Preparing yourself for ISO/IEC 27001 2013

2013 a Vintage Year for Security

Prof. Edward (Ted) Humphreys

(edwardj7@msn.com)

[Chair of the ISO/IEC and UK BSI Group responsible for the family of ISMS standards, ISO ISMS Press Officer]

Vienna, 19th September 2013

Agenda

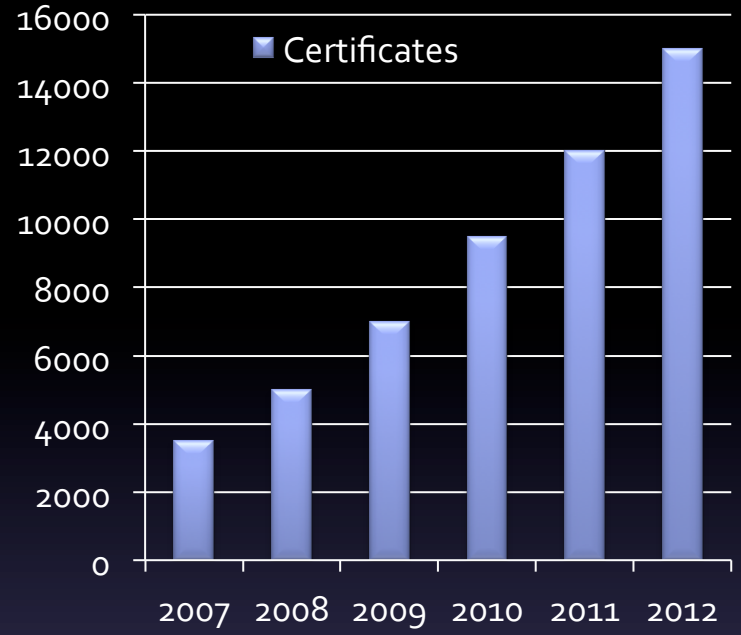
- Essence of information security management
- Why change (feedback, experiences and the NG MSS)?
- Overview of revised version
- Timeline and transition old to new
- Help and support

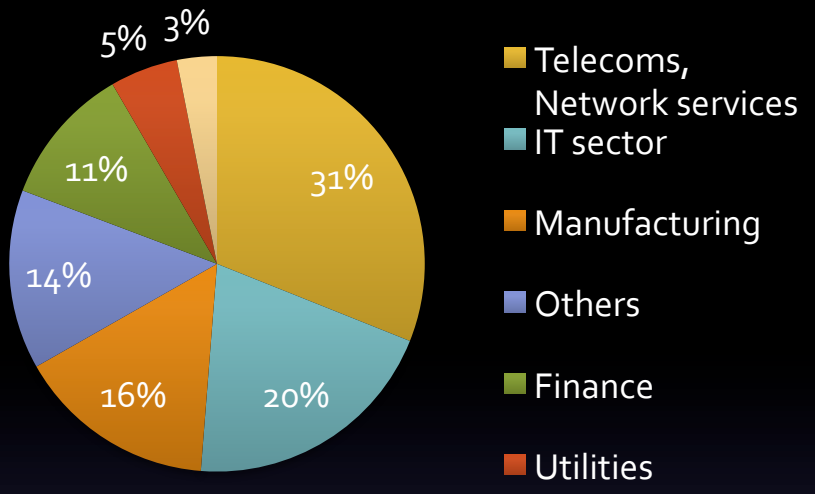
ISO/IEC 27001 ISMS

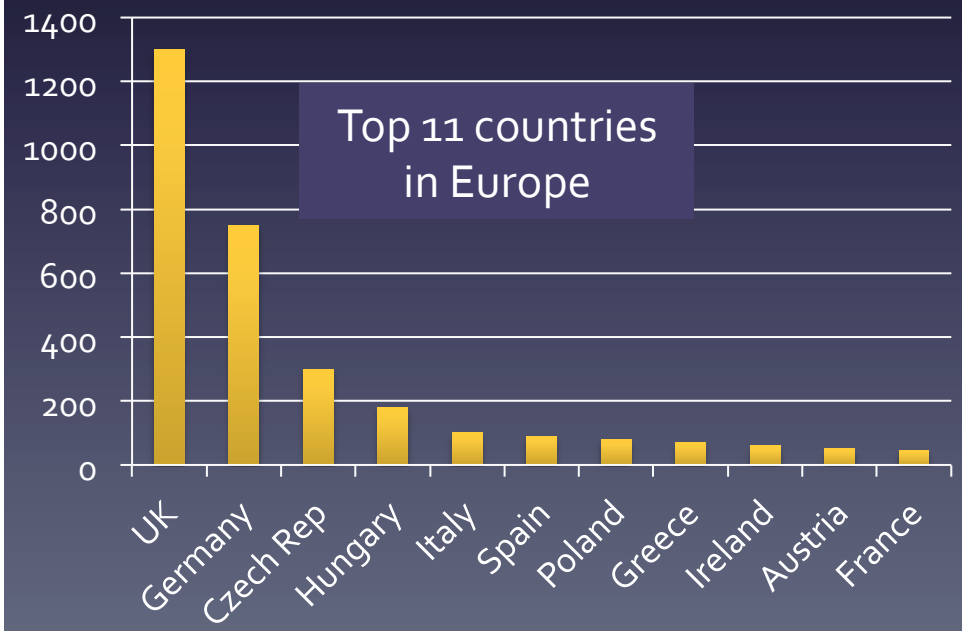
Since its launch in 2005, ISO/IEC 27001 has meet with resounding success around the world and across all market sectors with the number of third party certifications in 2013 now beyond the 16,000+ mark, covering over 100 countries.

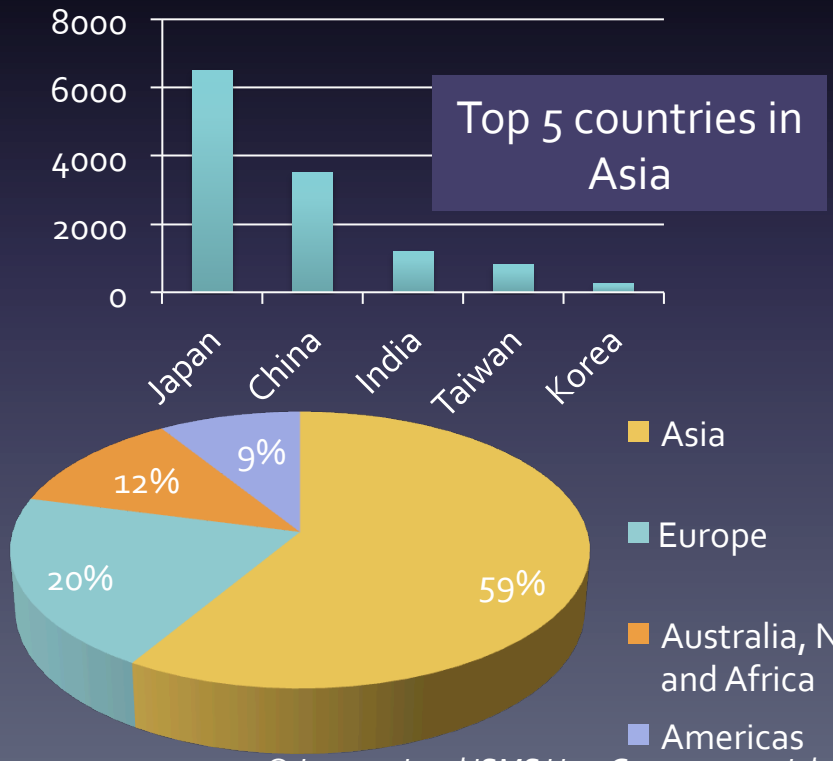
October this year will see the publication of the revised version of the internationally acclaimed standard for Information Security Management (ISO/IEC 27001). This revised version of ISO/IEC 27001 take us forward to a new era the Next Generation of management system standards (MSS).

