www.pwc.com.au

Information Security Management Systems

ISO 27001

July 2017

pwc

About the presenters

Jeremy Hibbert

Jeremy is a Senior Manager in PwC's Risk Assurance team, and the Queensland Digital Trust leader, responsible for the delivery of Information Security, Provacy, IT internal audit, IT project and risk assurance reviews.

Jeremy has in depth knowledge of Information Security across a range of industries, both public and private, and has worked for organisations in Australia, UAE, Qatar, and South Africa.

Tom Barham

Tom is a Manager in PwC's Risk Assurance team, and responsible for the delivery of training across Australia and New Zealand, in the areas of Quality, Environmental, OH&S, Information Security, Business Continuity and Risk Management, aligned to relevant ISO Standards.

As PwC's resident ISO expert, Tom has experience in applying and auditing the requirements of standards across both private and government entities.

ISO 27000 Series

27001	27002	27003	27004
Information security management systems - Requirements	Code of practice for information security management	ISMS Implementation guidance	Information security management measurement

27005	27006	27007	27799
Information security risk management	Requirements for bodies providing audits and certification of ISMS	Guidelines for information security management systems auditing	Information security management in health using ISO 27002

ISO 27001/27002

ISO 27001

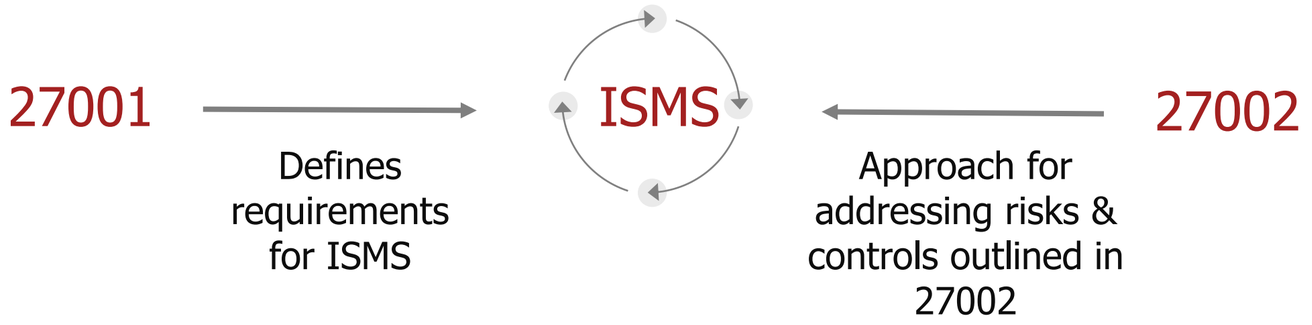
Management standard providing requirements for an information security management system (ISMS). Certification to the standard is possible, but not mandatory.

ISO 27002

Information security standard specifying best practice recommendations across several domains. The standard outlines hundreds of potential controls and control mechanisms.

ISMS

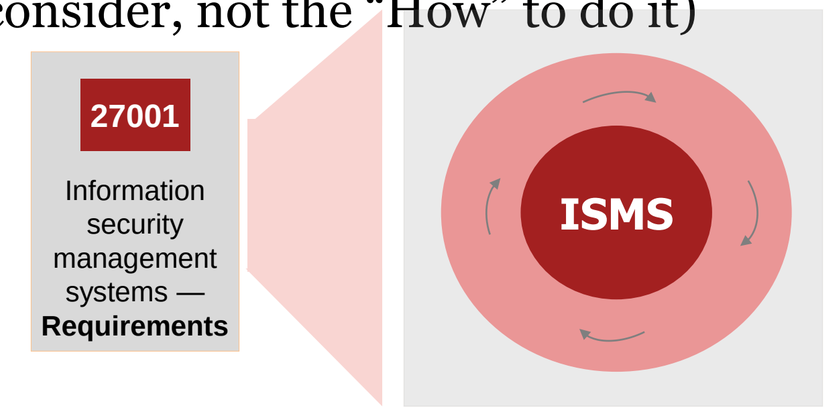
Systematic approach to managing information assets so that the assets remains secure. It includes people, processes, and IT systems by applying a risk management process.



ISO 27001: Requirements for an ISMS

What it IS NOT

- Just IT
- A mandate for all the controls in ISO 27002 (certification based on statement of applicability)
- Prescriptive in the procedures to follow to ensure compliance (that is, it tells you “What” to consider, not the “How” to do it)



One of the primary components of 27001 is providing a outline for developing an ISMS

