IMS-Smart

SMARTER MANAGEMENT SYSTEMS FOR SMARTER PEOPLE

Understanding the new ISO management system standards

(high level structure)

Dr. David Brewer, FBCS

IMS-Smart Limited

https://ims-smart.com

dbrewer@ims-smart.com

Agenda

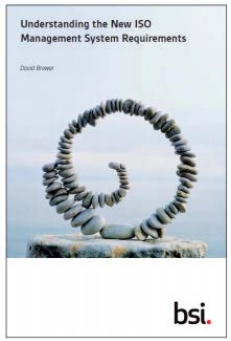
- Introductory remarks
- The new ISO directives
- Understanding the new requirements
- Transitioning to the new management system standards
- Summary

Introductory remarks - don't panic

There is a full explanation of ISO/IEC 27001:2013 in "An introduction to ISO/IEC 27001:2013" published by BSI

There is a free transition brochure:

And other books:

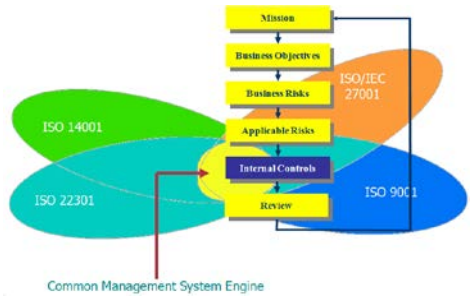


The new ISO directives

ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2013, Annex SL

Motivation – integrated management systems

- Many management system standards (MSS)
- They have much in common:
  - *Corrective actions, improvement, document control, etc.*
- Common requirements ought to be worded identically → "identical core text"
- Common structure is also useful → "high level structure"
- Ensures that MSS are designed to foster integrated management systems (IMS)



What differentiates one MSS from another → discipline-specific text

High level structure

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
   - 4.1 Understanding the organization and its context
   - 4.2 Understanding the needs and expectations of interested parties
   - 4.3 Determining the scope of the XXX management system
   - 4.4 XXX management system
5. Leadership
   - 5.1 Leadership and commitment
   - 5.2 Policy
   - 5.3 Organization roles, responsibilities and authorities
6. Planning
   - 6.1 Actions to address risks and opportunities
   - 6.2 XXX objectives and planning to achieve them
7. Support
   - 7.1 Resources
   - 7.2 Competence
   - 7.3 Awareness
   - 7.4 Communication
   - 7.5 Documented information
     - 7.5.1 General
     - 7.5.2 Creating and updating
     - 7.5.3 Control of documented information
8. Operation
   - 8.1 Operational planning and control
9. Performance evaluation
   - 9.1 Monitoring, measurement, analysis and evaluation
   - 9.2 Internal audit
   - 9.3 Management review
10. Improvement
    - 10.1 Nonconformity and corrective action
    - 10.2 Continual improvement

Think the standard as a blue print for how an ISMS works, not how to build one

Useful properties

- Order of implementation is irrelevant
- Effectively all requirements must be satisfied simultaneously
- No duplicate requirements

Remark about this in the introduction to the standard

High level structure

But they are listed in "An introduction to ISO/IEC 27001:2013" and the transition guide

0. Int
1. Sc
2. No
3. Te
4. Co
   4.
   4.
   4.
   4.
5. Lea
   5.
   5.
   5.
6. Pla
   6.
   6.
7. Su
   7.
   7.
   7.
   7.
   7.

Documented information

The requirements for documented information are spread throughout the standard. However, in summary they are:

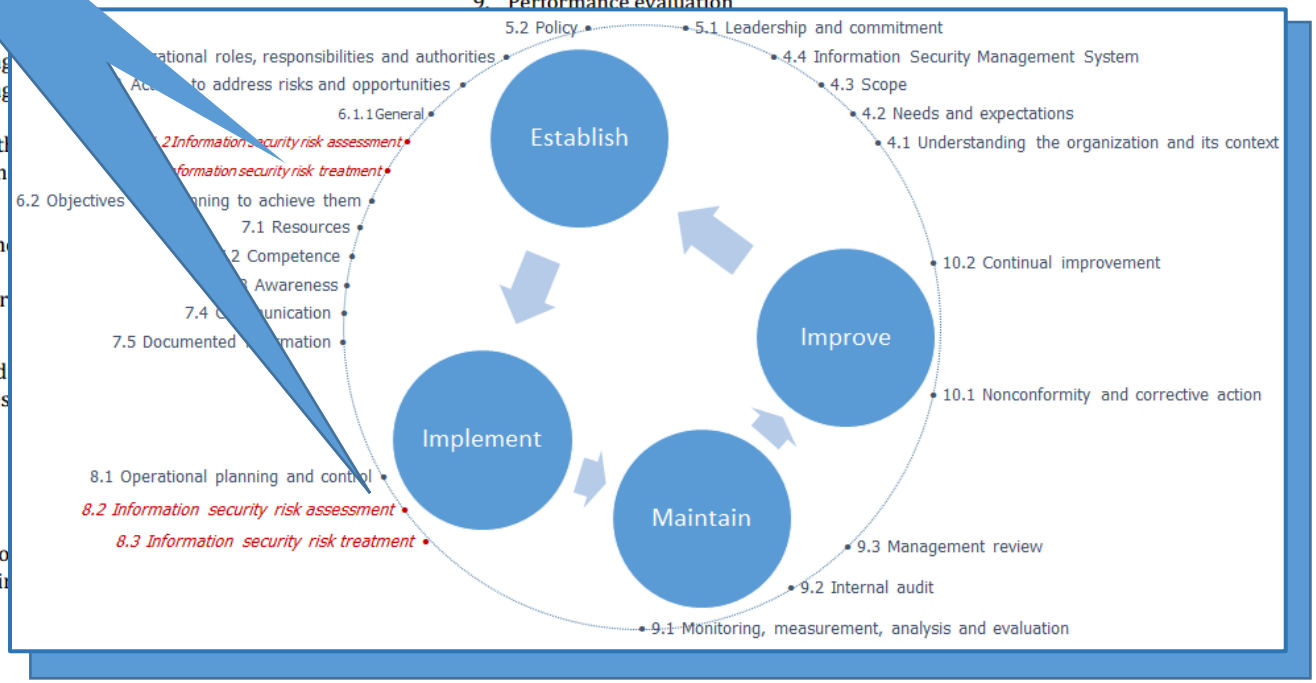
4.3	Scope of the ISMS	8.1	Operational planning and control
5.2	Information security policy	8.2	Results of the information security risk assessments
6.1.2	Information security risk assessment process	8.3	Results of the information security risk treatment
6.1.3	Information security risk treatment process	9.1	Evidence of the monitoring and measurement results
6.1.3 d)	Statement of Applicability	9.2 g)	Evidence of the audit programme(s) and the audit results
6.2	Information security objectives	9.3	Evidence of the results of management reviews
7.2 d)	Evidence of competence	10.1 f)	Evidence of the nature of the nonconformities and any subsequent actions taken
7.5.1 b)	Documented information determined by the organization as being necessary for the effectiveness of the ISMS	10.1 g)	Evidence of the results of any corrective action

- No duplicate requirements

High level structure + ISO/IEC 27001:2013

Discipline-specific text

3. Terms and defi
4. Context of the orga
   - 4.1 Understanding
   - 4.2 Understanding parties
   - 4.3 Determining t
   - 4.4 XXX managem
5. Leadership
   - 5.1 Leadership an
   - 5.2 Policy
   - 5.3 Organization r
6. Planning
   - 6.1 Actions to add
   - 6.2 XXX objectives
7. Support
   - 7.1 Resources
   - 7.2 Competence
   - 7.3 Awareness
   - 7.4 Communicatio
   - 7.5 Documented i
     - 7.5.1General
     - 7.5.2Creating and updating
     - 7.5.3Control of documented information
8. Operation
   - 8.1 Operational planning and control
9. Performance evaluation



Identical core text

4. Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its XXX management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine

— the interested parties that are relevant to the XXX management system, and

— the requirements of these interested parties.

E.g. quality, business continuity, information security, etc.

Discipline-specific text

Only appears in ISO/IEC 27001:2013

6.1.2 Information security risk assessment

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

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

Deviations

- Changes to identical core text
- Registered with ISO Technical Management Board)

An addition

A deletion

ISO/ IEC 27001 Clause	Change or addition
4.2 b)	The words 'relevant to information security' have been added.
4.3 c)	The list item 'c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.' has been added.
4.4	The phrase 'including the processes needed and their interactions' has been deleted.
5.1 b)	The word 'business' has been deleted together with the note that explains what a business process is.
5.2 b)	The words 'includes information security objectives (see 6.2) or' have been added.
5.2 c)	The words 'related to information security' have been added.