ISO/IEC 27001 ISMS Certifications

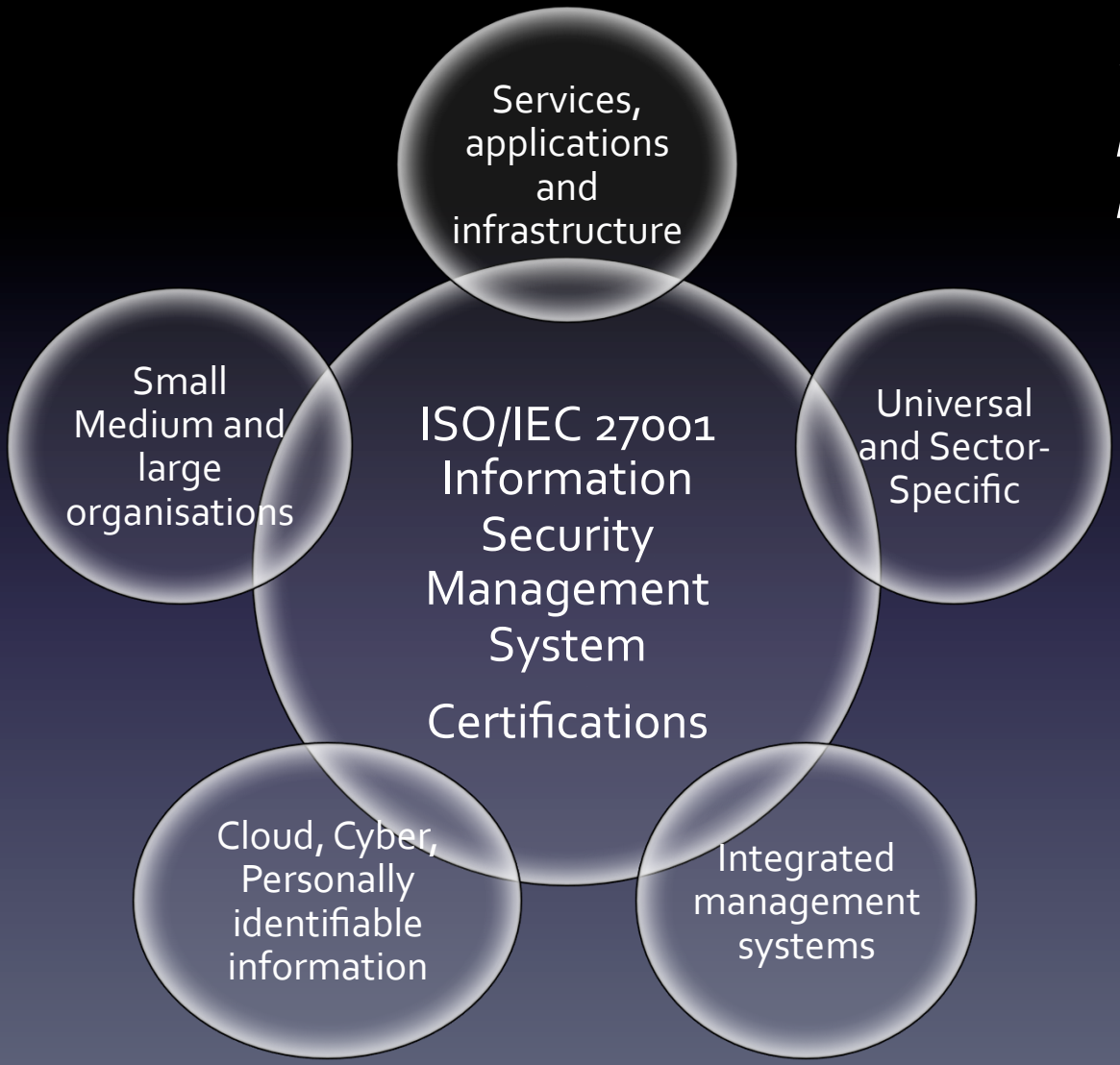








ISO/IEC 27001 - the global international certification standard



The biggest selling of all information security management standard

The international Common Language for information security management as spoken across the business world (including government use)

Essence of information security

- Confidentiality

  Information whether in storage, being processed or communicated, should be protected to ensure it is not leaked, disclosed or seen by those that are authorized to have access to and use of the information.

- Integrity

  Information whether in storage, being processed or communicated is accurate and complete, that it is correctly processed, and that it has not been modified in any unauthorized way.

- Availability
- Sensitive, critical and personally identifiable information

Essence of information security

- Sensitive information (examples)
  - *Trade secrets, company research,*
  - *Future commercial plans, new product plans*
  - *Customer and supplier information*
  - *Sales and marketing plans*
  - *Financial records*
- Critical information (examples)
  - *Financial records*
  - *Medical information*
  - *Manufacture and design information*
  - *Safety related information (e.g. industrial control systems)*

Essence of information security

- Personally identifiable information (PII)
  - any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

    NOTE To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person

    (ISO/IEC 29100 – Privacy Framework)
  - PII Principle – a natural person to whom the personally identifiable information (PII) relates

What is ISO/IEC 27001?

- **27001** is an **Information security management system** (ISMS) standard (a GRC standard)
  - Protecting the confidentiality, integrity, availability of assets
  - Protecting PII
  - Minimising information security risks
  - Maximising business opportunities and investments
  - Ensuring business continuity of systems and processes

What is ISO/IEC 27001?

- It is a *risk based management tool* for managing information security risks which encompasses the business process, critical system elements and critical system boundaries
- It involves a *continuous improvement programme* to maintain the effectiveness of an organisation's information security management to meet changing risk and threat environments

What is ISO/IEC 27001?

- Finally - 27001 provides the framework for 3rd-party audits and certification of an organisation's ISMS
  - Demonstrating you are managing information security risks
  - Providing 'fit-for-purpose' and 'duty of care' confidence and assurance to customers and stakeholders
  - Verifying your governance and risk management programme is effective

Revision of ISO Standards

- *Every 5-years ISO standards comes up for review*
  - *Confirmation, Revise, Withdraw*
- *Why it was decided to revise ISO/IEC 27001?*
  - *Based on a Justification Study and consultation with users in 2008/2009 is was decided to revise*
    - *To ensure 27001 remains current and useful*
    - *To take account feedback from interested parties on the use and effectiveness of ISMS in the market and on certification experiences*
    - *To be aligned with the Next Generation of Management System Standards*

Next Generation of Management System Standards (NG-MSS)

The NG-MSS is a trend towards harmonised, integrated and consistent management systems.

All ISO management system standards will in the future be aligned according to an agreed high level structure, identical core text and common terms and core definitions (ISO/IEC Directives Part 1, Annex SL, Appendix 3).

This will increase the value of such standards and be particularly useful for organisations that operate across multiple management system platforms.

