience**. We don't just understand security — we live it. From defensive fortification to offensive simulation, we are your digital guardians, committed to shielding your kingdom from ever-evolving threats.

Vision

Making cybersecurity robust and convenient at same time offering tailored services, trusted solutions, and meaningful impact — with zero tolerance for shortcuts or superficial fixes.

Mission

At HAACrypt, we believe that cybersecurity should never be a barrier — it should be convenient, seamless, and always-on. Because in a world where data is money, and money is data, you can't afford to be unprotected.

WHAT WE OFFER?

Payment Security

- PCI DSS v4.0.1 – Payment Card Industry Data Security Standard
- PCI 3DS v1.0 – Payment Card Industry 3-D Secure
- PCI S3 v1.2.1 – Payment Card Industry Secure Software Standard
- PCI PIN v3.1 - Payment Card Industry PIN Standard

Privacy and Compliance

- HIPAA – Health Insurance Portability & Accountability Act
- GDPR – General Data Protection Regulation

Testing Services

- Internal Vulnerability Assessment
- Internal Penetration Testing
- External Penetration Testing
- Web Application Penetration Testing
- Segmentation Penetration Testing
- Mobile Application Penetration Testing
- API Security Testing
- Source Code Review
- Network Device Configuration Review

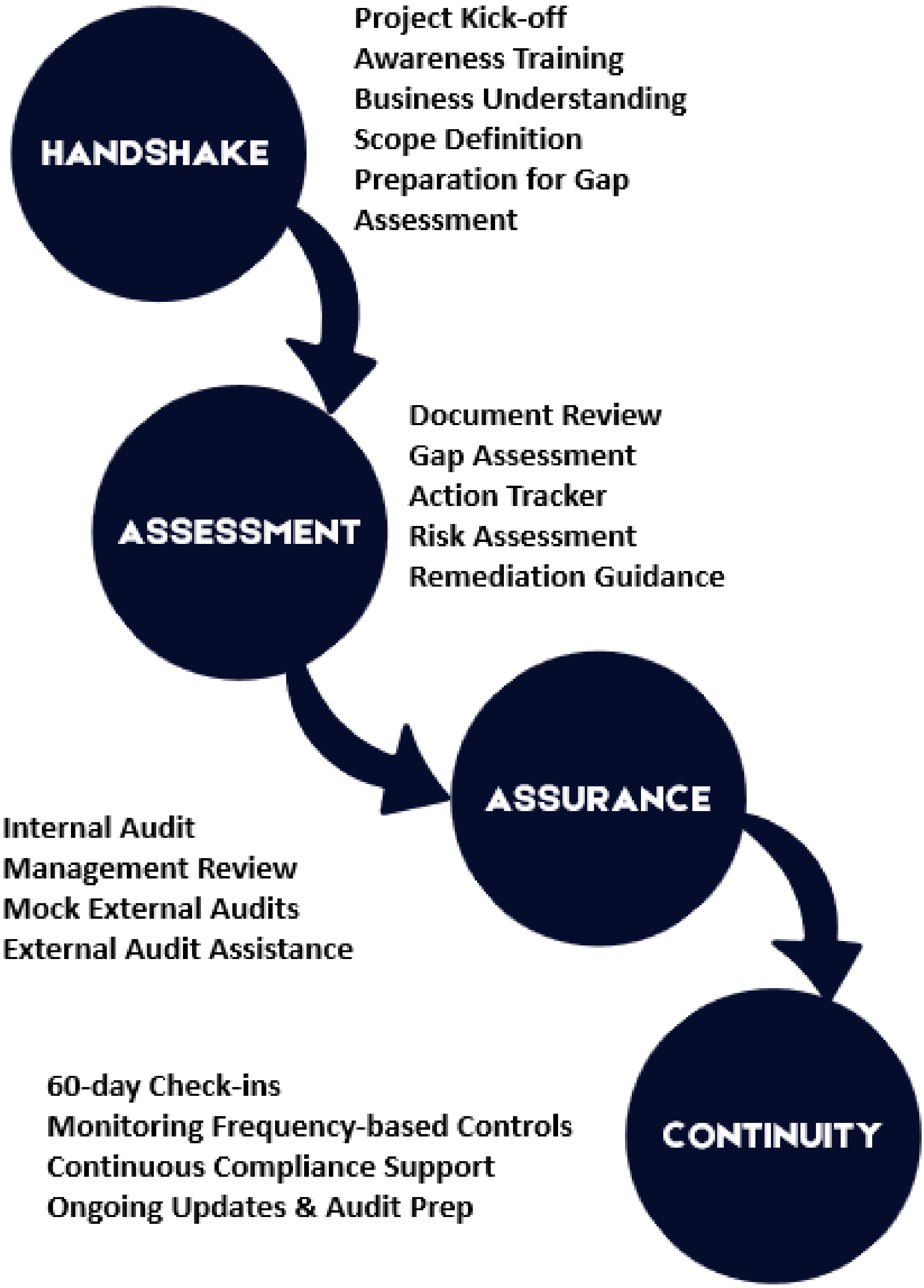
Management System

- ISO/IEC 27001:2022 – Information Security Management Systems (ISMS)
- ISO/IEC 27701:2019 – Privacy Information Management System (PIMS)

Framework Assessment

- AICPA SOC 2 (Type I & II)
- NIST Privacy Framework
- NIST CSF 2.0
- NIST SP 800-53
- DPDPA

THE HAAC WAY



HANDSHAKE

Project Kick-off
Awareness Training
Business Understanding
Scope Definition
Preparation for Gap Assessment

ASSESSMENT

Document Review
Gap Assessment
Action Tracker
Risk Assessment
Remediation Guidance

ASSURANCE

Internal Audit
Management Review
Mock External Audits
External Audit Assistance

CONTINUITY

60-day Check-ins
Monitoring Frequency-based Controls
Continuous Compliance Support
Ongoing Updates & Audit Prep

ISO/IEC 27001:2022 (ISMS)

ISO/IEC 27001 is the **leading international standard** for establishing, implementing, maintaining, and continually improving an **Information Security Management System (ISMS)**, helping organizations protect the confidentiality, integrity, and availability of information through a structured, risk-based approach and a defined set of controls in Annex A updated in 2022.

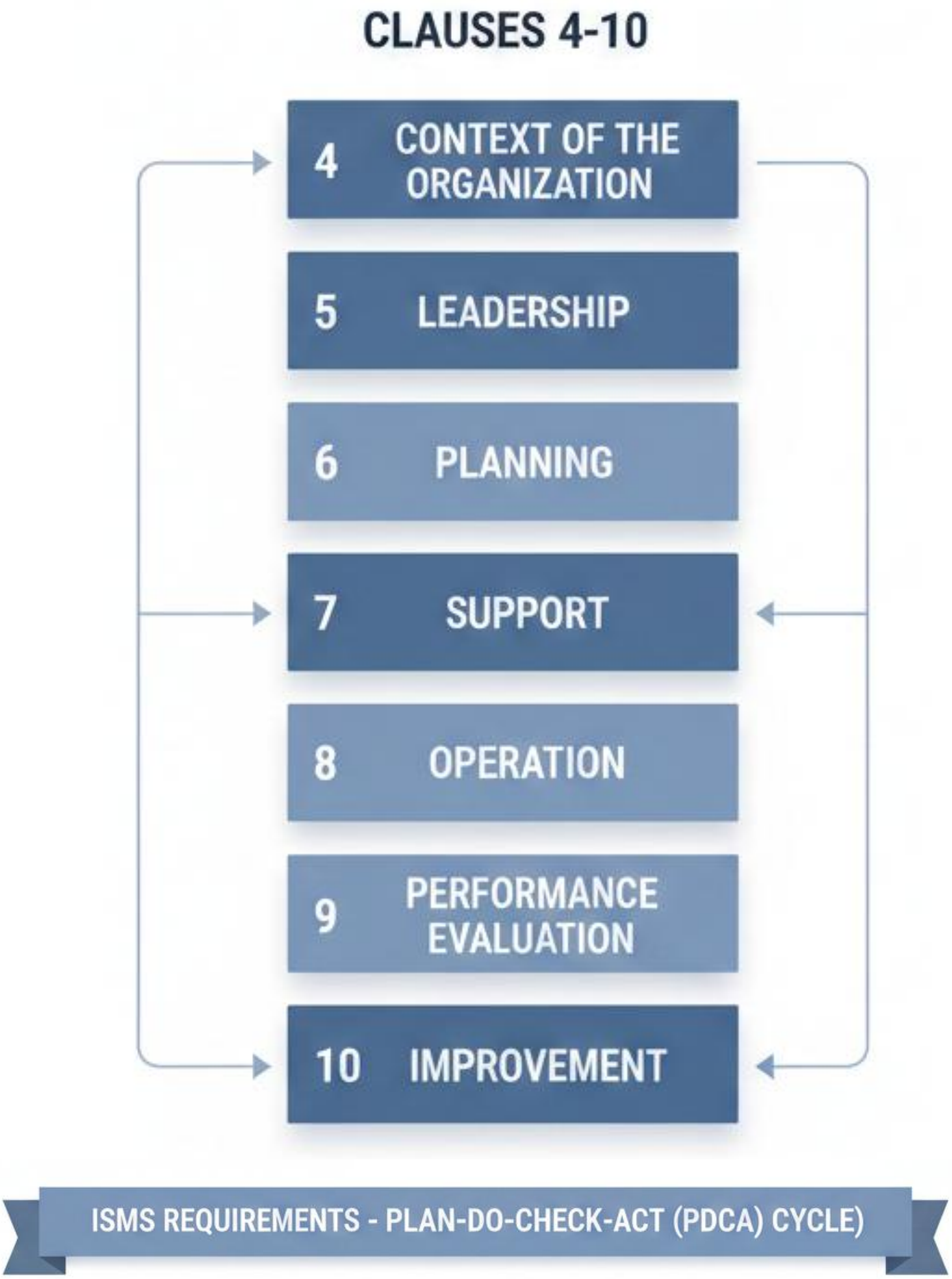
Clauses 4–10 : context, leadership, planning, support, operation, performance evaluation, and improvement.

