bsi.

...making excellence a habit.™

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

Introducing the 2013 revision of ISO/IEC 27001

INVESTORS IN PEOPLE

AWARDED FOR QUALITY · RELIABILITY · DISTINCTION UK Superbrands 2013

Outline

- Who is BSI?
- Status report
- Structure of ISO/IEC 27001
- How is ISO/IEC 27001 changing?
- Changes to control objectives and controls
- Transition arrangements

bsi.

Who is BSI? – 10 fast facts

Founded in 1901

Global independent business services organization

No owners/ shareholders … all profit reinvested into the business

Standards, assessment, testing, certification, training, software

National Standards Body in the UK

#1 certification body in the UK, USA & Korea

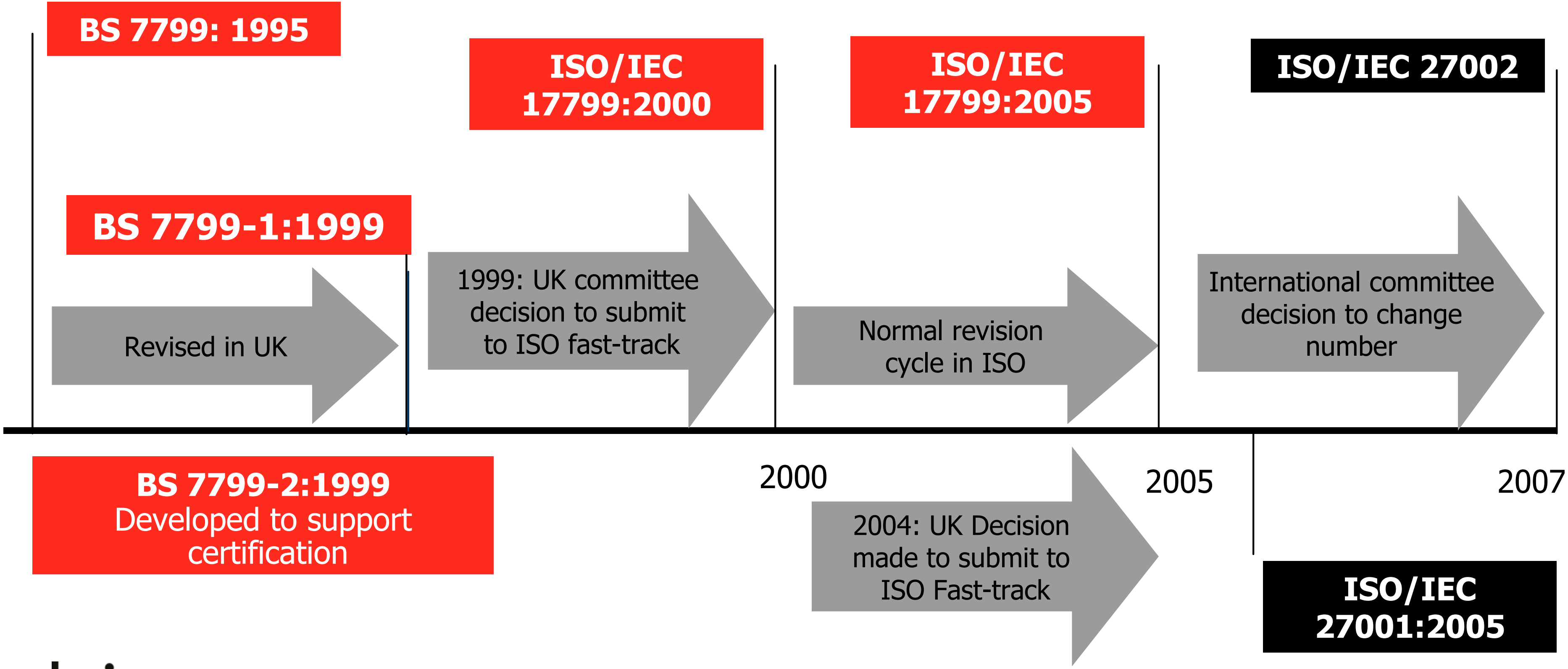
>2,900 staff and >50% non-UK

65 offices located around the world

70,000 clients in 150 countries

Trained over 73,000 people worldwide in 2012

ISO/IEC 27001 and 27002: Evolution



BS 7799: 1995

BS 7799-1:1999

Revised in UK

BS 7799-2:1999
Developed to support certification

ISO/IEC 17799:2000

1999: UK committee decision to submit to ISO fast-track

2000

ISO/IEC 17799:2005

Normal revision cycle in ISO

2004: UK Decision made to submit to ISO Fast-track

2005

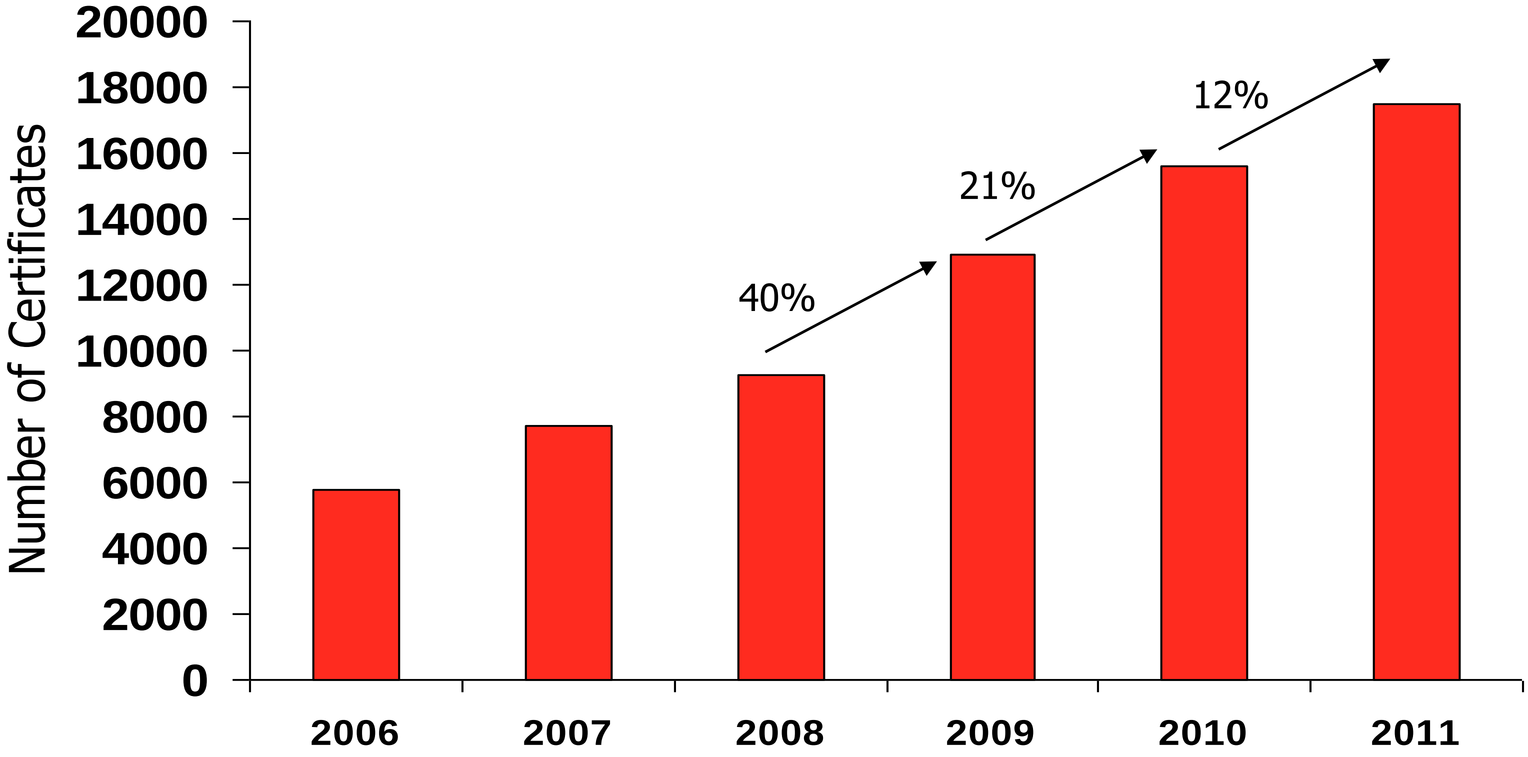
ISO/IEC 27002

International committee decision to change number

ISO/IEC 27001:2005

2007

Global growth in certification



Status report

- ISO/IEC 27001:2005 has been undergoing revision
- Draft International Standard (DIS) released to the National Standards Bodies on 16 January 2013
- Consultation closed 23 March 2013
- Draft International Standard (DIS) passed its DIS ballot at the meeting of the ISO Committee in April 2013
- The Final Draft International Standard (FDIS) was published on 9 July 2013
- The Final Draft Standard (FDIS) passed its FDIS ballot on 1 September 2013
- Both ISO/IEC 27001 and 27002 were published on 26 September

