ControlCase

ISO 27001 CERTIFICATION CHECKLIST

ISO 27001 is part of the ISO/IEC 27000 family of standards. This certification is part of the central framework of ISO 27000 relating to information security management. It lists each It is focuses on information security and enabling organizations to manage security assets. Taking a risk-based approach, ISO 27001 provides the requirements for an Information Security Management System (ISMS).

An ISMS (Information Security Management System) is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

Common challenges to implementing ISO 27001 include: formalizing business agreements and vendor management processes, managing vulnerabilities, patches and code rewrites, 24x7x365 management and monitoring of logs, encryption of PII, and training and documenting PII policies and procedures.

☐ WHAT IS ISO 27002?

- ISO 27002 is a supplementary standard that focuses on the information security controls that organizations might choose to implement.
- It addresses information security controls only.
- ISO 27002 is not a certification

☐ WHAT IS ISO 27701, 27017 & ISO 27018?

ISO/IEC 27701 is a privacy extension and ISO/IEC 27002 and provides additional guidance for the protection of privacy, which is potentially affected by the collection and processing of personal information. ISO 27017 is the Code of Practice for ISO/IEC 27002 for cloud services. ISO 27018 is for protection of PII in public clouds acting as PII processors.

☐ COMPLIANCE vs CERTIFICATION?

- ISO 27001 COMPLIANT means the organization follows the ISO 27001 standard.
- ISO 27001 CERTIFIED means the organization's Information Security Management System has been certified in compliance with the standard by auditors known as Certification Bodies (such as ControlCase InfoSec).

☐ WHO NEEDS ICO CERTIFICATION?

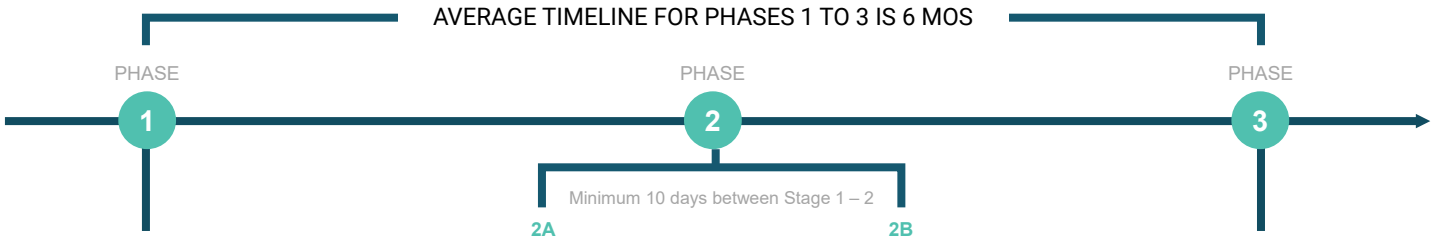
- Any organization that wishes or is required to formalize and improve business processes around information security, privacy and securing its information assets.
- The size/turnover of a business does not dictate the need for ISO 27001.

ISO 27001 COMPLIANCE CHECKLIST

Applicable domains to consider for ISO 27001 compliance:

- [ ] Information Security Policies
- [ ] Access Control
- [ ] Communications Security
- [ ] Business Continuity
- [ ] Organization of Information Security
- [ ] Cryptography
- [ ] SDLC
- [ ] Compliance
- [ ] Human Resource Security
- [ ] Physical & Environmental Security
- [ ] Supplier Relationship
- [ ] Asset Management
- [ ] Operations Security
- [ ] Incident Management

CONTROLCASE METHODOLOGY



ITERATIVE PRE-ASSESSMENT	ISO STAGE 1 AUDIT	ISO STAGE 2 AUDIT	DELIVERABLES
•Consolidated Pre-Assessment. •Using ControlCase Compliance Hub and Integrated Checklist. •Evaluation of policies and procedures. •Multiple rounds of assessment before Stage 1 & Stage 2 Audit.	Onsite/ Remote Average of 4 days	Onsite/ Remote Average of 6 days	ISO 27001 Certificate issued Extension Documents Released

ISO Certification is valid for 3 years.
Initial certification is performed in year 1and requires that surveillance audits are performed in year 2 and year 3.

ABOUT CONTROLCASE:

ControlCase is a CMMC RPO and a global provider of certification, cyber security, and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost-effective and comprehensive in both on-premise and cloud environments. ControlCase offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT and FedRAMP.

For more information email contact@controlcase.com