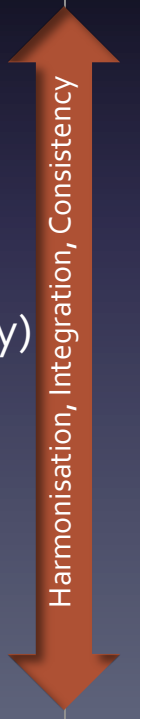
Next Generation of Management System Standards

- Trend towards harmonised, integrated and consistent management systems offering
  - Greater trade opportunities
  - Economies of scale through integrated scopes, policies and procedures
  - Maximising business investments and minimising business costs through integrated management systems
  - Improved operations through integrated performance evaluations

Next Generation of Management System Standards

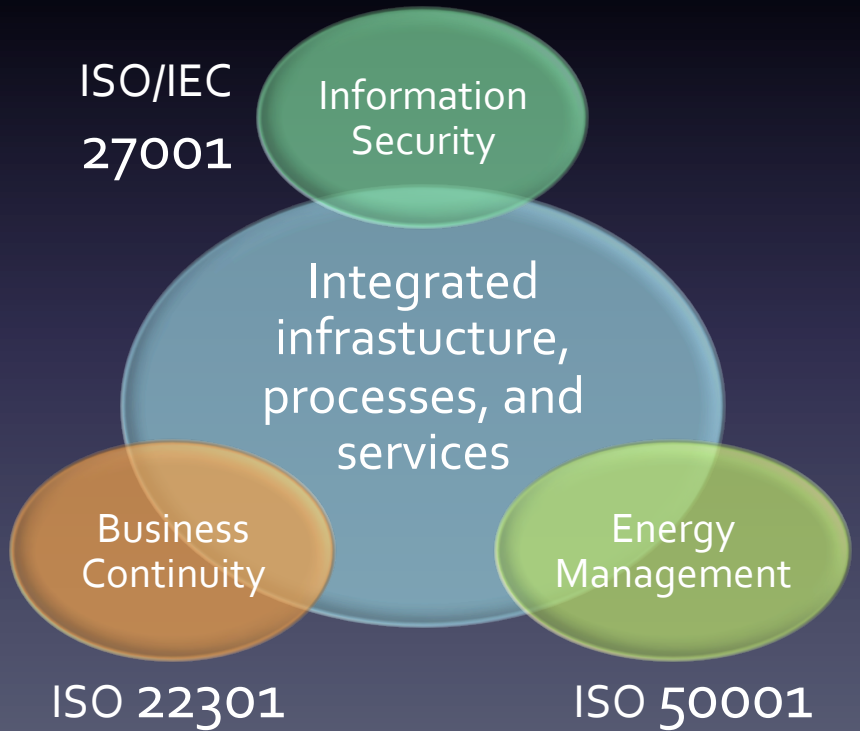
- Better management of risks through integrated platforms and infrastructure
  - Function: Quality, environment, information security, business continuity …
  - Sector: Telecoms, Finance, IT services, Energy, Manufacturing, Transportation, Healthcare …

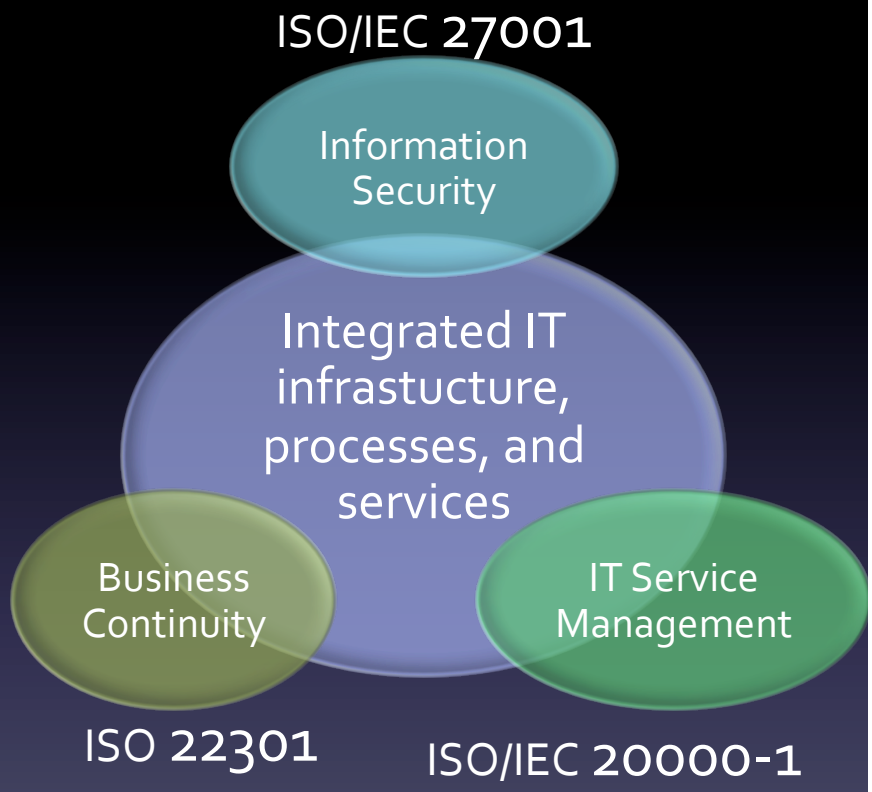
- ISO 9001 (quality)
- ISO 14001 (environment)
- ISO/IEC 20000-1 (IT service management)
- ISO 22301 (business continuity)
- ISO/IEC 27001 (information security management)
- ISO 50001 (energy management)
- … etc



Example of Integrated Management System Environments

For the Oil and Gas Industry
possibly also integrated with ISO 29001
(oil and gas management system)





IT Services Sector - Some operational benefits: integrated – risk management and impact assessment, incident handling, asset management …

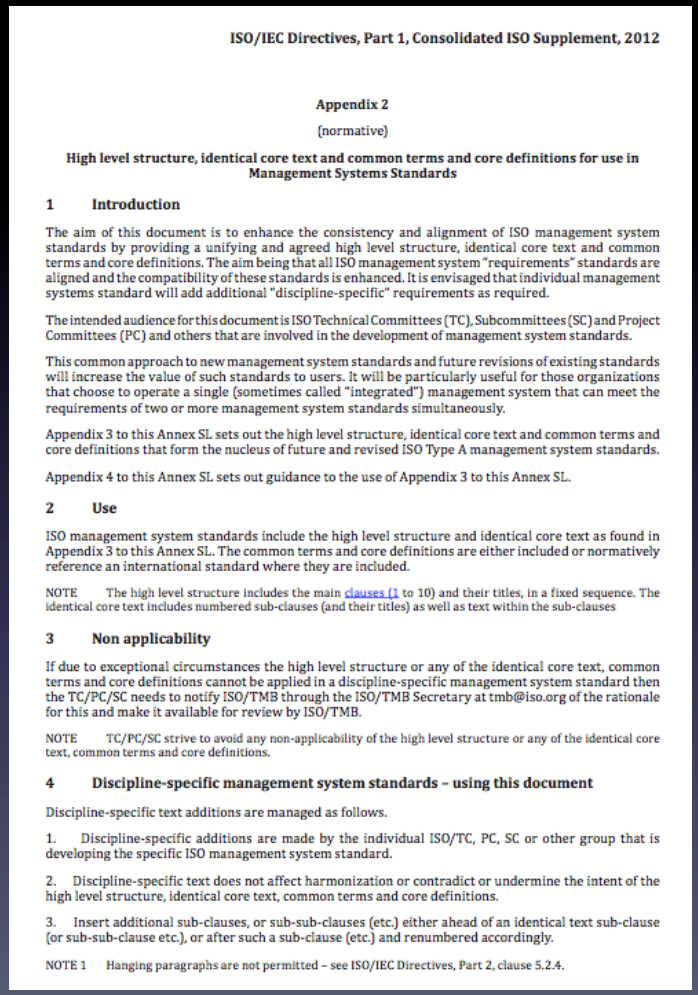
27001 2013 Edition
Greater Emphasis on Business Focus

- Adopting an ISMS is a strategic business decision

  establishing, implementing, maintaining and continually improving an ISMS to achieve effective information security
- Context, needs and expectations (4)
  - Understanding the organization and its context (4.1)
  - Understanding the needs and expectations of interested parties (4.2)
- Leadership (5)
- Risk management (6 and 8), and Performance evaluation (9)
- Continual improvement (10)

Overview of the Revised 27001

- *ISO/IEC 27001 has been re-structured and aligned with ISO/ IEC Directives Part 1, Annex SL, Appendix 2 and 3*
  - High-level structure
  - Identical core text
  - Common terms and core definitions



ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2012

Appendix 2

(normative)

High level structure, identical core text and common terms and core definitions for use in Management Systems Standards

1 Introduction

The aim of this document is to enhance the consistency and alignment of ISO management system standards by providing a unifying and agreed high level structure, identical core text and common terms and core definitions. The aim being that all ISO management system "requirements" standards are aligned and the compatibility of these standards is enhanced. It is envisaged that individual management systems standard will add additional "discipline-specific" requirements as required.