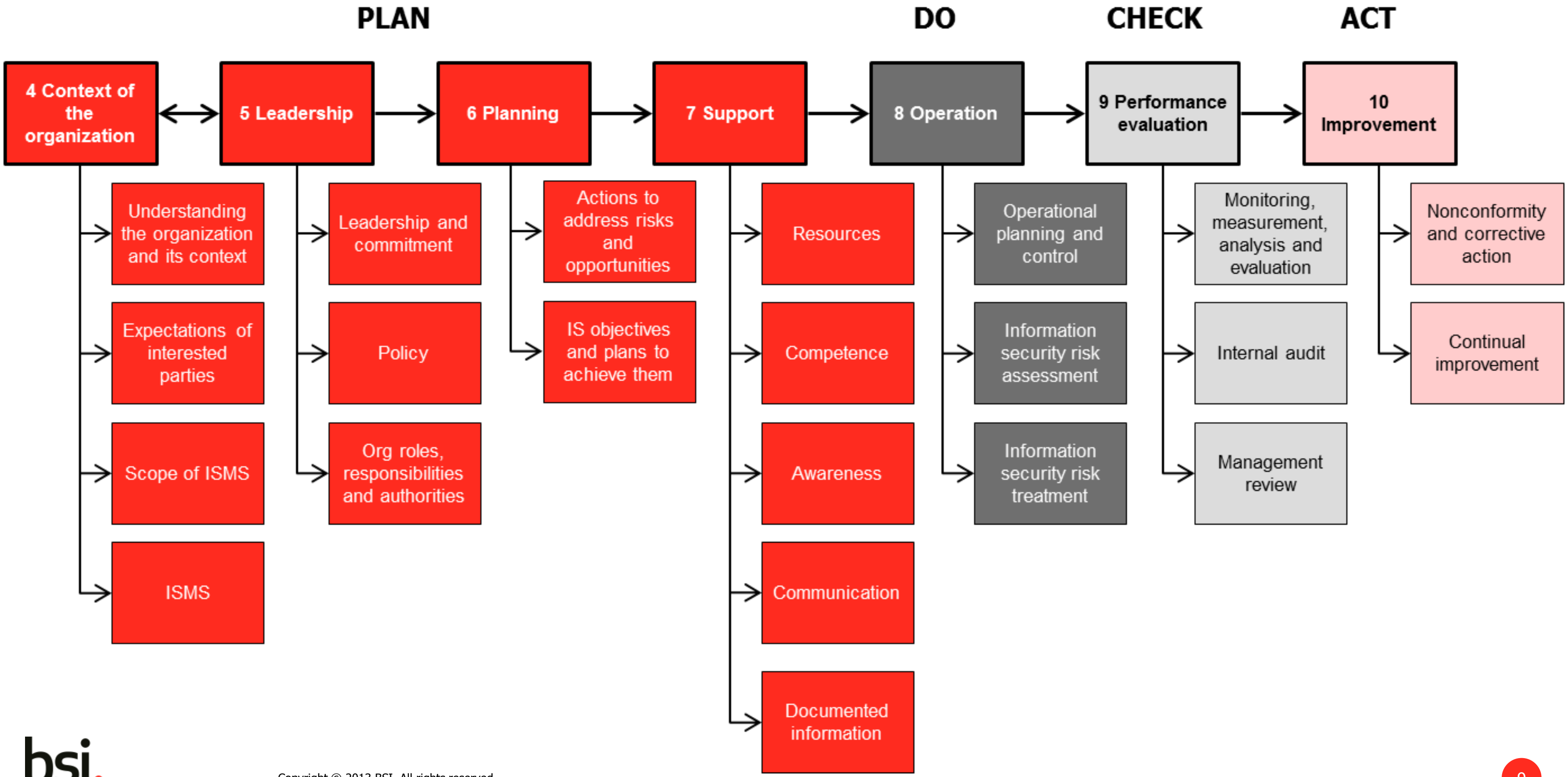
Key changes

- Standard has been written in accordance with Annex SL
- Does not emphasise Plan-Do-Check-Act cycle in same way as ISO/IEC 27001:2005
- Definitions in 2005 version have been removed and relocated to ISO 27000
- There have been changes to the terminology used
- Requirements for Management Commitments have been revised and are presented in the Leadership Clause
- Term preventive action has been replaced with "actions to address, risks and opportunities" and features earlier in the standard
- The risk assessment requirements are more general and are contained within clauses 6 and 8
- SOA requirements are similar but with more clarity on the determination of controls by the risk treatment process
- Greater emphasis on setting the objectives, monitoring performance and metrics
- The chapter on risk assessment and risk treatment has been relocated into section 6

New high level structure

- ISO/IEC 27001 has been developed using Annex SL
- Annex SL is for standards writers and provides a standardised text suitable for all ISO management system standards
- The new structure of the standard is to become common to all management system standards
- The intention is to standardise terminology and requirements for fundamental Management System requirements

