

ISO/IEC 27001:2013 webinar

11 June 2014



Dr. Mike Nash
Gamma Secure Systems Limited

**UK Head of Delegation,
ISO/IEC JTC 1/SC 27**



Introducing ISO/IEC 27001:2013 and ISO/IEC 27002:2013

New versions of the Information Security
Management System (ISMS) Standards



Mike Nash

Gamma Secure Systems Limited

UK Head of Delegation,
ISO/IEC JTC 1/SC 27

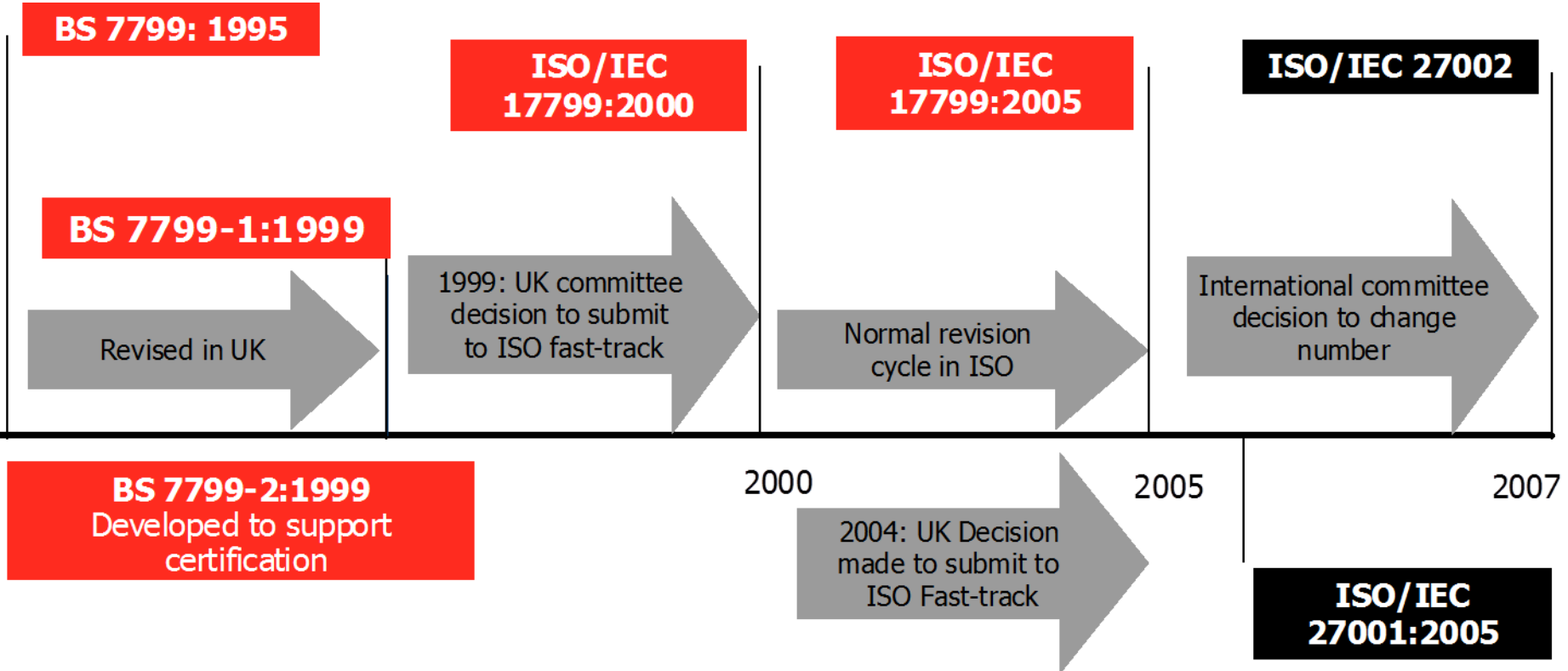
A little bit of history



ISO/IEC 27000 – a UK success story

- Original requirement identified by the Department of Trade and Industry (DTI) in late 1980s
 - UK companies held back by lack of information security advice and guidance
 - Market needed a “code of practice”
- Developed for DTI, published by BSI
- Became a British Standard, BS 7799, in 1995
 - Certification standard BS 7799-2 followed in 1999
- Became International Standards ISO/IEC 27001 and 27002 in 2005
- Other information security standards now being developed or harmonised into 270xx series standards

ISO/IEC 27001 and 27002: Evolution

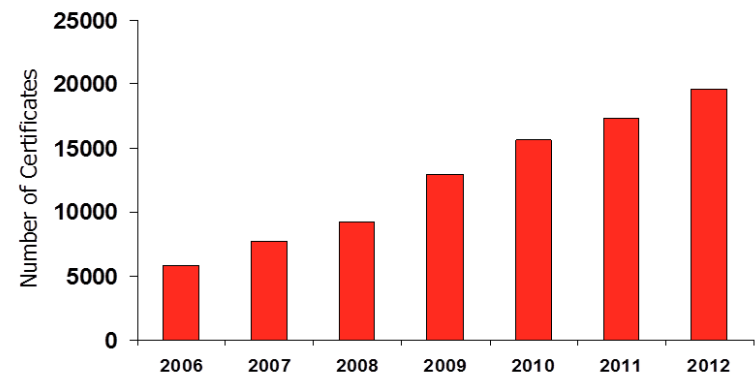


Why new editions now?