Other examples include moving text (e.g. in Clause 9.1)

Extract from "An introduction to ISO/IEC 27001:2013" by David Brewer, published by BSI

Understanding the new requirements

Definitions

- Take care
- There are lots of new definitions, e.g.

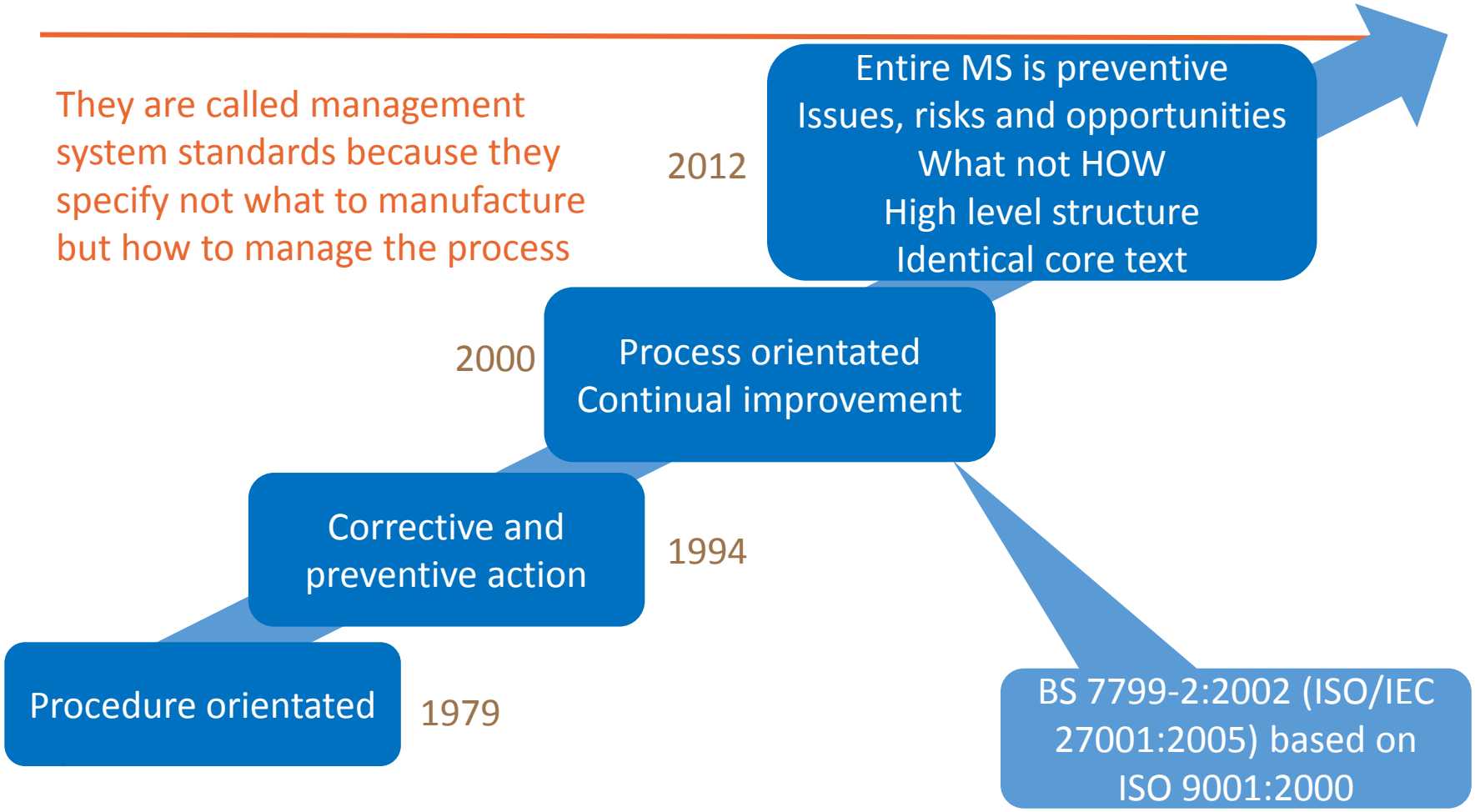
> **3.04**
> **management system**
> set of interrelated or interacting elements of an **organization** (3.01) to establish **policies** (3.07) and **objectives** (3.08) and **processes** (3.12) to achieve those objectives