ISO/IEC 27001:2013 structure

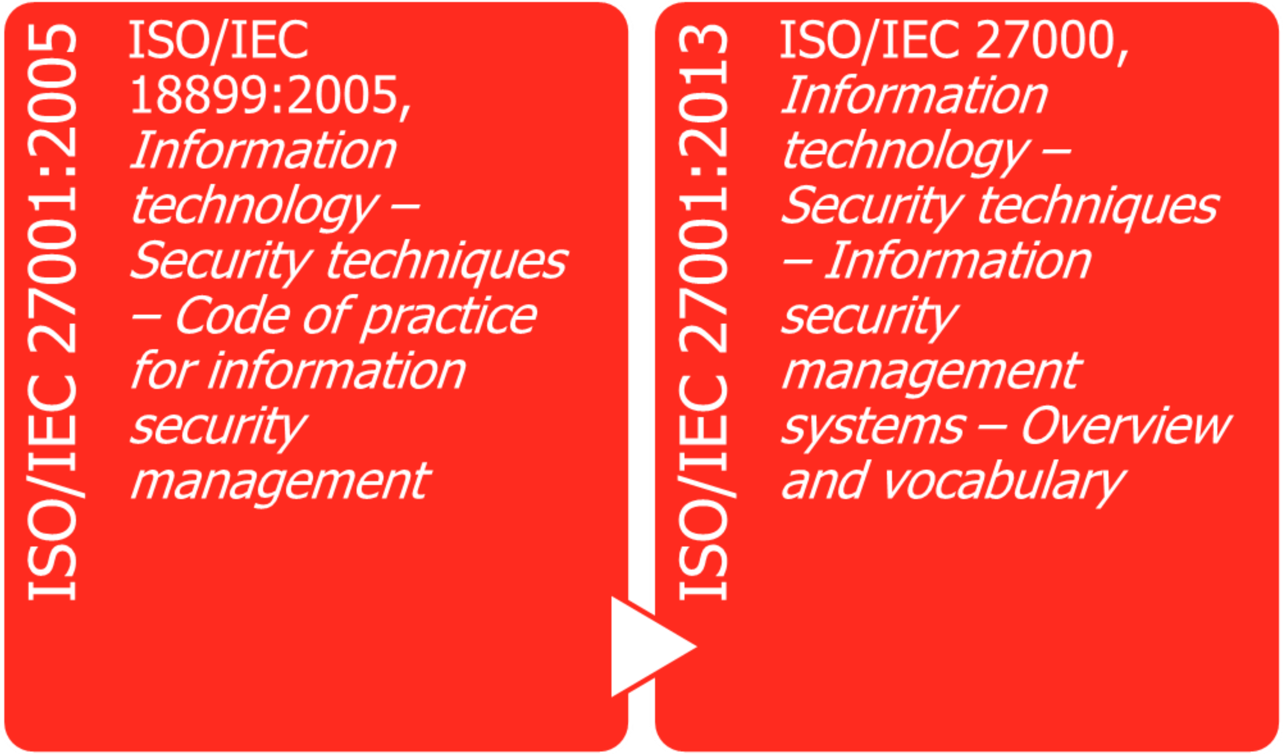

PLAN
DO
CHECK
ACT
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
Understanding the organization and its context
Expectations of interested parties
Scope of ISMS
ISMS
Leadership and commitment
Policy
Org roles, responsibilities and authorities
Actions to address risks and opportunities
IS objectives and plans to achieve them
Resources
Competence
Awareness
Communication
Documented information
Operational planning and control
Information security risk assessment
Information security risk treatment
Monitoring, measurement, analysis and evaluation
Internal audit
Management review
Nonconformity and corrective action
Continual improvement

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

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

bsi.

2. Normative references



ISO/IEC 27001:2005

ISO/IEC 18899:2005, *Information technology – Security techniques – Code of practice for information security management*

ISO/IEC 27001:2013

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3. Terms and definitions

- All of the definitions that were in the 2005 version have been removed
- Those that are still relevant have been relocated in ISO 27000
- Intention is to promote consistency of terms and definitions across the suite of ISO 27000 standards