Why revision now?

- All ISO Standards are regularly reviewed and updated if necessary
- Review of 27001:2005 and 27002:2005 identified that changes were necessary
 - Practical experience of building and operating ISMS
 - Growth of integrated management systems
 - Advances in risk assessment
 - Advances in information security technologies
 - Advances in information technology



The result ...

BS ISO/IEC 27002:2013




BSI Standards Publication

**Information technology —
Security techniques — Code
of practice for information
security controls**

bsi. ...making excellence a habit™

BS ISO/IEC 27001:2013



BSI Standards Publication

**Information technology —
Security techniques —
Information security
management systems —
Requirements**

bsi. ...making excellence a habit™

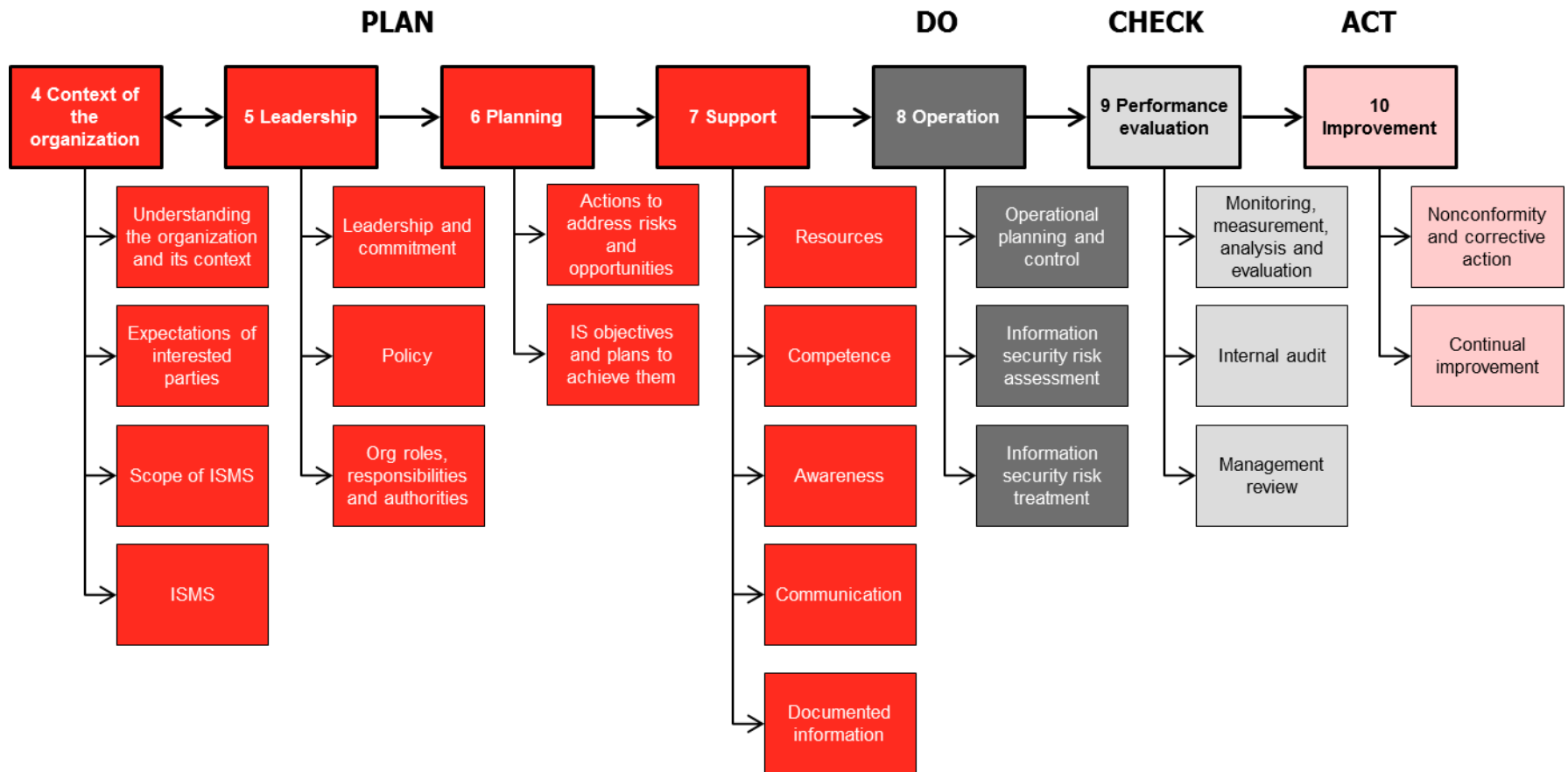
The new ISO/IEC 27001



ISO/IEC 27001:2013 follows the new ISO MSS common structure

- ISO/IEC 27001:2013 has been developed using “Annex SL”
 - “Annex SL” is now part of the Directives for producing ISO standards
- Mandatory common structure for all management system standards
 - Standardised terminology
 - Standardised fundamental management system requirements
 - Standardised common text for standard requirements
- This means ISO/IEC 27001:2013 has a different structure to 27001:2005
- All other ISO management systems standards (e.g. ISO 9001, ISO 14001, ...) will also be revised to follow “Annex SL” and use the common text
 - Will therefore have an identical structure to 27001:2013
 - And have identical text for identical requirements