The intended audience for this document is ISO Technical Committees (TC), Subcommittees (SC) and Project Committees (PC) and others that are involved in the development of management system standards.

This common approach to new management system standards and future revisions of existing standards will increase the value of such standards to users. It will be particularly useful for those organizations that choose to operate a single (sometimes called "integrated") management system that can meet the requirements of two or more management system standards simultaneously.

Appendix 3 to this Annex SL sets out the high level structure, identical core text and common terms and core definitions that form the nucleus of future and revised ISO Type A management system standards.

Appendix 4 to this Annex SL sets out guidance to the use of Appendix 3 to this Annex SL.

2 Use

ISO management system standards include the high level structure and identical core text as found in Appendix 3 to this Annex SL. The common terms and core definitions are either included or normatively reference an international standard where they are included.

NOTE The high level structure includes the main clauses (1 to 10) and their titles, in a fixed sequence. The identical core text includes numbered sub-clauses (and their titles) as well as text within the sub-clauses

3 Non applicability

If due to exceptional circumstances the high level structure or any of the identical core text, common terms and core definitions cannot be applied in a discipline-specific management system standard then the TC/PC/SC needs to notify ISO/TMB through the ISO/TMB Secretary at tmb@iso.org of the rationale for this and make it available for review by ISO/TMB.

NOTE TC/PC/SC strive to avoid any non-applicability of the high level structure or any of the identical core text, common terms and core definitions.

4 Discipline-specific management system standards – using this document

Discipline-specific text additions are managed as follows.

1. Discipline-specific additions are made by the individual ISO/TC, PC, SC or other group that is developing the specific ISO management system standard.

2. Discipline-specific text does not affect harmonization or contradict or undermine the intent of the high level structure, identical core text, common terms and core definitions.

3. Insert additional sub-clauses, or sub-sub-clauses (etc.) either ahead of an identical text sub-clause (or sub-sub-clause etc.), or after such a sub-clause (etc.) and renumbered accordingly.

NOTE 1 Hanging paragraphs are not permitted – see ISO/IEC Directives, Part 2, clause 5.2.4.

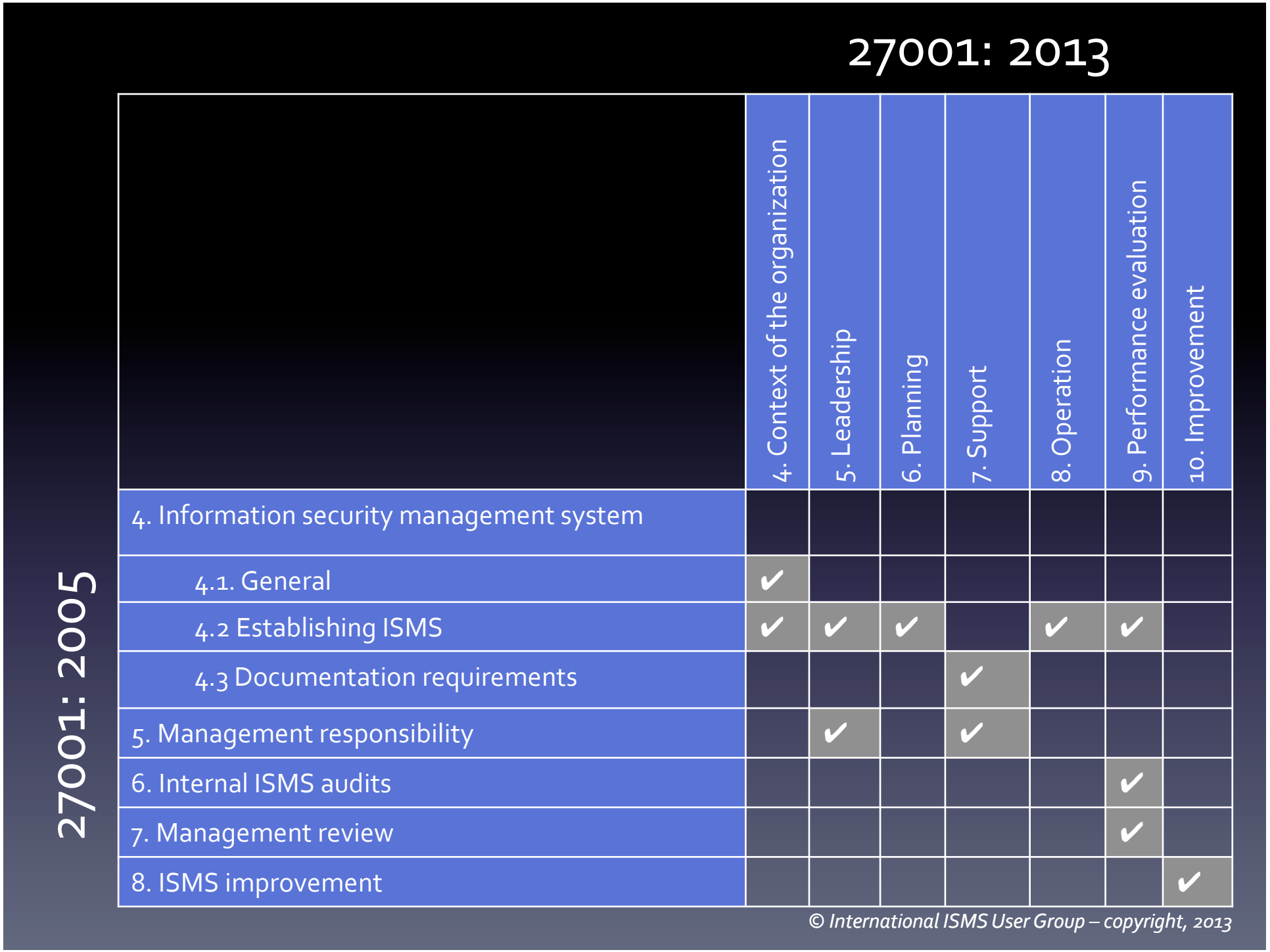
Alignment with ISO/IEC Directives Part 1, Annex SL, Appendix 2 and 3

27001: 2005 (old)

- Introduction
- Scope
- Normative references
- Terms and definitions
- Information security management system
- Management responsibility
- Internal ISMS audits
- Management review
- ISMS improvement
- Annex A (normative) Control objectives and controls
- Annex B (informative) OECD principles and this International Standard
- Annex C (informative) Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

27001: 2013 (new)

- Introduction
- Scope
- Normative references
- Terms and definitions
- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement
- Annex A (normative) Reference control objectives and controls


27001: 2013
27001: 2005
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement
4. Information security management system
4.1. General
4.2 Establishing ISMS
4.3 Documentation requirements
5. Management responsibility
6. Internal ISMS audits
7. Management review
8. ISMS improvement
✔
© International ISMS User Group – copyright, 2013

27001: 2005

- Information security management system
- Management responsibility
- Internal ISMS audits
- Management review
- ISMS improvement

ISMS specific text

27001: 2013

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Identical core text (Annex SL)

ISMS specific text (based on ISO/IEC 27001:2005)

27001: 2013

Common Chapter Heading

Identical core text (Annex SL)

ISMS specific text (based on ISO/IEC 27001:2005)

Example of Generic Text (Annex SL)

6 Planning

6.1 Actions to address risks and opportunities

When planning for the XXX management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to

— assure the XXX management system can achieve its intended outcome(s)

— prevent, or reduce, undesired effects

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities, and

b) how to

— integrate and implement the actions into its XXX management system processes

— evaluate the effectiveness of these actions.