Annex A lists 93 controls grouped into four themes: Organizational, People, Physical, and Technological.

Clauses 0–3 are introductory (scope, references, terms), while Clauses 4–10 are mandatory for certification.

The clauses specify the management system "what," and Annex A provides selectable control "how" to treat identified risks.

ISO/IEC 27001:2022 - Information Security Management System (ISMS)



CLAUSES 4-10

4 CONTEXT OF THE ORGANIZATION

5 LEADERSHIP

6 PLANNING

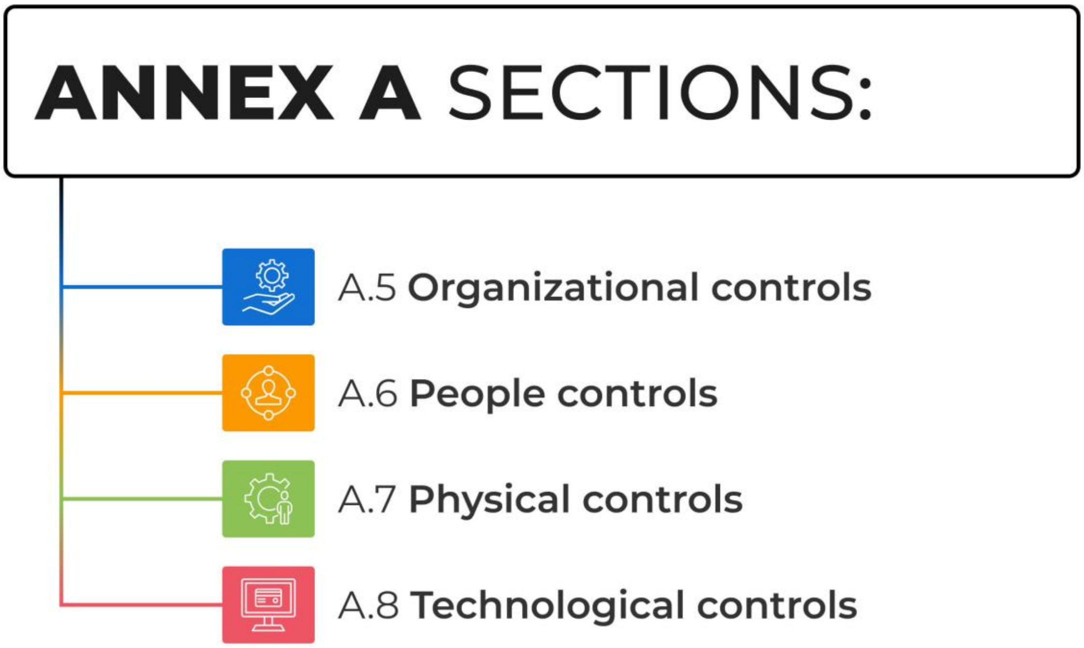
7 SUPPORT

8 OPERATION

9 PERFORMANCE EVALUATION

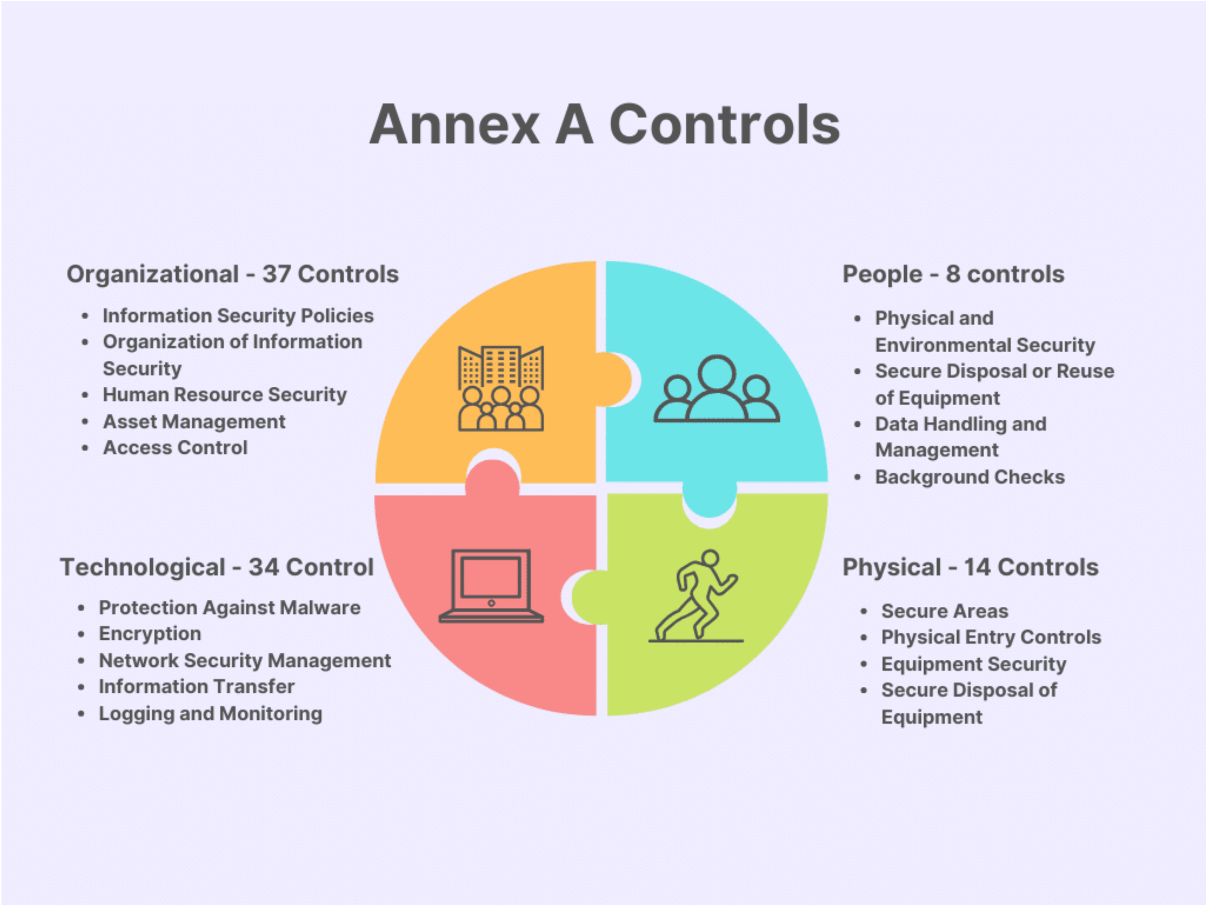
10 IMPROVEMENT

ISMS REQUIREMENTS - PLAN-DO-CHECK-ACT (PDCA) CYCLE)



ANNEX A SECTIONS:

- A.5 **Organizational controls**
- A.6 **People controls**
- A.7 **Physical controls**
- A.8 **Technological controls**



Annex A Controls

Organizational - 37 Controls

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control

People - 8 controls

- Physical and Environmental Security
- Secure Disposal or Reuse of Equipment
- Data Handling and Management
- Background Checks

Technological - 34 Control

- Protection Against Malware
- Encryption
- Network Security Management
- Information Transfer
- Logging and Monitoring

Physical - 14 Controls

- Secure Areas
- Physical Entry Controls
- Equipment Security
- Secure Disposal of Equipment

WHY IT MATTERS?