Extract from ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 4th edition, Appendix 2 to Annex SL

- Many are taken from Annex SL and ISO 31000 and are not in ISO/IEC 27000:2012, but they will be in the next version, due imminently
- If not in ISO/IEC 27000:2013, use the Oxford English Dictionary
- Can't wait: they are all in "An introduction to ISO/IEC 27001:2013", **plus explanations**

4th generation management system standards

They are called management system standards because they specify not what to manufacture but how to manage the process



New and updated concepts

New/updated concept	Explanation
Context of the organization	The environment in which the organization operates
Issues, risks and opportunities	Replaces preventive action
Interested parities	Replaces stakeholders
Leadership	Requirements specific to top management
Communication	There are explicit requirements for both internal and external communications
Information security objectives	Information security objectives are now to be set at relevant functions and levels
Risk assessment	**Identification of assets, threats and vulnerabilities is no longer a prerequisite for the identification of information security risks**
Risk owner	**Replaces asset owner**
Risk treatment plan	**The effectiveness of the risk treatment plan is now regarded as being more important than the effectiveness of controls**
Controls	**Controls are now determined during the process of risk treatment, rather than being selected from Annex A**
Documented information	Replaces documents and records
Performance evaluation	Covers the measurement of ISMS and risk treatment plan effectiveness
Continual improvement	Methodologies other than Plan-Do-Check-Act (PDCA) may be used

Extract from BSI's ISO/IEC 27001 transition guide

To explain further, we consider transition …

Transitioning to the new standard

Background

- Practical experience of transitioning a real ISMS
- Work performed in support of the development of IO/IEC 27001:2013
  - *Sabrina Feng, Head Risk & Security, AXA Group Solutions*
  - *David Brewer, IMS-Smart Limited*
- Started with CD1 (April 2011) through to FDIS (April 2013)
  - *Five times: CD1, CD2, CD3, DIS, FDIS*
- Purpose: to ensure ISMS requirements were implementable
  - *Early days not always the case*
  - *Issues feedback to the UK shadow committee and then to ISO*
  - *Resolved at the next ISO meeting*
  - *All requirements are now implementable*

Types of change

- Areas where changes may be minimal
- Areas that potentially require a rethink
- Areas requiring updating
- New requirements that may be already satisfied
- New requirements that may present a challenge

Areas where changes may be minimal

- Documented information
- Policy
- Risk assessment
- Control of documentation
- Terms of reference for top management
- Responsibilities
- Awareness
- Internal audit
- Management review
- Corrective action
- Improvement

Still have documents and records, just now called 'documented information' (but several document requirements have been deleted)

Don't need assets, threats and vulnerabilities, but there is no need to change if it is working for you