Annex SL (Generic Text)

27001: 2013 text

6 Planning

6.1 Actions to address risks and opportunities

When planning for the XXX management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to

— assure the XXX management system can achieve its intended outcome(s)

— prevent, or reduce, undesired effects

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities, and

b) how to

— integrate and implement the actions into its XXX management system processes

— evaluate the effectiveness of these actions.

Identical core text

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities, and

e) how to

1) integrate and implement these actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

ISMS specific text

6.1.2 Information security risk assessment

The organization shall define an information security risk assessment process that:

a) establishes and maintains information security risk criteria, including the risk acceptance criteria;

b) determines the criteria for performing information security risk assessments; and

c) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

The organization shall:

d) Identify the information security risks.

1) Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS.

2) Identify the risk owners.

e) Analyse the information security risks.

1) Assess the potential consequences that would result if the risks identified in 6.1.1 e) 1) were to materialize.

2) Assess the realistic likelihood of the occurrence of the risks identified in 6.1.1 e) 1).

27001: 2013 text

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities, and

e) how to

1) integrate and implement these actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define an information security risk assessment process that:

a) establishes and maintains information security risk criteria, including the risk acceptance criteria;

b) determines the criteria for performing information security risk assessments; and

c) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

The organization shall:

d) Identify the information security risks.

1) Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS.

2) Identify the risk owners.

e) Analyse the information security risks.

1) Assess the potential consequences that would result if the risks identified in 6.1.1 e) 1) were to materialize.

2) Assess the realistic likelihood of the occurrence of the risks identified in 6.1.1 e) 1).

ISMS specific text

3) Determine the levels of risk.

f) Evaluate the information security risks.

1) Compare the analysed risks with the risk criteria established in 6.1.2 a) and establish priorities for treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE: Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1: Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no important control options are overlooked

NOTE 2: Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be needed.

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 a), b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls in Annex A;

e) formulate an information security risk treatment plan;

f) obtain risk owner's approval of the information security risk treatment plan and the acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE: The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000.

27001: 2013 text

Example of core text (Annex SL) only no ISMS specific text

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE: Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected.

Overview of the Revised 27001

Common terms and core definitions

Appendix 3

(normative)

High level structure, identical core text, common terms and core definitions

NOTE In the Identical text proposals, XXX = an MSS discipline specific qualifier (e.g. energy, road traffic safety, IT security, food safety, societal security, environment, quality) that needs to be inserted. Blue italicized text is given as advisory notes to standards drafters.

Introduction

NOTE Specific to the discipline.

1 Scope

NOTE Specific to the discipline.

2 Normative references

NOTE Clause Title shall be used. Specific to the discipline.

3 Terms and definition

NOTE Clause Title shall be used. Terms and definitions may either be within the standard or in a separate document. To reference Common terms and Core definitions + discipline specific ones.

For the purposes of this document, the following terms and definitions apply.

NOTE 1 The following terms and definitions constitute an integral part of the "common text" for management systems standards. Additional terms and definitions may be added as needed. Notes may be added or modified to serve the purpose of each standard.

NOTE 2 Bold type in a definition indicates a cross-reference to another term defined in this clause, and the number reference for the term is given in parentheses.

NOTE 3 Where the text "XXX" appears throughout this clause, the appropriate reference should be inserted depending on the context in which these terms and definitions are being applied. For example: "an XXX objective" could be substituted as "an information security objective".

3.01
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its **objectives** (3.08)

NOTE 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.02
interested party (preferred term)
stakeholder (admitted term)
person or **organization** (3.01) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.03
requirement
need or expectation that is stated, generally implied or obligatory

NOTE 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

NOTE 2 to entry: A specified requirement is one that is stated, for example in documented information.

3.04
management system
set of interrelated or interacting elements of an **organization** (3.01) to establish **policies** (3.07) and **objectives** (3.08) and **processes** (3.12) to achieve those objectives

NOTE 1 to entry: A management system can address a single discipline or several disciplines.

NOTE 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

NOTE 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.05
top management
person or group of people who directs and controls an **organization** (3.01) at the highest level

NOTE 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 to entry: If the scope of the **management system** (3.04) covers only part of an organization then top management refers to those who direct and control that part of the organization.

3.06
effectiveness
extent to which planned activities are realized and planned results achieved

3.07
policy
intentions and direction of an **organization** (3.01) as formally expressed by its **top management** (3.05)

3.08
objective
result to be achieved

NOTE 1 to entry: An objective can be strategic, tactical, or operational.

NOTE 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and **process** (3.12)).

NOTE 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an XXX objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 to entry: In the context of XXX management systems XXX objectives are set by the organization, consistent with the XXX policy, to achieve specific results.

3.09
risk
effect of uncertainty

NOTE 1 to entry: An effect is a deviation from the expected — positive or negative.

NOTE 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 3 to entry: Risk is often characterized by reference to potential **events** (ISO Guide 73, 3.5.1.3) and **consequences** (ISO Guide 73, 3.6.1.3), or a combination of these.

NOTE 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (ISO Guide 73, 3.6.1.1) of occurrence.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an **organization** (3.01) and the medium on which it is contained

NOTE 1 to entry: Documented information can be in any format and media and from any source.

NOTE 2 to entry: Documented information can refer to

— the **management system** (3.04), including related **processes** (3.12);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.12
process
set of interrelated or interacting activities which transforms inputs into outputs

3.13
performance
measurable result

NOTE 1 to entry: Performance can relate either to quantitative or qualitative findings.

NOTE 2 to entry: Performance can relate to the management of activities, **processes** (3.12), products (including services), systems or **organizations** (3.01).

3.14
outsource (verb)
make an arrangement where an external **organization** (3.01) performs part of an organization's function or **process** (3.12)

NOTE 1 to entry: An external organization is outside the scope of the **management system** (3.04), although the outsourced function or process is within the scope.

3.15
monitoring
determining the status of a system, a **process** (3.12) or an activity

NOTE 1 to entry: To determine the status there may be a need to check, supervise or critically observe.