The new ISO/IEC 27001:2013 structure



Comparison with 2005 structure

27001:2005 (old)	27001:2013 (new)
0 Introduction	0 Introduction
1 Scope	1 Scope
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions
4 Information security management system	4 Context of the organization
5 Management responsibility	5 Leadership
6 Internal ISMS audits	6 Planning
7 Management review	7 Support
8 ISMS improvement	8 Operation
Annex A (normative) Control objectives and controls	9 Performance evaluation
Annex B (informative) OECD principles and this international standard	10 Improvement
Annex C (informative) Correspondence between ISO 9001:2000; ISO 14001:2004; and this international standard	Annex A (normative) Reference control objectives and controls

Terms and definitions

- All of the definitions that were in the 2005 version have been removed
- Those that are still relevant are included in ISO/IEC 27000:2014
- Ensures consistency of terms and definitions across the suite of ISO/IEC 270xx standards

Context versus “establish the ISMS”

- The new “context” clause requires understanding of the organization and its needs
 - Determine external and internal issues
 - Consider interested parties and their requirements
 - Requirements of interested parties may include legal and regulatory requirements and contractual obligations
- Context determines the information security policy and objectives
 - And how the organization will consider risk and the effect of risk on its business
- An appropriate scope for the ISMS is now required

Leadership

- Replaces management responsibility clause
- Leadership is more than just management
- Top management leadership must be demonstrable and active
- Top management sets information security policy
- Top management must ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated

Planning

- New Planning clause establishes information security objectives and guiding principles for the ISMS as a whole
- When planning the ISMS, the context of the organization should be taken into account through the consideration of the risks and opportunities
- The organization's information security objectives must be clearly defined with plans in place to achieve them
- Risk assessment requirements are more general reflecting an alignment of ISO/IEC 27001 with ISO 31000
- The changes to risk assessment will make it easier for organizations to select from a wide range of methodologies
- The SOA requirements are largely unchanged

Support

- The Support clause identifies what is required to establish, implement and maintain and continually improve an effective ISMS, including:
 - Resource requirements
 - Competence of people involved
 - Awareness of and communication with interested parties
 - Requirements for document management
- The new standard refers to “documented information” rather than “documents and records” and requires that they be retained as evidence of competence
- There is no longer a list of documents you need to provide or particular names they must be given
- The new revision puts the emphasis on the content rather than the name

Operation

- Organizations must plan and control the processes needed to meet their information security requirements including:
 - keeping documents
 - management of change
 - responding to adverse events
 - the control of any outsourced processes
- Operation planning and control also mandates:
 - The carrying out of information security risk assessments at planned intervals
 - The implementation of an information security risk treatment plan

Performance evaluation

- Internal audits and management review continue to be key methods of reviewing the performance of the ISMS and tools for its continual improvement
- The new requirements for measurement of effectiveness are more specific and far reaching than the 2005 version which referred to effectiveness of controls
- To ensure its continuing suitability, adequacy and effectiveness, management must consider any changes in external and internal issues

Improvement

- The organization must react to any non conformity identified, take action to control and correct it, and deal with the consequences
- Nonconformities within the ISMS have to be dealt with, corrective actions must ensure they don't recur or occur elsewhere
- As with all management system standards, continual improvement is a core requirement of the standard

Other changes from ISO/IEC 27001:2005

- Does not emphasise Plan-Do-Check-Act cycle in same way as ISO/IEC 27001:2005 did
- There have been changes to the terminology used
- The term “preventive action” has been replaced with “actions to address, risks and opportunities” and features earlier in the standard
- SOA requirements are similar but with more clarity on the determination of controls by the risk treatment process
- Greater emphasis on setting objectives, monitoring performance and metrics