Inputs are no longer specified but discussion topics are

Need to react to nonconformities as appropriate

Suitability & adequacy as well as effectiveness

Areas that potentially require a rethink

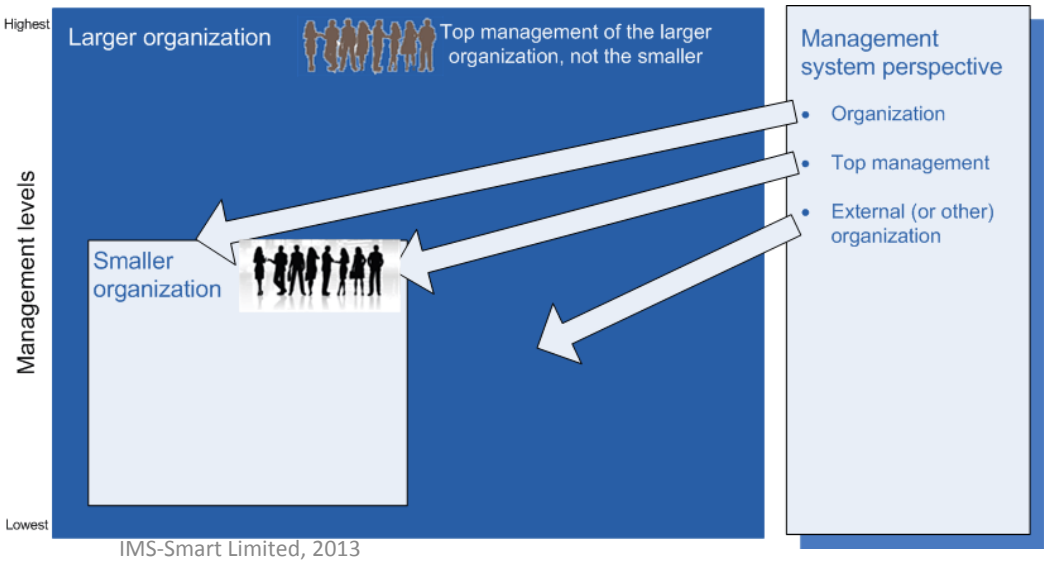
Scope of the management system

Information security objectives

Scope of ISMS = Everything of interest to the ISMS, i.e. not the scope of certification

Includes activities performed by external organisations
Clause 4.3 c) will help

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.



At relevant functions and levels, e.g.

- Policy
- ISMS process and risk treatment plan
- Management action

Need to define responsibilities and target dates

Areas requiring updating

Statement of Applicability

No longer required to SELECT controls from Annex A

SOA (Statement of Applicability) requirements pretty much the same as in ISO/IEC 27005:2005

1. 114 controls, there are mapping tables, but best approach is to regenerate the SOA, using it as a cross-check of your existing controls
2. Beware, once deemed “applicable”, ensure that what you do really does conform to the Annex A definition of the control

New requirements that may be already satisfied

Interested parties and their requirements

Integration

Communication

Likely already to be known

Remember though: a requirement is a need or expectation that is stated, generally implied or obligatory

'Good governance' requirement – customers/public will have an expectation that good information security practice is followed

Try representing your business functions as workflow diagrams: if ISMS requirements are spread throughout them, the integration requirement is probably met

Do you have someone or a group of people who are responsible for internal and external communications?

New requirements that may present a challenge

Issues

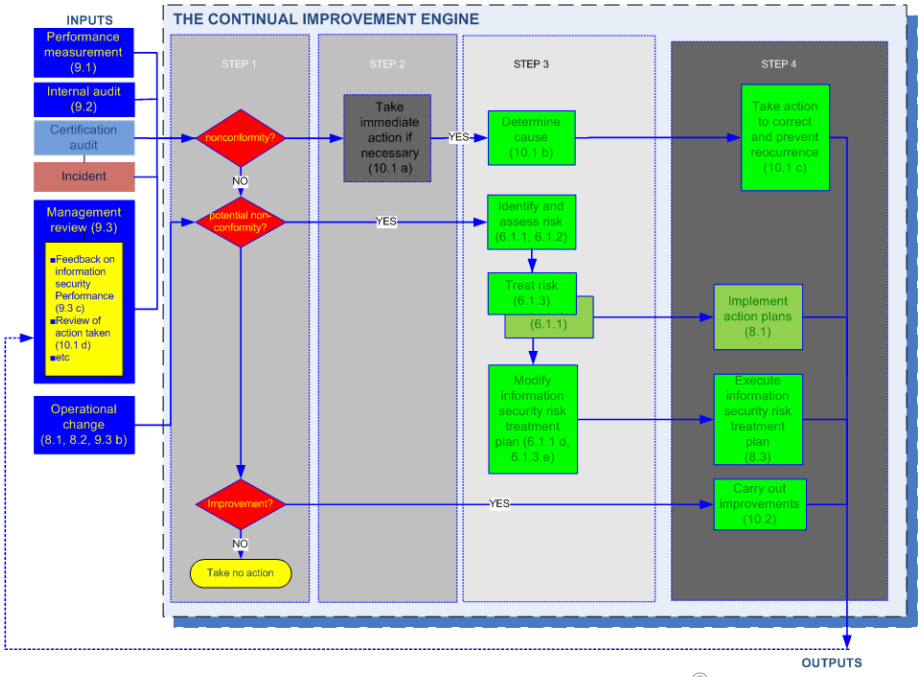
Actions to address risks and opportunities

Monitoring, measurement, analysis and evaluation

E.g. motivation for having an ISMS; information security; management issues, business context etc., More ideas in the book