3.16
measurement
process (3.12) to determine a value

3.17
audit
systematic, independent and documented **process** (3.12) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.18
conformity
fulfilment of a **requirement** (3.03)

3.19
nonconformity
non-fulfilment of a **requirement** (3.03)

3.20
correction
action to eliminate a detected **nonconformity** (3.19)

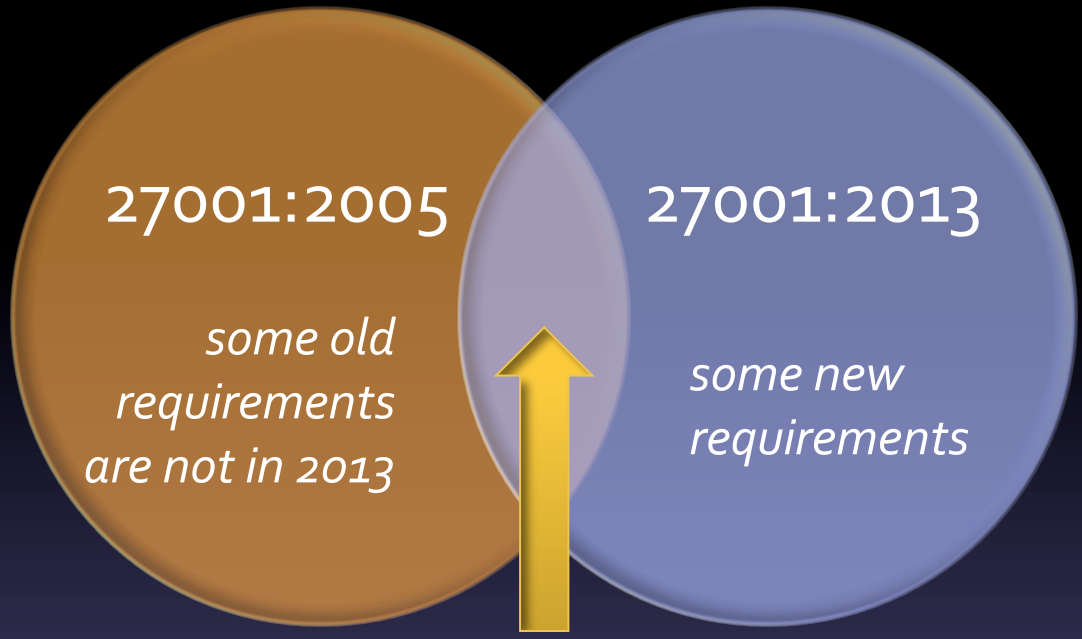
3.21
corrective action
action to eliminate the cause of a **nonconformity** (3.19) and to prevent recurrence

3.22
continual improvement
recurring activity to enhance **performance** (3.13)

Overview of the Revised 27001

- *The ISO/IEC 27001 risk management has been aligned with ISO 31000 (risk management standard)*
- *Some new requirements and some of the existing requirements (in 2005 version) have been modified and some deleted*
- *Annex A Reference control objectives and controls - revised to be aligned with the revision of ISO/IEC 27002: 2005*

27001:2005 vs 27001:2013



Requirements retained from 2005

- *Identical wording*
- *Equivalent requirement different wording*
- *Similar requirement (not identical or equivalent, but have a similar intent)*
- *Less restrictive (narrower requirement)*
- *More restrictive (broader requirement)*

Clause 4 Context of the organisation

- Understanding the organization and its context
- Understanding the needs and expectations of interested parties
- Determining the scope of the information security management system

Greater emphasis on Business Focus

Clause 5 Leadership

- Leadership and commitment
- Policy
- Organizational roles, responsibilities and authorities

Greater emphasis on Business Leadership Commitment

Clause 6 Planning

- Actions to address risks and opportunities
  - *Information security risk assessment*
  - *Information security risk treatment*
- Information security objectives and plans to achieve them

Dealing with risks

The risk assessment requirements are more general because the revised version of 27001 has been aligned with ISO 31000:2009 (Risk management — principles and guidelines):

- Removal of requirement: - to identify risks it is not necessary to identifying assets, threats and vulnerabilities. If your current organisational risk assessment method uses an approach based on assets, threats and vulnerabilities this is is perfectly acceptable. However, you can use other alternatives methods that are equally valid to identify, assess and evaluate your risks.

Dealing with risks

The risk assessment requirements are more general because the revised version of 27001 has been aligned with ISO 31000:2009 (Risk management — principles and guidelines):

- The SOA the requirements are basically those of the 2005 version, however you do not need to "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.

Dealing with risks

The risk assessment requirements are more general because the revised version of 27001 has been aligned with ISO 31000:2009 (Risk management — principles and guidelines):

- Preventative actions (8.3 of the 2005 version of 27001) has been deleted from the revised version but is recast in 6.1.1 as a general risk management requirement:

  6.1.1 … determine the risks and opportunities that need to be addressed to:

  a) ensure the information security management system can achieve its intended outcome(s);

  b) prevent, or reduce, undesired effects

Dealing with risks

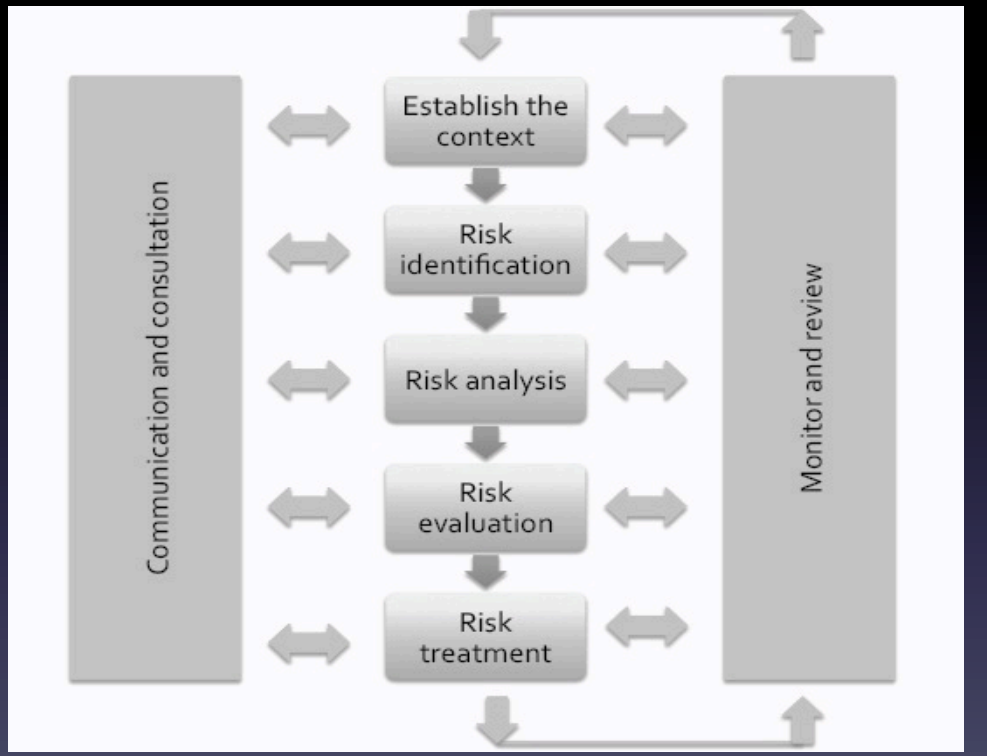
27001:2013

6 Planning
6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
6.1.3 Information security risk treatment
6.2 Information security objectives and plans to achieve them

8 Operation
8.2 Information security risk assessment
8.3 Information security risk treatment

9.3 Management review

ISO 31000:2009 (Risk management — principles and guidelines):



Clause 7 Support

- Resources
- Competence
- Awareness
- Communication
- Documented information

Greater emphasis on Business Capability

Clause 8 Operations

- Operational planning and control
- Information security risk assessment
- Information security risk treatment

