



## ISO 27001 COMPLIANCE ASSESSMENT

Information security is on top of mind for every organization starting at the highest levels. Organizations must ensure the confidentiality, integrity and availability (CIA) of their digital information to prevent any disruption in business operations. Growing information security risks from threat actors, both internal and external, add to the challenges of ever-changing regulatory requirements. Organizations must continuously monitor people, process, and technology to govern and manage security risks. Without appropriate governance and management frameworks, a data breach can have long-term impacts, including loss of revenue, loss of reputation, and potentially loss of employee, customer and shareholder trust.

ISO 27001 is an information security framework published by the International Organization of Standardization (ISO) to help organizations identify, analyze and address information security risks. An ISO 27001 compliance assessment helps organizations to review and understand appropriate policies and procedures needed to meet the requirements of the Information Security Management System (ISMS). It is the first step to ensure the CIA of a company's digital information and assure continuous business operations.

### ISO 27001 COMPLIANCE ASSESSMENT

SoftwareONE's ISO 27001 Compliance Assessment helps customers quickly evaluate their readiness and identify areas of non-compliance. SoftwareONE security consultants work closely with customers to understand their organizational structure, business processes and the scope of their ISO 27001 compliance. Key stakeholders responsible for ISO 27001 controls are interviewed to understand information security policies, procedures and practices. Based on the interviews, supporting documentation, and the effectiveness of existing controls, SoftwareONE will evaluate the compliance and risk posture with all ISO 27001 requirements and provide a detailed report with recommended next steps.

#### 1. Scope



Identify scope of ISO 27001 compliance, Business units

#### 2. Prepare



Interview and review to understand ISO 27001 policies, processes and controls

#### 3. Evaluate



Evaluate and analyze controls and summarize areas of compliance and non-compliance

#### 4. Report



Detailed executive report highlighting areas of non-compliance for each control and recommended next steps

## ISO 27001 CONTROL GROUPS AND CONTROLS

SoftwareONE's ISO 27001 Compliance Assessment helps customers understand their risk posture against 14 control groups and 114 distinct controls.

Control Group	# of Controls
Information security policies	2
Organization of information security	7
Human resource security	6
Asset management	10
Access Control	14
Cryptography	2
Physical and environmental security	15
Operations security	14
Communications security	7
System acquisition, development and maintenance	13
Supplier relationships	5
Information security incident management	7
Information security aspects of business continuity management	4
Compliance with requirements, i.e., policies, external requirements and regulations	8

## ISO 27001 COMPLIANCE REPORT

Each ISO 27001 Compliance Assessment customer receives a comprehensive report identifying areas of non-compliance. Customers can use the report to prioritize next steps towards ISO 27001 certification. SoftwareONE can also help plan and prioritize the strategy and roadmap to close identified gaps.

**ISO 27001 COMPLIANCE SUMMARY AGAINST CONTROLS**

