ISO/IEC 27001:2013 Launch Event

London

27 November 2013

Agenda

Time	Session
08.30-09.00	Registration
09.00-09.05	Welcome
09.05-09.45	**Introducing ISO/IEC 27001:2013 and ISO/IEC 27002:2013** Dr. Mike Nash, Gamma Secure Systems Limited
09.45-10.30	**Understanding the new ISO management system systems (high level structure)** Dr. David Brewer, IMS-Smart Ltd
10.30-10.45	**ISO/IEC 27001 Transition arrangements** Suzanne Fribbins, EMEA Product Marketing Manager – Risk
10.45-11.05	Morning tea and coffee break
11.05-11.35	**Security Information and Event Management** Robert Christian
11.35-12.05	**2013 Information Security Breaches Survey** Andrew Miller, Director, PricewaterhouseCoopers
12.05-12.35	**How criminals take advantage of the lack of security awareness** Simon Schofield, BAE Systems Detica
12.35-13.30	Complimentary networking lunch

Supported by:

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

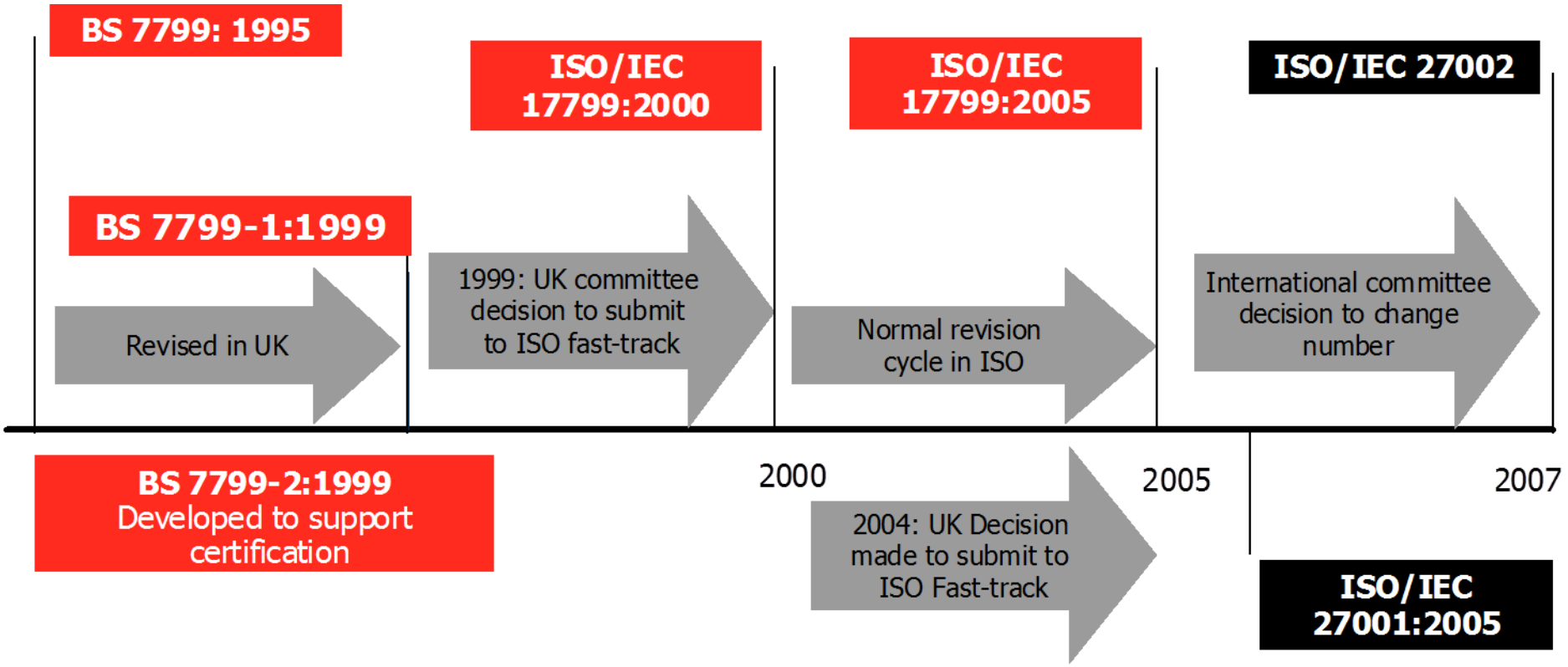
bsi.