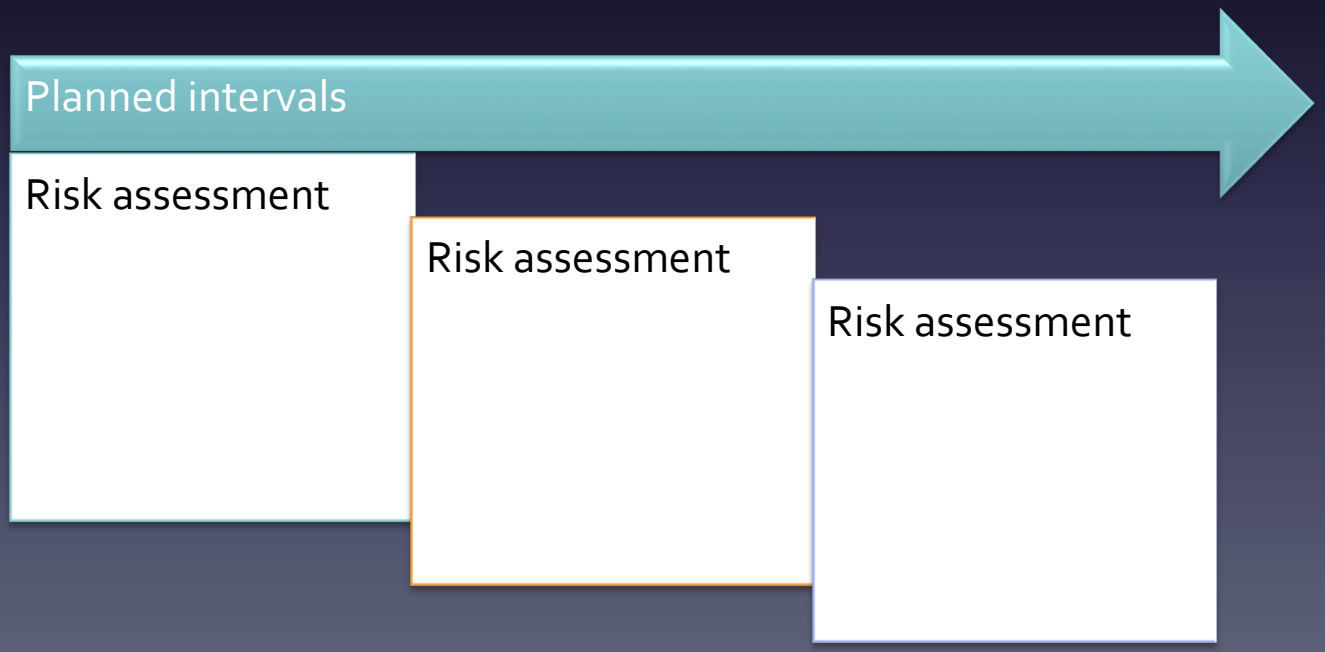
Clause 8.1 Operational planning and control

In this operational phase the organisation should be planning, implementing and controlling those processes that are essential to satisfy the information security requirements and implement those actions decided in the Planning phase (clause 6.1).

This phase is also about having processes and plans in place to achieve the information security objectives in an operational context (clause 6.2).

Clause 8.2 Information security risk assessment

- Risk assessment should be a process that the organisation uses
  - At planned intervals to ensure that the ISMS remains effective with regard to managing the risks (annually, biannually, quarterly …)



Clause 8.2 Information security risk assessment

- Risk assessment should be a process that the organisation uses
  - When there are changes that might affect the effectiveness of the ISMS or when a significant security event or incident warrants an immediate review of the risks associated with the ISMS or when there are other changes in the organisation that might have an impact of performance and effectiveness of the ISMS

Clause 8.3 Information security risk treatment

Implementing the treatment plan that was developed during the Planning phase (6.1.3)

Aspect
What needs to be done/actions to be taken to implement the required information security processes, policies, procedures, controls …
What resources are required to carry the work (people, budgets, technology, services, processes …)
Who are the responsible parties for the work
When should the work start and finish
How will the results be reviewed, tested and evaluated to check the work has been carried out correctly and it achieves the desired outcomes

Clause 9 Performance evaluation

- Monitoring, measurement, analysis and evaluation
- Internal audits
- Management review

Clause 9.1 Monitoring, measurement, analysis and evaluation

It is essential that an organisation shall have processes in place to evaluate the information security performance and the effectiveness of the ISMS

What is monitored and measured will give an indication of how well the ISMS is doing

(27001:2005 vs 2013) - measurements

4.2.2 Implement and operate ISMS

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results …

4.2.3 Monitor and review the ISMS

b) Undertake regular reviews of the effectiveness of the ISMS … taking into account … results from effectiveness measurements …

c) Measure the effectiveness of controls to verify that security requirements have been met.

4.3.1 General

g) documented procedures needed by the organization to ensure the effective planning, operation and … and describe how to measure the effectiveness of controls …

7 Management review of ISMS

7.2 Review input

f) results from effectiveness measurements;

7.3 Review output

e) Improvement to how the effectiveness of controls is being measured.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The security management system organization shall evaluate the information security performance and the effectiveness .

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE: The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analyzed and evaluated; and

f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

(27001:2005 vs 2013) - measurements

4.2.2 Implement and operate ISMS

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results …

4.2.3 Monitor and review the ISMS

b) Undertake regular reviews of the effectiveness of the ISMS … taking into account …. results from effectiveness measurements …

c) Measure the effectiveness of controls to verify that security requirements have been met.

4.3.1 General

g) documented procedures needed by the organization to ensure the effective planning, operation and … and describe how to measure the effectiveness of controls …

7.2 Review input

f) results from effectiveness measurements;

7.3 Review output

e) Improvement to how the effectiveness of controls is being measured.

9.3 Management reviews

The management review shall include consideration of:

a) ……..

c) feedback on the information security performance,

including trends in:

1) nonconformities and corrective actions;
2) monitoring and measurement results;

Clause 9.2 Internal audit

Organizations need to conduct internal audits, to check the ISMS conforms to requirements of ISO/IEC 27001 and to ensure that the ISMS functions as intended, and that it identifies weak links in the system as well as potential opportunities for improvement.

- *Conducting ISMS internal audits is mandatory for claiming conformance to ISO/IEC 27001*
- *The ISMS internal audit also acts as a feedback mechanism for the top management and other interested parties*

Clause 9.3 Management review

The input to the management review process, should include:

- Feedback from interested parties
- Feedback on information security performance
- Reports from internal ISMS audits
- Risk assessment results
- Status on risk treatment
- Changes to internal and external needs, expectations and requirements
- Identified opportunities
- Actions from previous reviews

Clause 10 Improvement

- Nonconformity and corrective action
- Continual improvement

Remaining Revision Time-Line

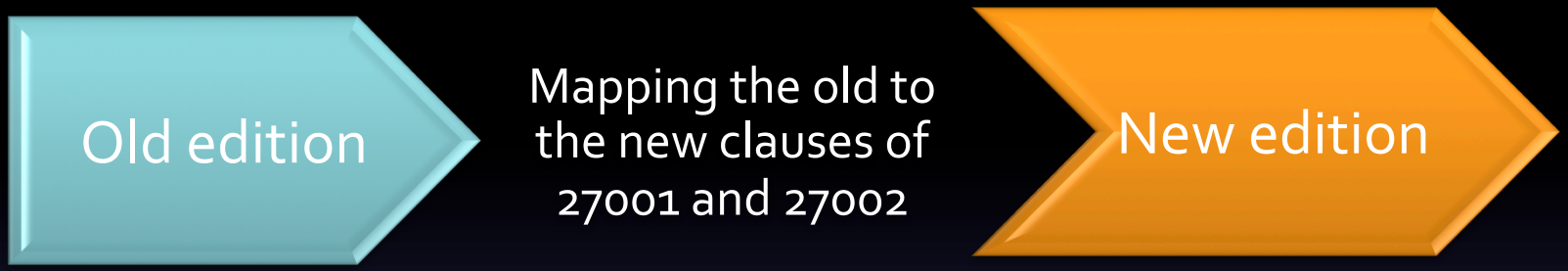
ISO/IEC 27001 New Edition (2013)

- *27001 FDIS ballot results are now available Sept*
- *27001 editors and ISO editors are currently preparing the final draft (correcting typographical errors)*
- *Scheduled date of publication is currently (editing closure) 1st Oct*

I am certified to ISO 27001:2005. What will this revision mean for me?