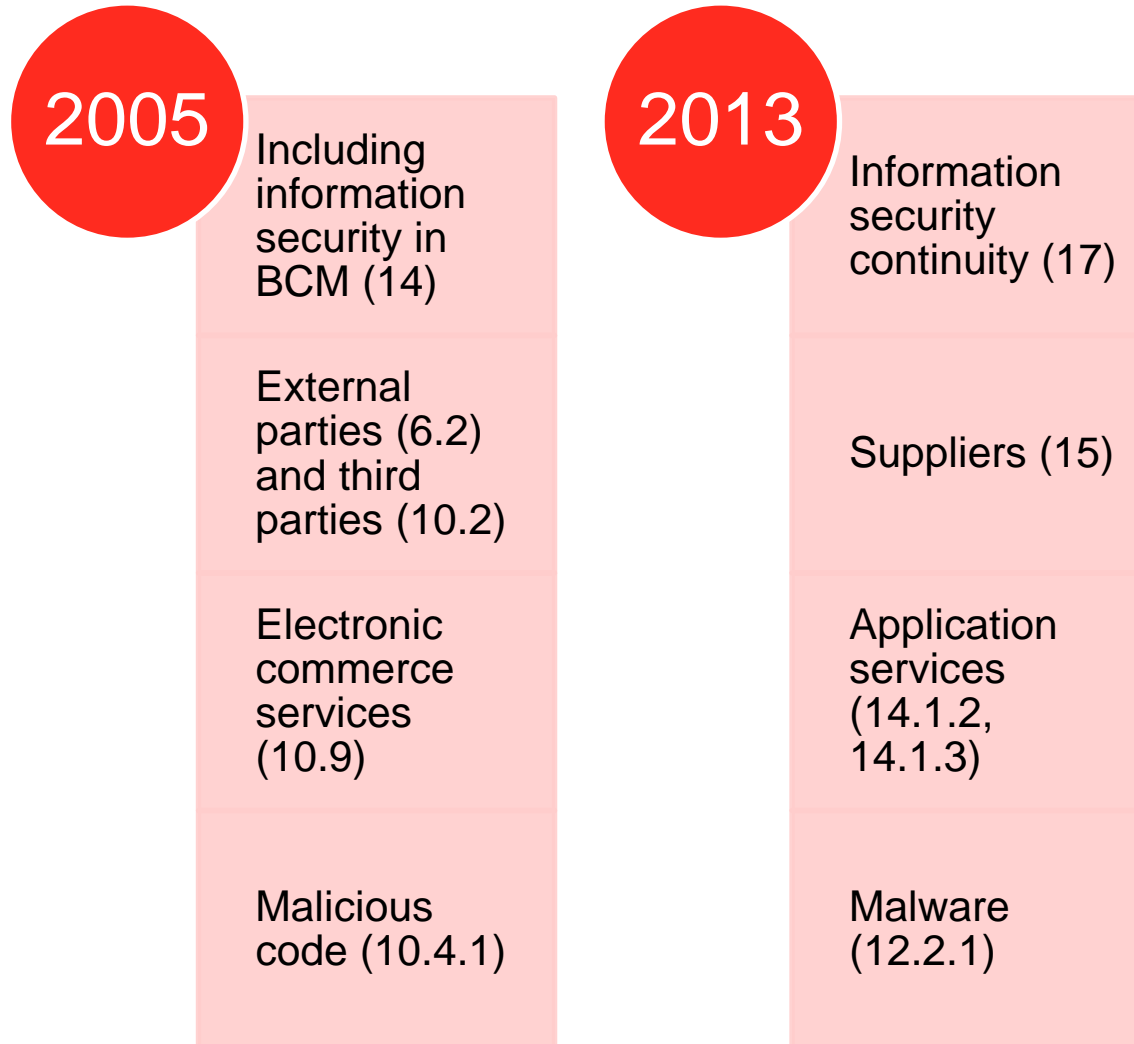
The new ISO/IEC 27002



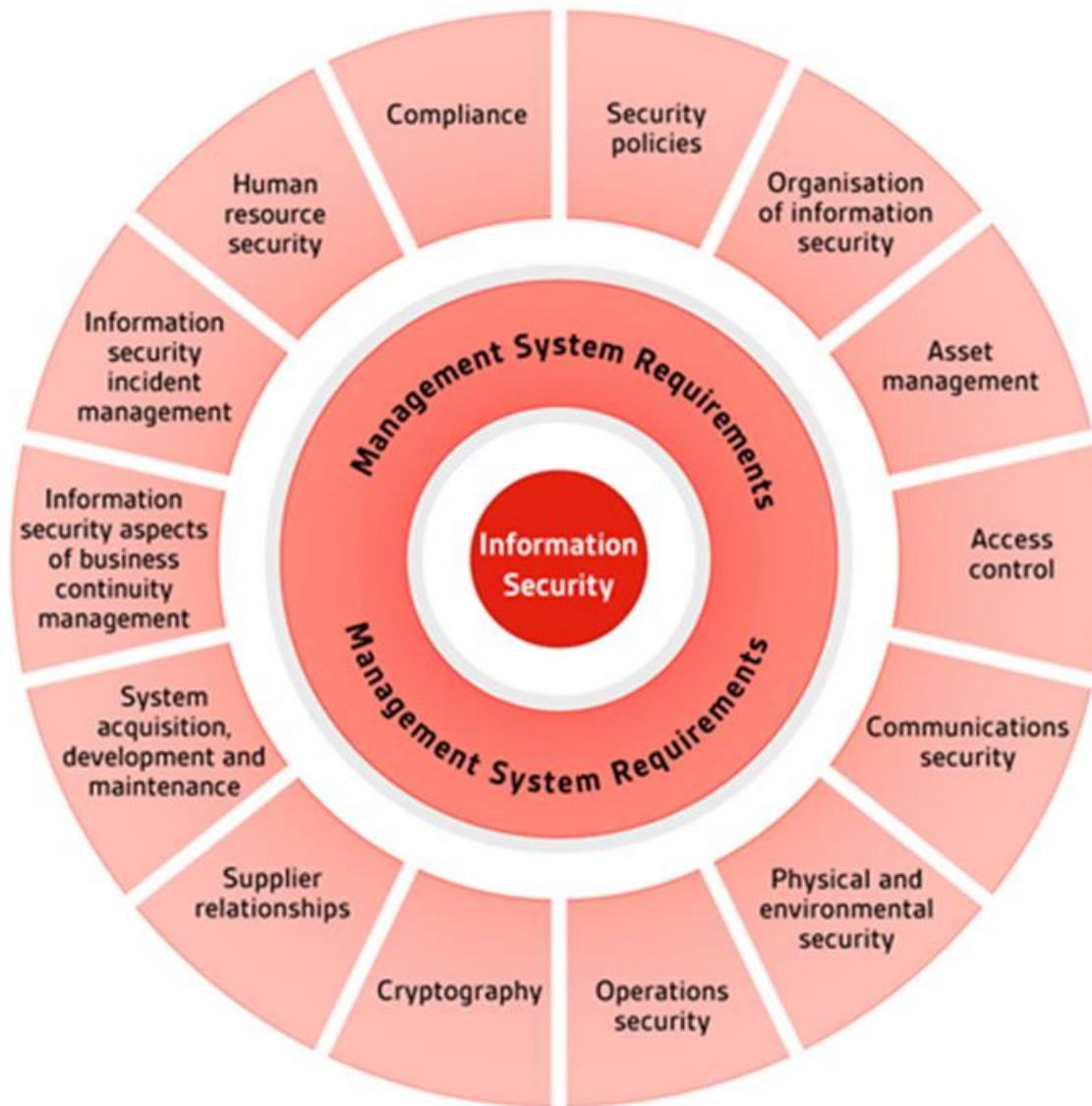
ISO/IEC 27002:2013 – revised and updated