Revenue enablement

Speeds enterprise procurement and vendor due-diligence, shortening sales cycles and unlocking bigger deals through recognized, third-party certification

Risk and loss reduction

Lowers breach likelihood and impact via a structured, risk-based ISMS, cutting potential outage, legal, and remediation costs

Regulatory defensibility

Provides a mapped, auditable control framework that supports compliance with privacy and sector requirements, reducing fines and audit friction

Operational governance

Embeds leadership-driven security, clear accountability, and continuous improvement, improving uptime and board-level assurance

Brand trust and investor confidence

Demonstrates provable security to customers, partners, and investors, strengthening reputation and competitive positioning

ISO 27001 METHODOLOGY

HANDSHAKE

Project Initiation & Planning

Conducting a **Kick-off** to define objectives, stakeholders, methodology, and timelines.

Delivering **ISMS Awareness Sessions** to the key stakeholders and core ISMS team.

Securing **Management Commitment** to allocate necessary resources.

Developing a detailed **Project Plan** and **Communication Matrix** for consistent updates.

Creating and sharing the **Project Initiation Document**

ASSESSMENT

ISMS Scoping

Define the **ISMS Scope**, considering internal/external factors and interested parties.

Develop a **draft Statement of Applicability (SoA)** based on the current business context and identified controls.

Gap Assessment

Perform a thorough **assessment of existing policies, processes, and controls**.

Compare the current state against ISO/IEC 27001 requirements.

Deliver a **Gap Analysis Report** along with an **Action Tracker** to provide a clear remediation roadmap.

Risk Assessment and Treatment

Develop a **Risk Management methodology**

Conduct **Risk Assessment**

Prepare a Risk Treatment Plan to mitigate identified risks.

Assist in selecting and implementing appropriate Annex A controls.

ASSURANCE

Implementation Support

Finalizing the **Statement of Applicability** for risk control.

Assisting in the development of **information security policies, procedures, and supporting documents**.

Guiding the **deployment of controls** and maintaining **records of their implementation**.

Providing **ongoing consultations** during control implementation and monitoring.

Monitoring performance to ensure objectives are achieved.

Internal Audit and Support During External Audit

Performing **Internal Audit** to confirm readiness for certification.

Managing non-conformities and ensuring corrective actions.

Providing detailed audit reports with findings and recommendations.

Facilitating **management review meetings** with actionable insights.

Assisting before and during **external audit** to ensure a successful outcome.

CONTINUITY

Post-Certification Support

Conducting **60-day check-ins** to review ISMS effectiveness.

Monitoring frequency-based controls to maintain compliance.

Providing continuous compliance support and updates.

Assisting during **surveillance audits** to keep you audit-ready.

Offering ongoing guidance to adapt to evolving requirements.

TIMELINES FOR ISO 27001

ISO/IEC 27001:2022 – ISMS Implementation Support, Consultation and Internal Audit

Activity	Estimated Man Day(s)
Project Initiation & Planning	3
ISMS Scoping	5
Gap Assessment	14
Risk Assessment & Treatment	18
Implementation Support	
Internal Audit & Management Review	15
Certification Support	To be defined by the External Auditor
Post-Certification Support	Continuous Activity
Total	55

NOTE: These timelines mentioned above are as per statistical data. These timelines may vary depending on the scope and the availability of the relevant stakeholders.

ISO/IEC 27701:2019 (PIMS)

ISO/IEC 27701 is the privacy extension to ISO/IEC 27001 and 27002 that defines how to establish, implement, maintain, and continually improve a **Privacy Information Management System (PIMS)** for organizations acting as **PII contr**ollers and/or **processors**, aligning security and privacy to manage personal data responsibly and demonstrate accountability to laws like GDPR.

Clauses 5–8 add PIMS requirements to ISO 27001.

Separate guidance for PII controllers and processors.

Annexes map controls and legal references (e.g., GDPR).

Integrates via PDCA and Annex SL with the ISMS.

WHY IT MATTERS?

Revenue enablement

Demonstrable privacy compliance (PIMS) reduces enterprise due-diligence friction, accelerates procurement, and opens regulated-market deals.

Risk and loss reduction

Systematic identification and treatment of privacy risks lowers breach likelihood/impact, cutting incident, legal, and remediation costs

Regulatory defensibility

Mapped, auditable practices for PII handling strengthen posture for GDPR/CCPA and local laws, reducing enforcement and litigation risk

Operational efficiency

Integrates with ISO 27001 to avoid duplicate programs, standardize processes, clarify ownership, and streamline audits and evidence

Brand and investor trust

Independent certification or conformance signals accountable data stewardship, boosting reputation, retention, and valuation narratives.