Organizations certified to the 2005 edition of the standard will need to upgrade their information security management system to comply with the requirements of the new edition. The transition period for upgrading has not yet been decided but typically this is two-three years from when the new edition is published. In addition, accredited certifying bodies should also use the transition period to update their activities to fit the requirements of the new edition. At the end of this transition period, the only valid certificates will be those that state conformity to the new requirements of ISO/IEC 27001:2013.

(ISO) SD3 Transition Maps



The purpose of SD3 is to show the corresponding relationship between the 2005 versions of ISO/IEC 27001 and ISO/IEC 27002 and the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002.

To be published by ISO as a transition guide (Oct 2013).

(ISO) SD3 Transition Maps (example)

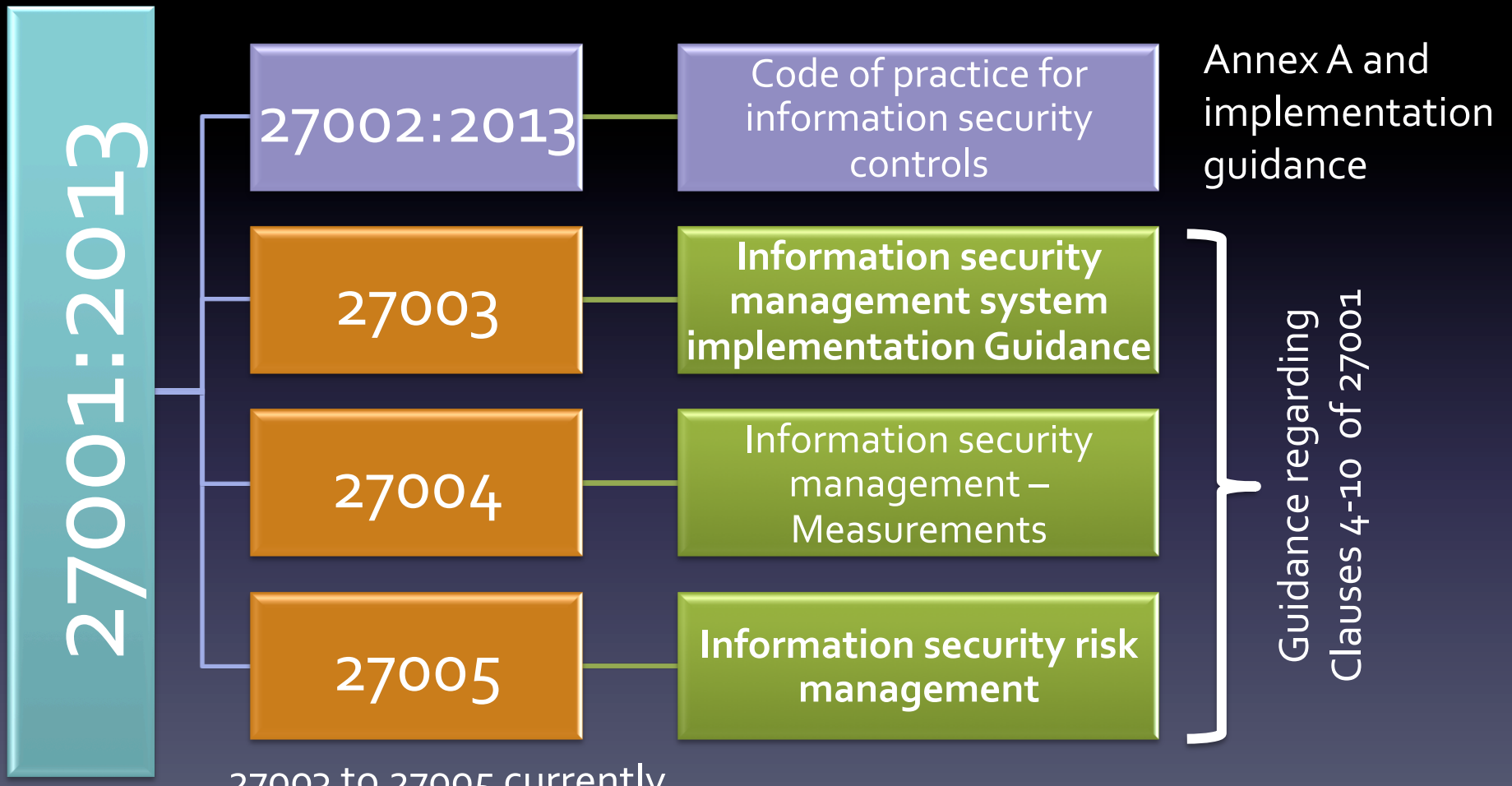
27001:2013	27001:2005
4.2 Understanding the needs and expectations of interested parties, a)interested parties that are relevant to the information security management system	New requirement
4.2 Understanding the needs and expectations of interested parties, b) the requirements of these interested parties relevant to information security.	5.2.1 Provision of resources The organization shall determine and provide the resources needed to: c) identify and address legal and regulatory requirements and contractual security obligations; 7.3 Review output The output from the management review shall include any decisions and actions related to the following: c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to: 4) regulatory or legal requirements; 5) contractual obligations

Delivering the New Version

Implementing the new version

- Documentation changes to reflect new structure
- Implement new requirements
- Where appropriate make necessary adjustments to the implementation of existing requirements
- Take account of new and modified controls (Annex A)
- Training staff

27001 Implementation Support

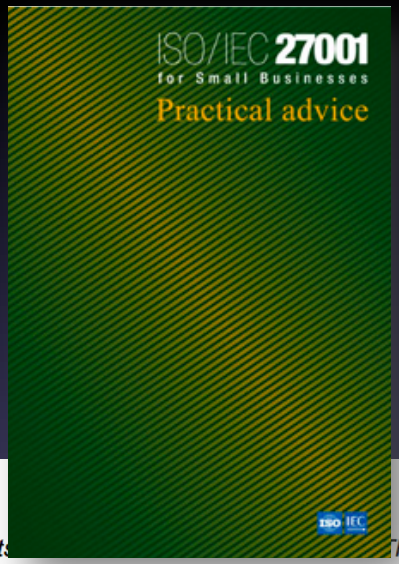


Sources of Help

Sources of Help

"Are You Ready For 27001 – 2013" – World Tour

On-line FAQ
ISO Articles
ISO Handbook – ISMS for SMEs
World Tour 'Are you ready' Seminars …



ISO ISMS Press Officer
(edwardj7@msn.com)

The new cyber warfare

Cyber threats continue to plague governments … these threats are on the rise as cyber criminals increase their focus and know-how. The problem demands an international solution. ISO/IEC 27001 provides a management framework for assessing and treating risks, whether cyber-oriented or otherwise, that can damage business, governments, and even the fabric of a country's national

New version of ISO/IEC 27001 to better tackle IT security risks

Final words

Be ready, be prepared to deploy the revised version because the certification transition deadline may only be 2-3 years away

Forewarned is forearmed; to be prepared is half the victory.
Miguel de Cervantes

Thanks For Listening

Prof. Edward (Ted) Humphreys

(edwardj7@msn.com)

Vienna, 19 Sept 2013