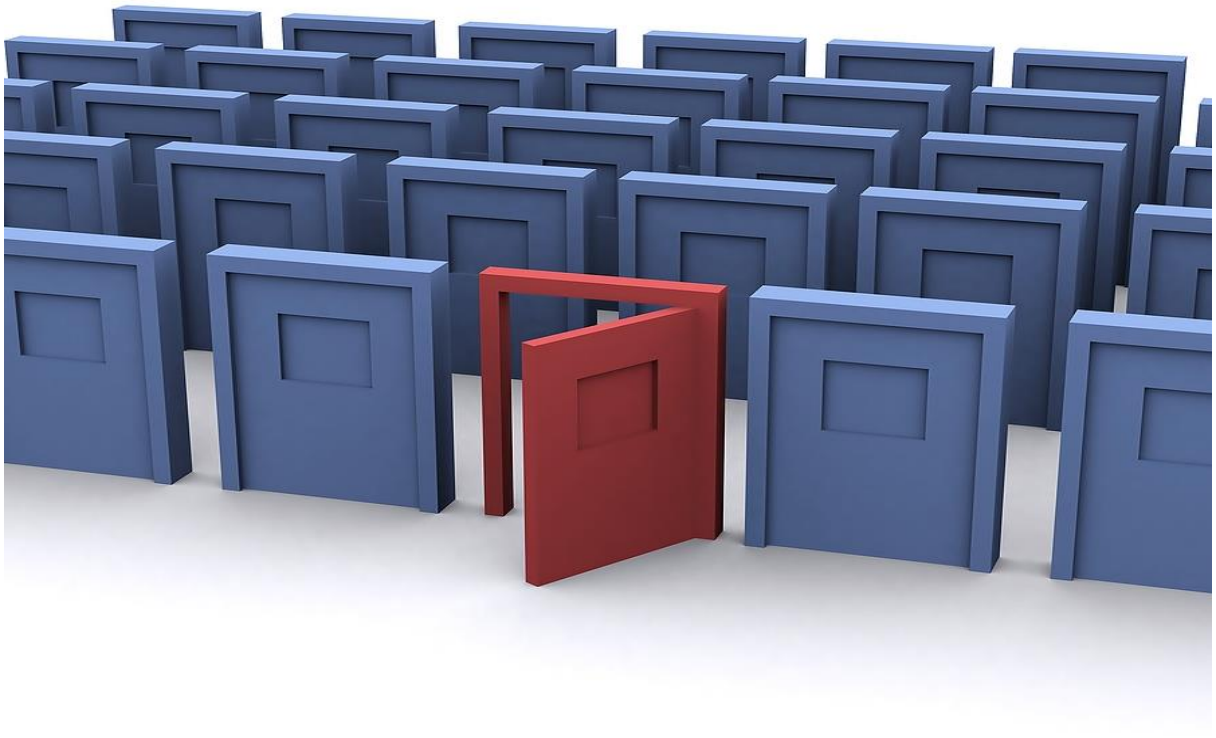
# Overview of ISO/IEC 27001:2013



## Introduction

The much awaited new standard ISO/IEC 27001:2013 has been released on 25th September. This is the first change that has been made to the standard in 8 years. The new standard is more focus and aligned to the organization objectives.

Since we understand that information security management system is an integral part of the organization's processes and overall management structure, we have put together this particular document for the better overview on the new standard ISO/IEC 27001:2013 released.

This document gives you an overview of the structure of the new standard ISO/IEC 27001:2013. The comparison of the standard structure between the new standard with the old standard will give a better understanding on the changes to the new standard. The document can be used and serves as a basic guideline for the transition from the older standard ISO/IEC 27001:2005 to the newer standard ISO/IEC 27001:2013.