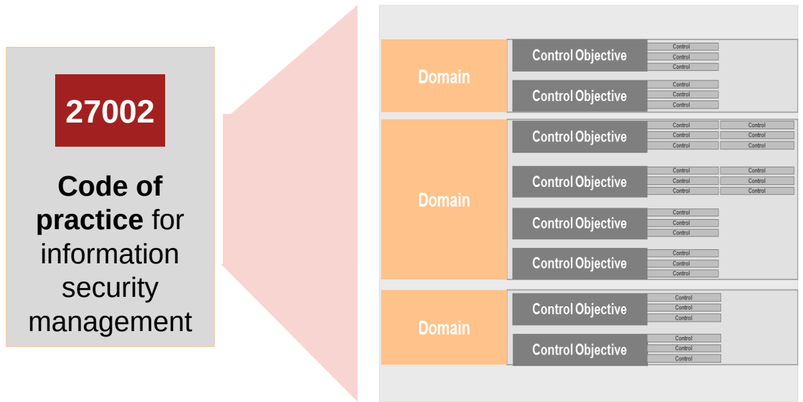
What it IS

- A business risk management tool
- A standard specification for ISMS, which is a system that senior management can use to control information security
- The means by which an organization is certified to a quality system of implementing best practice security controls (i.e., ISO 27002)
- Anticipated to be the de facto international security certification

ISO 27002: Code of Practice for ISMS

What it IS NOT

- A certification standard!
- An industry or technical standard
- A detailed description of security processes
- Product or technology oriented



Recommendations across several domains, which outlines controls and control objectives.

What it IS

- An internationally recognized Information Security Management Standard published by ISO
- High level, broad in scope, and conceptual in nature
- Relevant to today's security management and was most recently updated in October 2013
- Regarded as international best practice security standard in regards to protecting information assets

Benefits of the ISO 27001/2 Framework

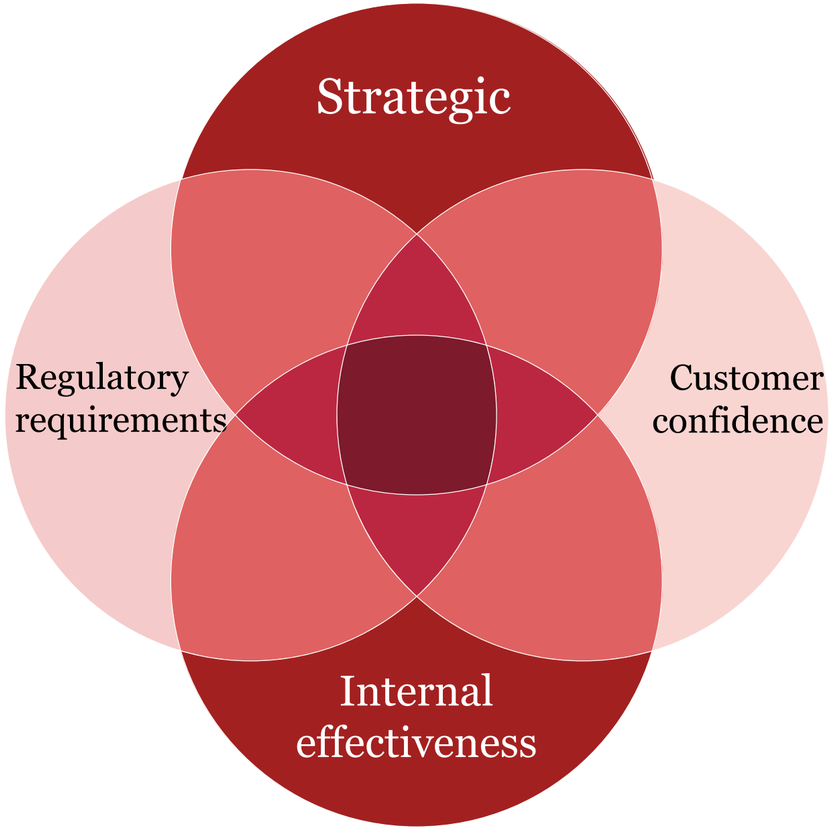
Reasons for implementing the ISO 27001 ISMS and associated ISO 27002 controls include:

Strategic – Better manage security within the broader external risk environment

Customer Confidence – Show customers that their data will be reasonably protected by the organization, or to differentiate the organization from competitors

Regulatory Requirements – Introduce a framework to integrate and manage widely varying regulations

Internal Effectiveness – Manage information effectively as a good practice



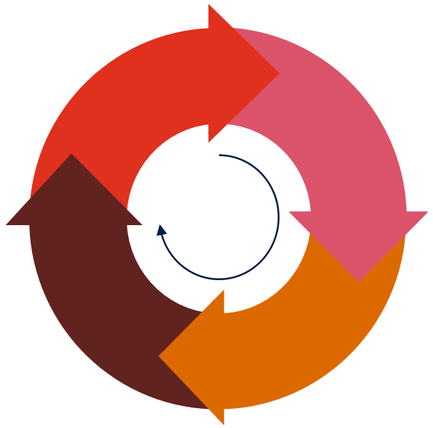
Source: Implementing Information Security based on ISO 27001/ISO 17799

ISO 27001 and ISO 27002

ISO/IEC 27001:2013

14 Domains | **114** Controls

Continual Improvement Process



ISO/IEC 27002:2013

Domains

5 Information security policies

6 Organization of information security

7 Human resource security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security

13 Communications security

14 Systems acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

17 Information security aspects of business continuity management

18 Compliance

Statement of Applicability

Defines which of the suggested controls will be applied and for those that are applicable, the way the controls will be applied

A Statement of Applicability is required for certification and provides rationale on the exclusion / inclusion of controls for the organization

www.pwc.com.au

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au

WL 127040178