Not necessarily a problem …

It depends on how you have been treating preventive action



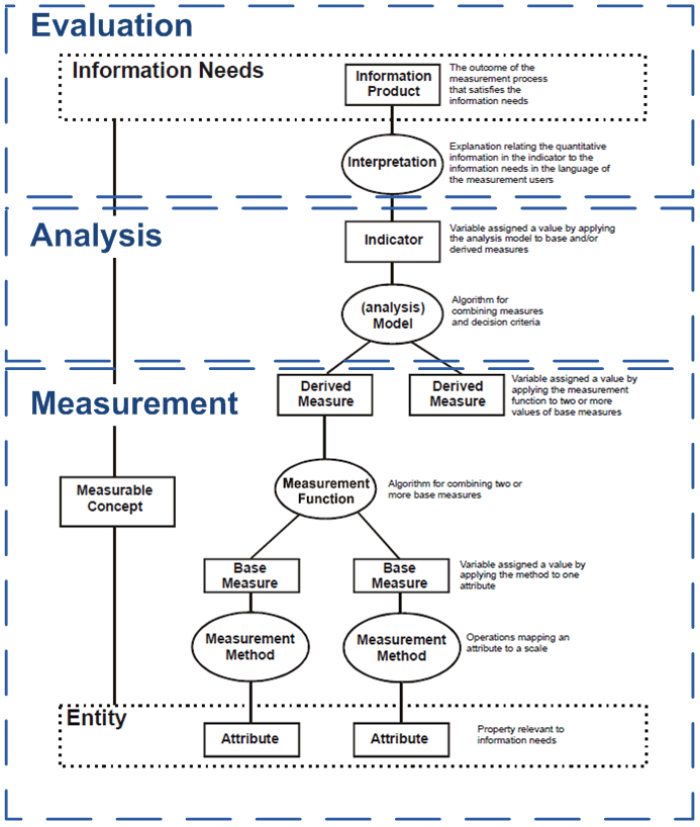
New requirements that may present a challenge

Issues

Actions to address risks and opportunities

Monitoring, measurement, analysis and evaluation

Best treat this as new



- Work out what you (top management) wants to know about IS performance and ISMS effectiveness
- Think KPIs, is a good start
- Then work out what you need to measure and monitor
- Don't measure and monitor for the sake of it
- Requirements will change
- ISO/IEC 27004 is being revised
- Read the book☺

Deleted requirements

Clause (in ISO/IEC 27001:2005)	Deleted requirement	Clause (in ISO/IEC 27001:2005)	Deleted requirement
4.2.1(g)	The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.	4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.
4.2.1(i)	Obtain management authorization to implement and operate the ISMS.	4.3.3	and of all occurrences of significant security incidents related to the ISMS.
4.2.3(a)(1)	promptly detect errors in the results of processing;	5.2.1(b)	ensure that information security procedures support the business requirements;
4.2.3(a)(2)	promptly identify attempted and successful security breaches and incidents;	5.2.1(d)	maintain adequate security by correct application of all implemented controls;
4.2.3(a)(4)	help detect security events and thereby prevent security incidents by the use of indicators; and	6(d)	The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.
4.2.3(a)(5)	determine whether the actions taken to resolve a breach of security were effective.	8.2	The documented procedure for corrective action shall define requirements for:
4.2.3(h)	Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).	8.3	The documented procedure for preventive action shall define requirements for:
4.3.1	Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible.	8.3(d)	recording results of action taken (see 4.3.3); and
4.3.1	It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.	8.3(e)	reviewing of preventive action taken.
4.3.1(c)	procedures and controls in support of the ISMS;	8.3(e)	The priority of preventive actions shall be determined based on the results of the risk assessment.
4.3.2	A documented procedure shall be established to define the management actions needed to:		

Summary

Summary

- All new and revised management system standards, e.g. ISO/IEC 27001, must conform to new high level structure and identical core text
- Greater clarity, what not how, no duplications
- Purpose built for integrated management systems
- Latest leap in the evolution of MSS – 4th generation
- New and updated concepts, read the definitions carefully
- Practical advice on transitioning (the transition guide)
- Good supporting documentation

IMS-Smart

SMARTER MANAGEMENT SYSTEMS FOR SMARTER PEOPLE

Understanding the new ISO management system standards

Dr. David Brewer, FBCS

IMS-Smart Limited

https://ims-smart.com

dbrewer@ims-smart.com