

# ISO 27001 ISMS THIRD PARTY CERTIFICATION SCHEME

## WHAT IS ISO 27001?

### Information Security Management System

An information security management system is a management system that focuses on driving and improving information security through identification, managing and minimizing information security threats. ISO 27001 requires organization to establish information security policy and objectives, determine process requirements, establish operational controls, tracking performance through monitoring and measurement, implement corrective action and conducting management review. In essence, it consists of the following clauses,

Clause 4	Information security management system
Clause 5	Management responsibility
Clause 6	Internal ISMS audits
Clause 7	Management review of the ISMS
Clause 8	ISMS improvement

### Compatibility

Based on the Deming PDCA (Plan-do-check-act) cycle, ISO 27001 has the same basic structure as other international management system standards such as ISO 9001 or ISO 14001. It offers a common framework for integrating different management systems.

### WHY IS IT RELEVANT?

ISO 27001 is a requirement standard which means organizations can be certified to it. It is generic in nature and is applicable to organizations of various sizes and background.

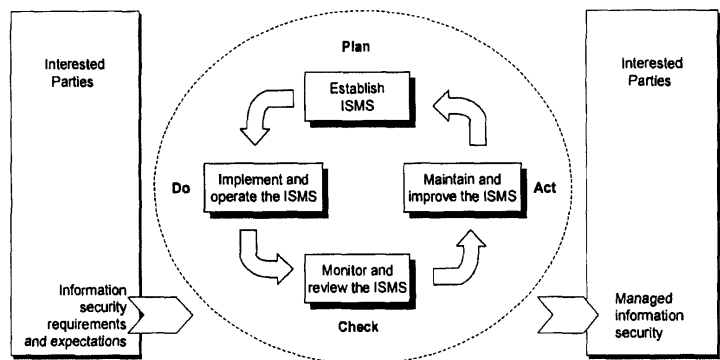


Figure 1 — PDCA model applied to ISMS processes

### Benefits

Apart from due diligence benefits and enhancement in creditability through third party certification, an effective ISO 27001 management system shall deliver the following inherent benefits,

- Sustainable and improving information security performance
- Platform for information security risk control and improvement
- Reduction in security breaches
- Improved staff motivation and information security consciousness
- Due diligence and demonstration of information security commitment



### HOW SHOULD I PROCEED?

In order to capitalize the full offer of ISO 27001, organizations shall acquire an accurate understanding of the requirements and the intent of the standard. Perform a gap analysis to determine the status of the organization compared to the certification requirements. From top management to front line staff, all levels of staff shall acquire an appropriate level of understanding of the standard. Top management commitment is a critical success factor. Work on a realistic plan and not the least, ensure a strong buy-in from everybody.

i-VAC Certification offers a full range of ISO 27001 improvement based training courses and certification services to address your needs. Contact us at [care@i-vac.com](mailto:care@i-vac.com).