ISO 27701 METHODOLOGY

HANDSHAKE

Project Initiation & Planning

Conducting a **Kick-off** to define **PIMS** objectives, stakeholders, methodology, and timelines.

Delivering PIMS **Awareness Sessions** to key stakeholders and the core privacy/ISMS team.

Management Commitment to allocate necessary resources for privacy governance.

Developing a detailed **Project Plan** and **Communication Matrix** for consistent updates.

Creating **PID** - scope, controller/processor, methodology, and milestones.

ASSESSMENT

PIMS Scoping

Define the **PIMS Scope**, PII categories, processing purposes, controller/processor roles, locations, systems, and third parties.

Develop a **Privacy Statement of Applicability (P-SoA)** based on current privacy context.

Gap Assessment

Perform a thorough **assessment of existing policies, processes, and controls**.

Compare the current state against ISO/IEC 27701 requirements.

Deliver a **Gap Analysis Report** along with an **Action Tracker** to provide a clear remediation roadmap.

Privacy Risk Assessment and Treatment

Develop a **Privacy Risk Management methodology**

Conduct **Privacy Risk Assessment**

Prepare a Risk Treatment Plan to mitigate identified risks.

Assist in selecting and implementing appropriate controls.

ASSURANCE

Implementation Support

Finalizing the **Privacy Statement of Applicability** for risk control.

Assisting in the development of **privacy policies, procedures, and supporting documents**.

Guiding the **deployment of controls** and maintaining **records of their implementation**.

Providing **ongoing consultations** during control implementation and monitoring.

Monitoring performance to ensure objectives are achieved.

Internal Audit and Support During External Audit

Performing **Internal Audit** to confirm readiness for certification.

Managing non-conformities and ensuring corrective actions.

Providing detailed audit reports with findings and recommendations.

Facilitating **management review meetings** with actionable insights.

Assisting before and during **external audit** to ensure a successful outcome.

CONTINUITY

Post-Certification Support

Conducting **60-day check-ins** to review PIMS effectiveness.

Monitoring frequency-based controls to maintain compliance.

Providing continuous compliance support and updates.

Assisting during **surveillance audits** to keep you audit-ready.

Offering ongoing guidance to adapt to evolving requirements.

TIMELINES FOR ISO 27701

ISO/IEC 27701:2019 – PIMS Implementation Support, Consultation and Internal Audit

Activity	Estimated Man Day(s)
Project Initiation & Planning	3
PIMS Scoping	5
Gap Assessment	14
Privacy Risk Assessment & Treatment	18
Implementation Support	
Internal Audit & Management Review	15
Certification Support	To be defined by the External Auditor
Post-Certification Support	Continuous Activity
Total	55

NOTE: These timelines mentioned above are as per statistical data. These timelines may vary depending on the scope and the availability of the relevant stakeholders.

PRICING STRUCTURE

HAACrypt follows a transparent and modular pricing model designed to fit organizations of all sizes. Pricing is categorized into One-Time, Annual, and Add-On components.

Pricing Categories

One-Time Fees

Gap assessment
Risk assessment
Documentation
Internal audit
Control implementation support
Final audit readiness
VAPT report + remediation support

Add-On Services

Additional VAPT re-testing
Adding new scopes
Employee security awareness program
Custom documentation
Third-party audit liaisoning
Cloud architecture security review
SIEM/SOC setup consulting

Resource Augmentation

- Dedicated Analysts for you

WHY CHOOSE HAACRYPT?

Addressing Critical Needs - HAACrypt was founded to meet the growing demand for robust cybersecurity solutions in our rapidly expanding digital landscape.

Expertise-Driven Protection - Our team brings hands-on experience in both defensive security and offensive penetration testing to comprehensively safeguard digital assets.

Proactive Digital Guardianship - We serve as dedicated protectors of your digital infrastructure, implementing layered security measures before threats emerge.

Trusted Cybersecurity Partner - Organizations rely on us as their vanguard against cyber threats, with 24/7 monitoring and rapid response capabilities.

Comprehensive Threat Defence - From risk assessment to incident response, we provide end-to-end protection to secure your digital ecosystem.

Compromise belongs in negotiations, not cybersecurity.

While others offer partial solutions, HAACrypt delivers absolute protection - because in digital warfare, almost secure means already breached.

For Sales Queries Reach us	**For Technical Queries Reach us**
✉ **sales@haacrypt.com**	✉ **technical@haacrypt.com**

www.haacrypt.com

in *haacrypt*