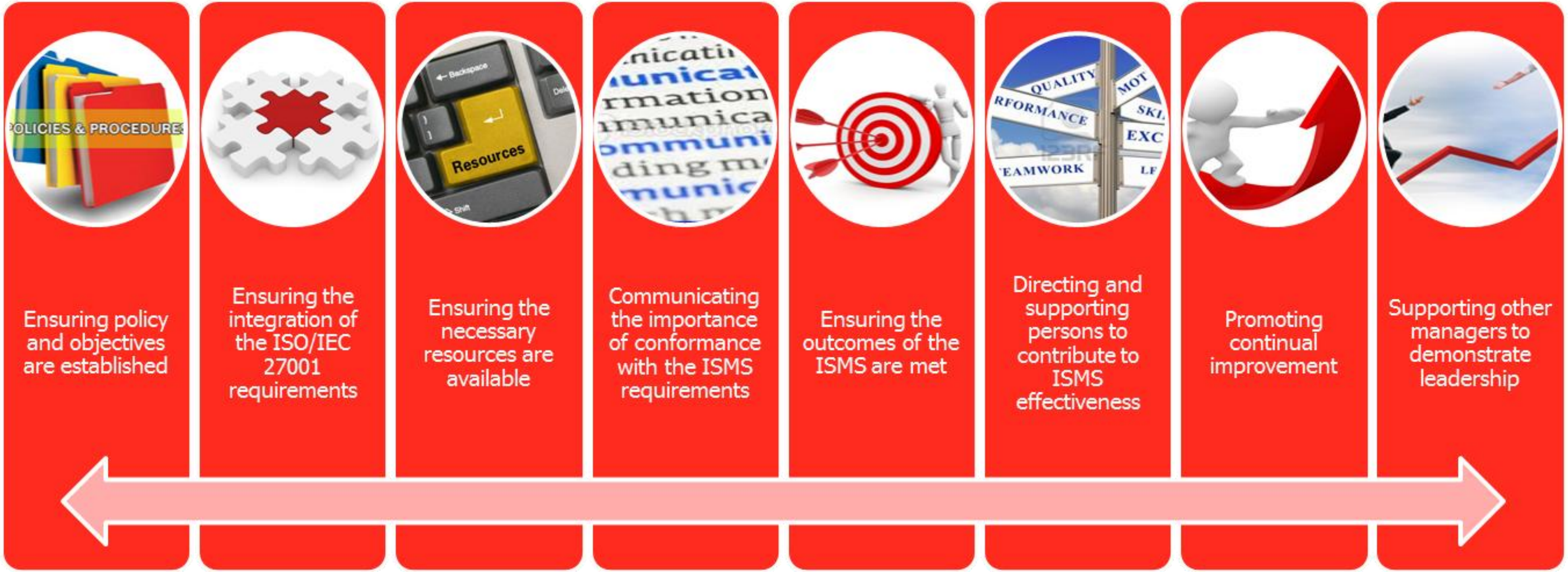
4. Context of the organization

- Clause 4 requires the organization to determine its external and internal issues
- There is a clear requirement to consider interested parties and their requirements
- The requirements of interested parties may include legal and regulatory requirements and contractual obligations
- This will determine its information security policy and objectives and how it will consider risk and the effect of risk on its business
- Consideration of an appropriate scope for the ISMS is required

5. Leadership

- Clause 5 of the standard summarizes the requirements specific to top management's role in the ISMS
- The new standard requires that top management leadership be more demonstrable and active
- ISMS policy now referred to as information security policy, however original policy requirements still present
- Clause 5 contains a requirement that top management ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated

How must management demonstrate its commitment?



Ensuring policy and objectives are established

Ensuring the integration of the ISO/IEC 27001 requirements

Ensuring the necessary resources are available

Communicating the importance of conformance with the ISMS requirements

Ensuring the outcomes of the ISMS are met

Directing and supporting persons to contribute to ISMS effectiveness

Promoting continual improvement

Supporting other managers to demonstrate leadership

6. Planning

- New section relating to establishment of 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 organizations information security objectives must be clearly defined with plans in place to achieve them
- The risk assessment requirements are more general reflecting an alignment of ISO/IEC 27001 with ISO 31000
- The changes to risk assessment are designed to make it easier for organizations to select from a wide range of methodologies
- The SOA requirements are largely unchanged

7. Support

- Clause 7 details the support 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

8. Operation

- ISO/IEC 27001 requires that organizations plan and control the operation of 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