- New title - code of practice for information security controls
- Revised structure – more logical grouping of controls
- Changes to terminology to reflect industry changes
- Additional controls to reflect changes in security technology and advances in IT
- Some similar existing controls combined together
- Extra implementation guidance
- Historical content removed

Changes in emphasis and terminology



New, cleaner organization of controls



A rough mapping of control groups

ISO/IEC 27002:2005		ISO/IEC 27002:2013	
5	Security policy	5	Security policies
6	Organization of information security	6	Organization of information security
8	Human resource security	7	Human resource security
7	Asset management	8	Asset management
11	Access control	9	Access control
12.3	Cryptographic controls	10	Cryptography
9	Physical and environmental security	11	Physical and environmental security
10	Communications and operations management	12	Operations security
		13	Communications security
12	Information systems acquisition, development and maintenance	14	System acquisition, development and maintenance
	N/A	15	Supplier relationships
13	Information security incident management	16	Information security incident management
14	Business continuity management	17	Information security aspects of business continuity management
15	Compliance	18	Compliance

New or significantly broadened controls

- 6.1.5 Information security in project management
- 12.6.2 Restrictions on software installation
- 14.2.1 Secure development policy
- 14.2.5 Secure system engineering principles
- 14.2.6 Secure development environment
- 14.2.8 System security testing
- 15.1.1 Information security policy for supplier relationships
- 15.1.3 Information and communication technology supply chain
- 16.1.4 Assessment of and decision on information security events
- 16.1.5 Response to information security incidents
- 17.2.1 Availability of information processing facilities

Summary of key changes from ISO/IEC 27002:2005

- New title – Code of practice for information security controls
- Controls have been reordered and reduced – 133 to 114 controls
- Historical content removed
 - Some supporting text will move to implementation guidance (ISO/IEC 27003)
 - No duplication of ISO/IEC 27001 risk assessment/treatment
 - No “essential” controls in foreword
- Control titles better matched to content
- Implementation guidance revised and improved

Impact on other 27000 Standards



Impact on other 270xx standards

- ISO/IEC 27000, Overview and vocabulary, has been updated
 - Contains a single set of definitions used by all 270xx Standards
 - Available as a free download from ISO Geneva
- Inspection and audit standards are being updated
 - Important for supply chain inspection requirements
 - ISO/IEC 27006 now at second Committee Draft
- Sector specific ISMS standards will be updated
- ISO/IEC 27011 (ITU-T X.1051), IEC 62443-2-1, ISO 27799, etc...
 - "Standard for ISMS standards" (ISO/IEC 27009) under development
 - Introduction of "common text" directive will remove unnecessary deviations
 - Expect to see "sector specific certification" more widely used

Additional information

- The 270xx Standards committee JTC 1/SC 27 is trying to help users understand the changes
- Developed additional information on changes and transition
 - Copyright issues
 - Payment issues
- A minor problem has been found in ISO/IEC 27001 and 27002 concerning “assets associated with information”. Will be resolved by issuing technical corrigenda (i.e. a small change to wording).

Dr. David Brewer IMS-Smart Limited

Member ISO JTC 1 SC27 WG1
Co-editor for the revision of
ISO/IEC 27004



Understanding the new ISO management system standards

High level structure



Dr David Brewer

FBCS

IMS-Smart Limited

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 also a free transition guide:



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

Remark about this
in the introduction
to the standard

Useful properties

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

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

High level structure

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

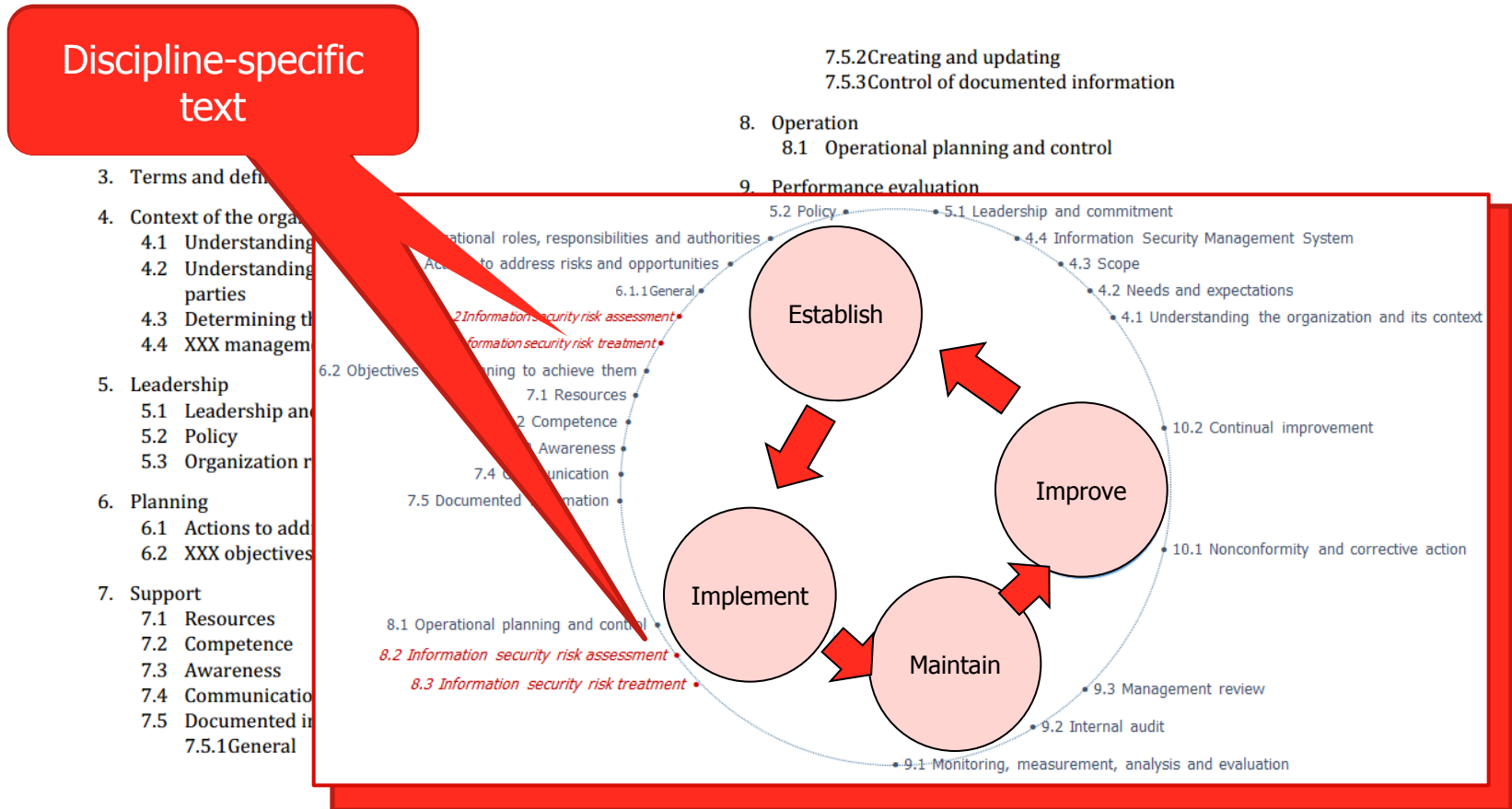
Documented information

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



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.

Note: there is no documented information requirement for 4.1 and 4.2. How you demonstrate conformance is up to you: There are 38 requirements in total like this