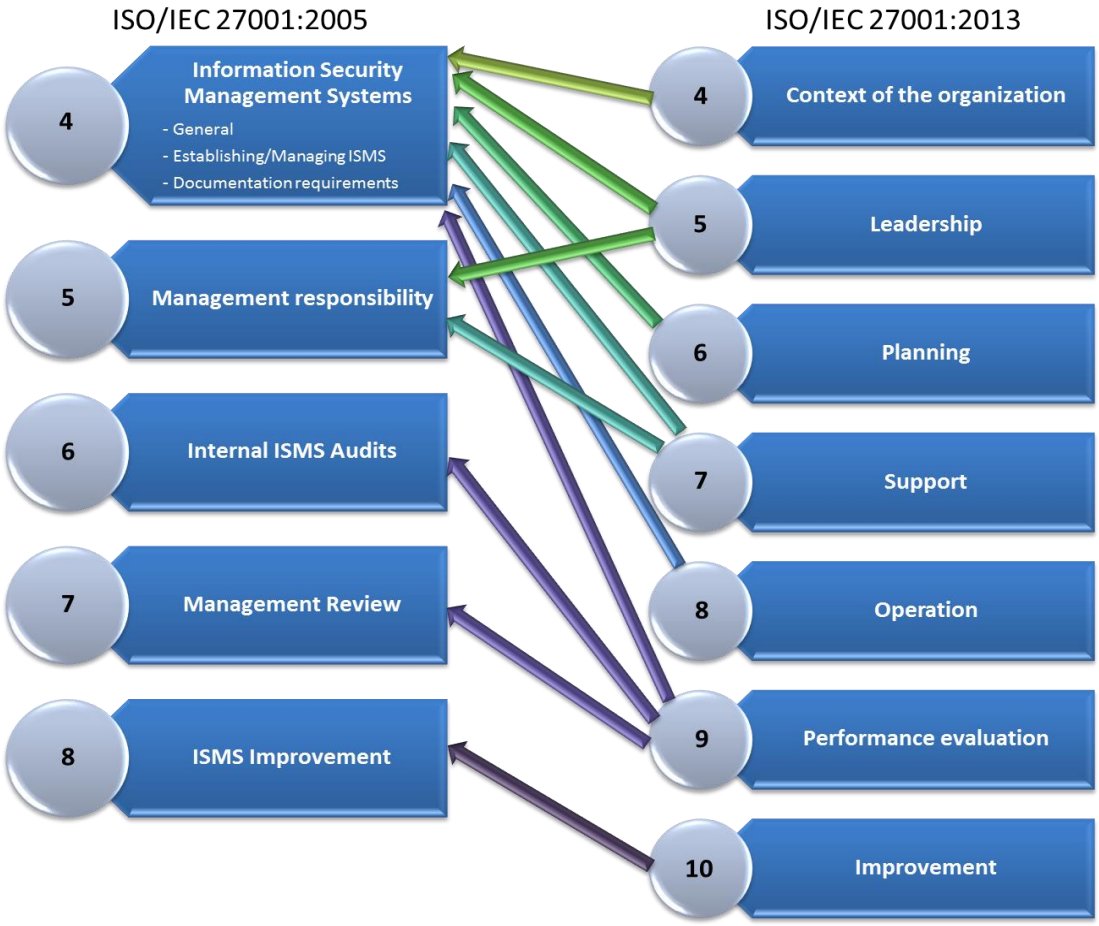
## Comparison of Structure between ISO/IEC 27001:2005 & ISO/IEC 27001:2013

The new standard has been aligned with other management system (MS) standards (such ISO 22301 and up-coming ISO 9001, etc.). Also going forward the new structure will be followed for all ISO standards. This standard has ten clauses mentioned in it: Introduction, Normative References, Terms and Definitions, Context of the Organisation, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement. We will highlight the main changes that have taken place in each section.

Below figures give an overview of the clauses in the old and new standard.


## Comparison of Clauses between ISO/IEC 27001:2005 & ISO/IEC 27001:2013

The below figure gives an overview of how the clauses are arranged in the new standard as compared to the clauses arranged in the old standard. The clauses in the new standard have been detailed out as compared to the old standard.




Some of the changes which need to be highlighted which needs to be considered:

- The Plan-Do-Check-Act (PDCA) model has been removed, however continual improvement is still there and the organisation can select a process model as per the organisation needs.
- The scope of the new standard is also very similar to the old version, and states that all of the requirements specified in Clauses 4 to 10 must be met without exception in order to claim conformance with the standard.
- Normative reference to ISO/IEC 27002 has been removed and ISO/IEC 27000 is the only normative reference.

- All of the definitions that were in the 2005 version have been removed and those that are still relevant have been relocated in ISO/IEC 27000. This has been done to help ensure consistency of terms and definitions across all the standards in the 27000 series of standards.

- The general requirement, given in 4.1 of the older standard, which was to implement the ISMS, the same is found in 4.4 of the new standard

- The requirements to determine the scope of the ISMS has two new sets of requirements added: "Understanding the organization and its context" and "Understanding the needs and expectations of interested parties".

- The requirements for providing a framework for setting objectives are more detailed in the new standard and the objectives are to be set at "relevant functions and levels".

- The liberty of choosing the risk assessment methodology has been given to the organisation and the organisation is no longer required to identify assets, threats and vulnerabilities in order to identify risk. The organisation can choose any process to identify risk.

- The SOA requirements are largely unchanged from the old standard and the new standard makes it clear that you do not "select" controls from Annex A. Instead you "determine" the controls you need as part of risk treatment and compare those controls with those in Annex A to ensure that no important control has been overlooked and provide a justification for inclusion or exclusion.

- The word preventive action has been removed and the new standard considers correction & corrective action only.

- The documentation requirements remain unchanged and can be found in 7.5 of the new standard. The new standard refers to "documented information" rather than "documentation and records".

- The requirements for internal audit, providing resources and management review remain the same as per the old standard. A more detailed requirements for measurement of effectiveness is mentioned in the new standard

- Continual improvement remains the same as mentioned in the old standard.


Wings2i
Enabling Ideas and Innovations
Wings2i IT Solutions Pvt Ltd.
3rd Floor, BOSS SQUARE,
No:80, 1st Cross, 2nd Main,
BTM Layout 2nd Stage,
Bangalore - 560 076
info@wings2i.com
+91-80-65371700/1