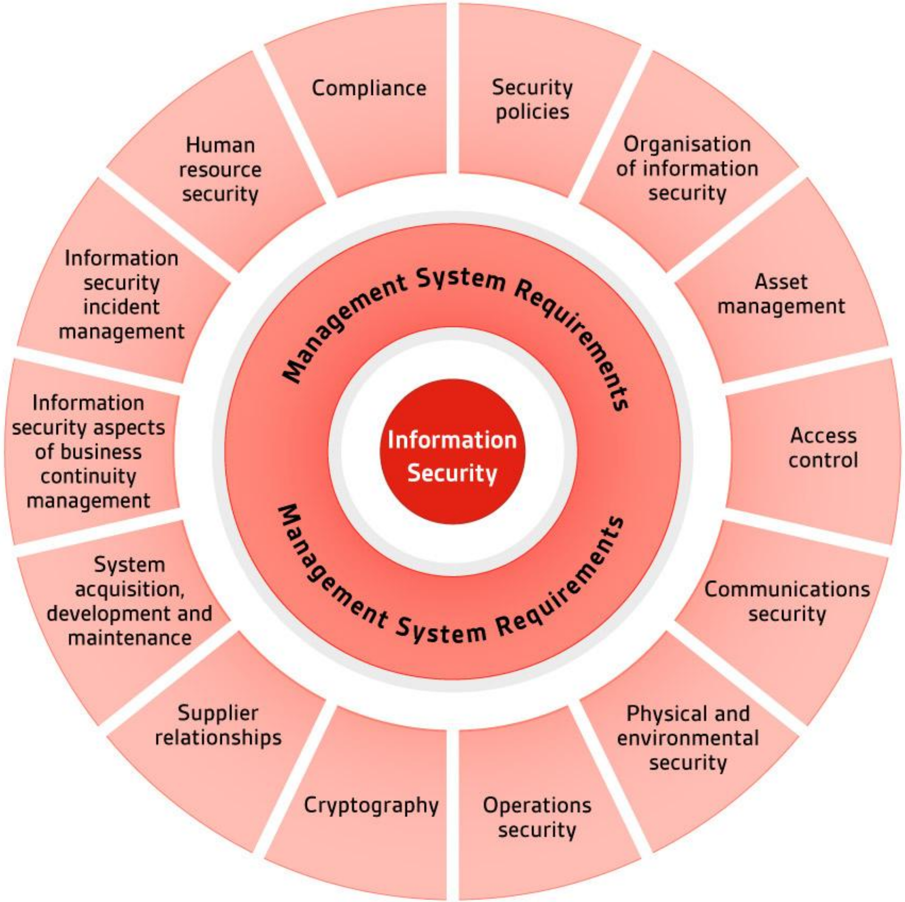
9. Performance evaluation

- 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

10. Improvement

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

Controls (Annex A and ISO/IEC 27002)


Compliance
Security policies
Organisation of information security
Asset management
Access control
Communications security
Physical and environmental security
Operations security
Cryptography
Supplier relationships
System acquisition, development and maintenance
Information security aspects of business continuity management
Information security incident management
Human resource security
Management System Requirements
Management System Requirements
Information Security

bsi.

New controls

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

Sample changed controls

2005	2013
Business continuity management (14)	Information security continuity (17)
External parties (6.2) and third parties (10.2)	Suppliers (15)
Electronic commerce services (10.9)	Application services (14.1.2, 14.1.3)
Malicious code (10.4.1)	Malware (12.2.1)

Mapping of control groups in Annex A

ISO/IEC 27001:2005		**ISO/IEC FDIS 27001:2013**	
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	Information systems acquisition, development and maintenance (12.3 only)	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

Summary of changes to ISO/IEC 27002

- Title has changed – Code of practice for information security controls
- Controls have been recorded and reduced – 133 to 114 controls
- Supporting text moved to implementation guidance (ISO 27003)
- Titles better matched to content
- Removal of term “contractors”
- Less prescriptive detail
  - Fewer lists
  - No specification of “essential” controls
  - No instructions for risk assessment/treatment

Top tips for making your transition to ISO/IEC 27001:2013

- 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

Transition arrangements

- Transition arrangements in the UK will be determined by UKAS and elsewhere by the national accreditation body
- A transition period will be set (likely one to two years duration)
- Registrations to the old standard will likely be permitted for a period of time after the new standard has been published, 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 within the next 12 months) OR
  - Certify direct to ISO/IEC 27001:2013

Transition arrangements

- Organizations that are certified with BSI to ISO/IEC 27001:2005 will be provided with:
  - A transition guideline
  - A transition timescale
- Widely expected that transitions will be conducted during planned assessment visits

Contact us

Dubai UAE:	+971 4 336 4917
Abu Dhabi UAE:	+971 2 443 9660
Qatar:	+974 44 29 2568 / 2569 / 2570

bsi.me@bsigroup.com

bsi.

...making excellence a habit.™