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

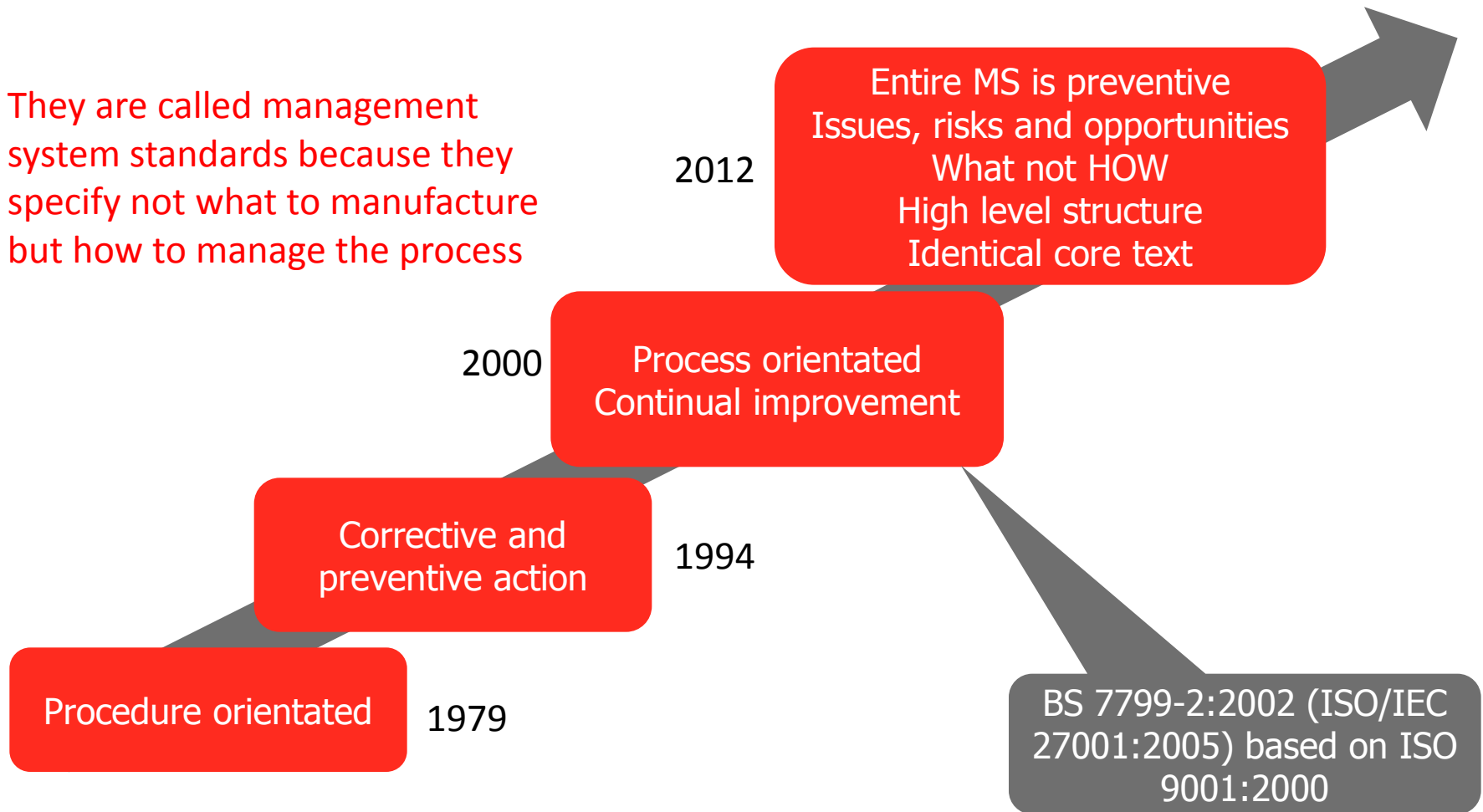
set of interrelated or interacting elements of an **organization** (3.01) to establish **policies** (3.07) and **objectives** (3.08) and **processes** (3.12) to achieve those objectives

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

- They are in ISO/IEC 27000:2014
- If its not there, use the OED

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 parties	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

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

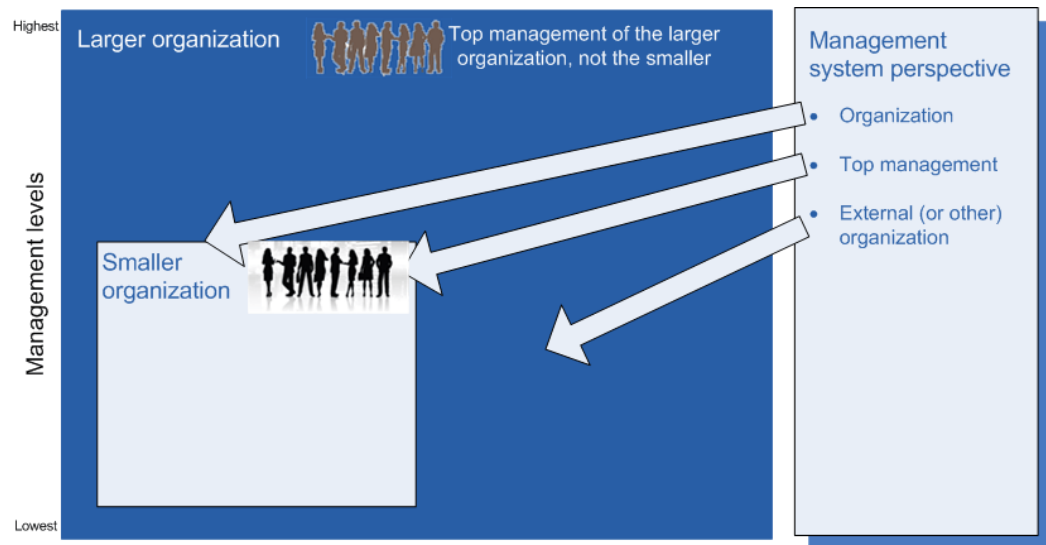
Scope of the management system
Information security objectives

Includes activities performed by external organizations
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

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. Don't forget to include all the controls determined by your risk treatment process (i.e., not just Annex A controls)
3. Beware, if an Annex A control is deemed necessary, ensure that what you do really does conform to the Annex A definition of the control

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

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?

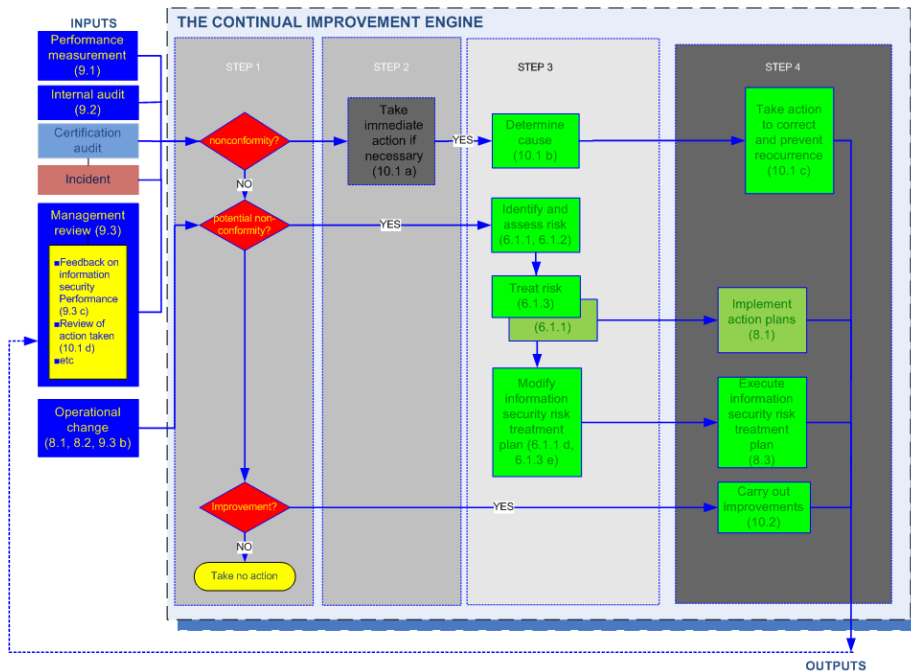
New requirements that may present a challenge

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

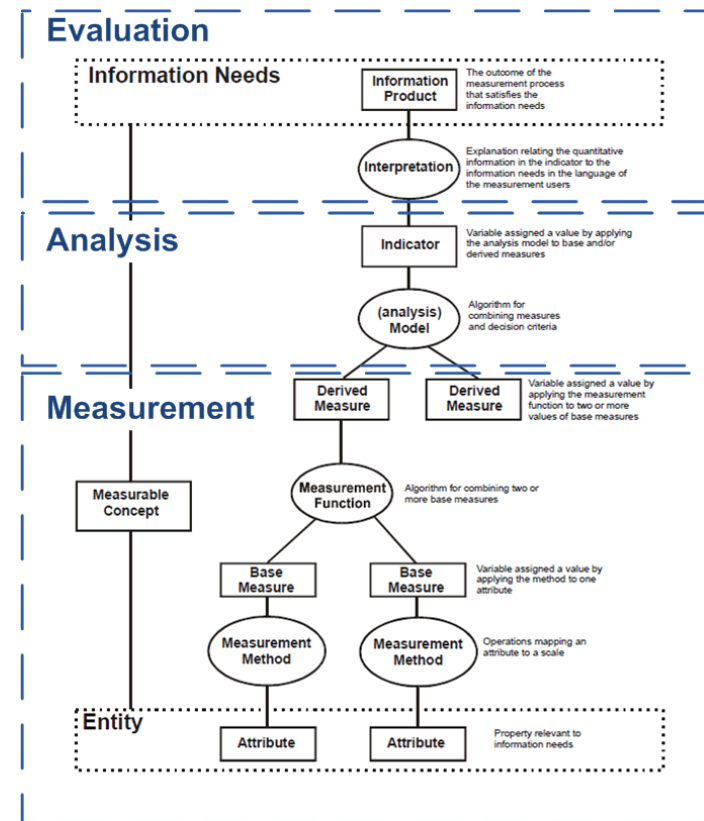
Issues

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

ISO/IEC 27001:2005 to 2013 transition arrangements



Suzanne Fribbins
EMEA Product Marketing Manager
British Standards Institution (BSI)

Suzanne Fribbins
BSI

Product Marketing Manager – Risk



Transition arrangements

- Transition arrangements in the UK have been determined by UKAS
- A transition period has been set – 2 years duration
- Registrations to the old standard will be permitted for 12 months (1 October 2014), after which only registrations to the new standard will be permitted
- Organizations working towards compliance with ISO/IEC 27001 can choose to either:
 - Be assessed against the 2005 version and transition with our other customers (as long as your visits are completed by 1 October 2014) OR
 - Certify direct to ISO/IEC 27001:2013

Transition arrangements

- Organizations that are certified with BSI to ISO/IEC 27001:2005 have been provided with:
 - A transition guideline
 - A transition timescale
- Transitions will be conducted during routine continuing assessment visit (CAV)

Free tools and resources



- Transition guide – Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013



- Mapping guide – Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013

- Webinar – The wait is over ...ISO/IEC 27001:2013 is here

Training

- ISO/IEC 27001:2013 Requirements (1 day)
- ISO/IEC 27001:2013 Implementer (2 days)
- ISO/IEC 27001:2013 Lead Implementer (3 days)
- ISO/IEC 27001:2013 Internal auditor (3 days)
- ISO/IEC 27001:2013 Lead auditor (5 days)
- Transition from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 (1 day)
- Lead Auditor Transition from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 (2 days)
- For more information visit www.bsigroup.com/training



New information security books now available

Do you need additional information to help you make the transition?

Whether you are new to the standard, just starting the certification process, or already well on your way, our books will give you a detailed understanding of the new standards, guidelines on implementation, and details on certification and audits – all written by leading information security specialists, including David Brewer, Bridget Kenyon, Edward Humphreys and Robert Christian.

Sample chapters are available

Find out more www.bsigroup.com/27books

Top tips for making the transition

- Make changes to your documentation to reflect new structure (as necessary)
- Implement new requirements
- Review effectiveness of current control set
- Assume every control may have changed
- Carry out an impact assessment
- Review transitional information provided by BSI

Questions?