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

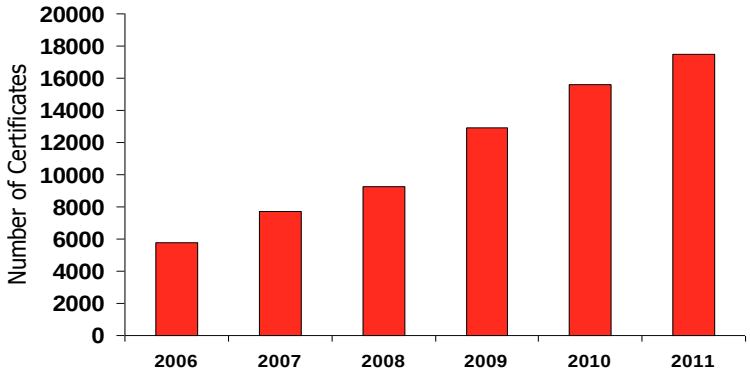


Supported by:

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



Supported by:

The result …

bsi.

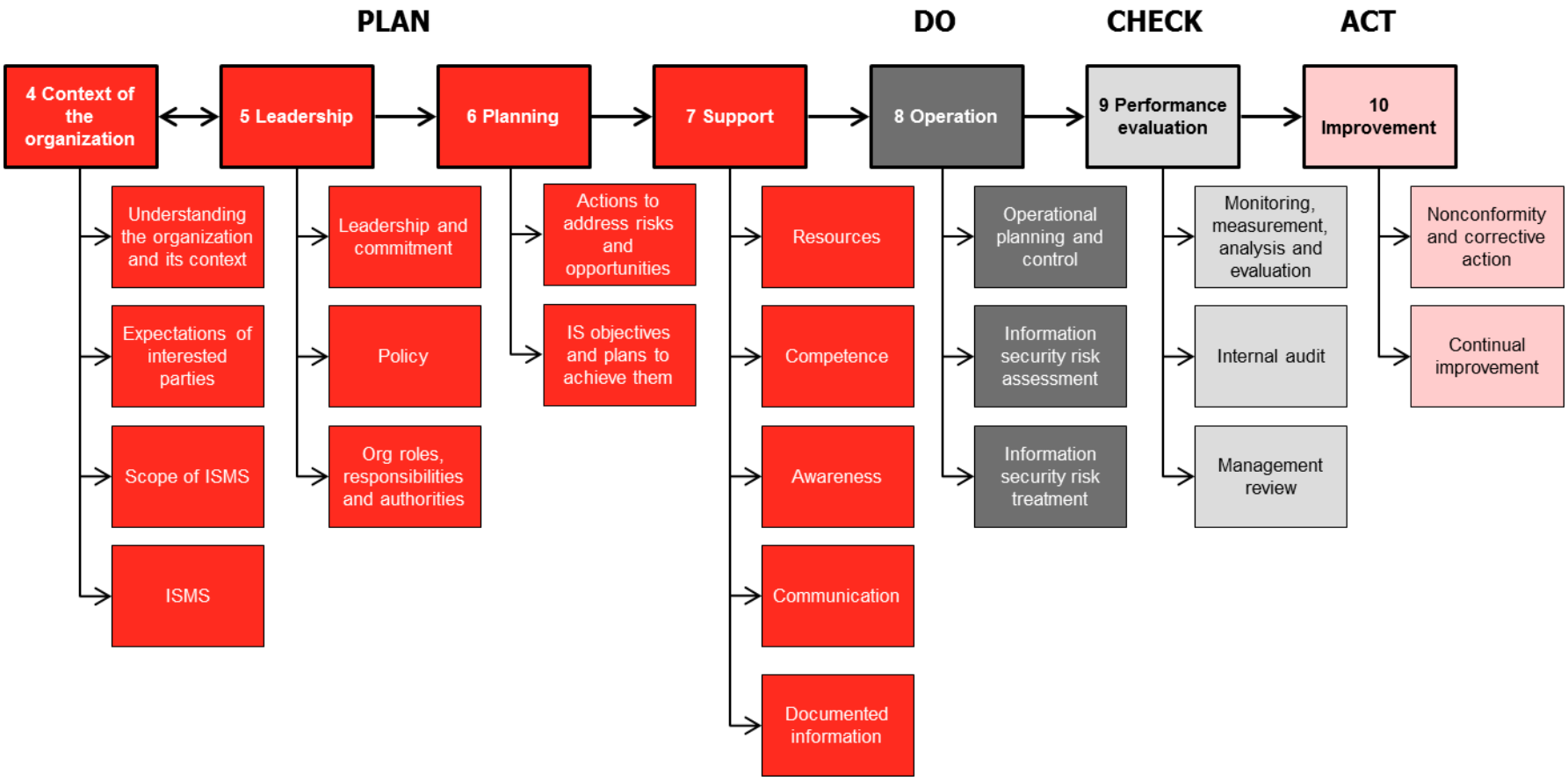
Supported by: pwc

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 will be included in ISO/IEC 27000
- Intention is to promote 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

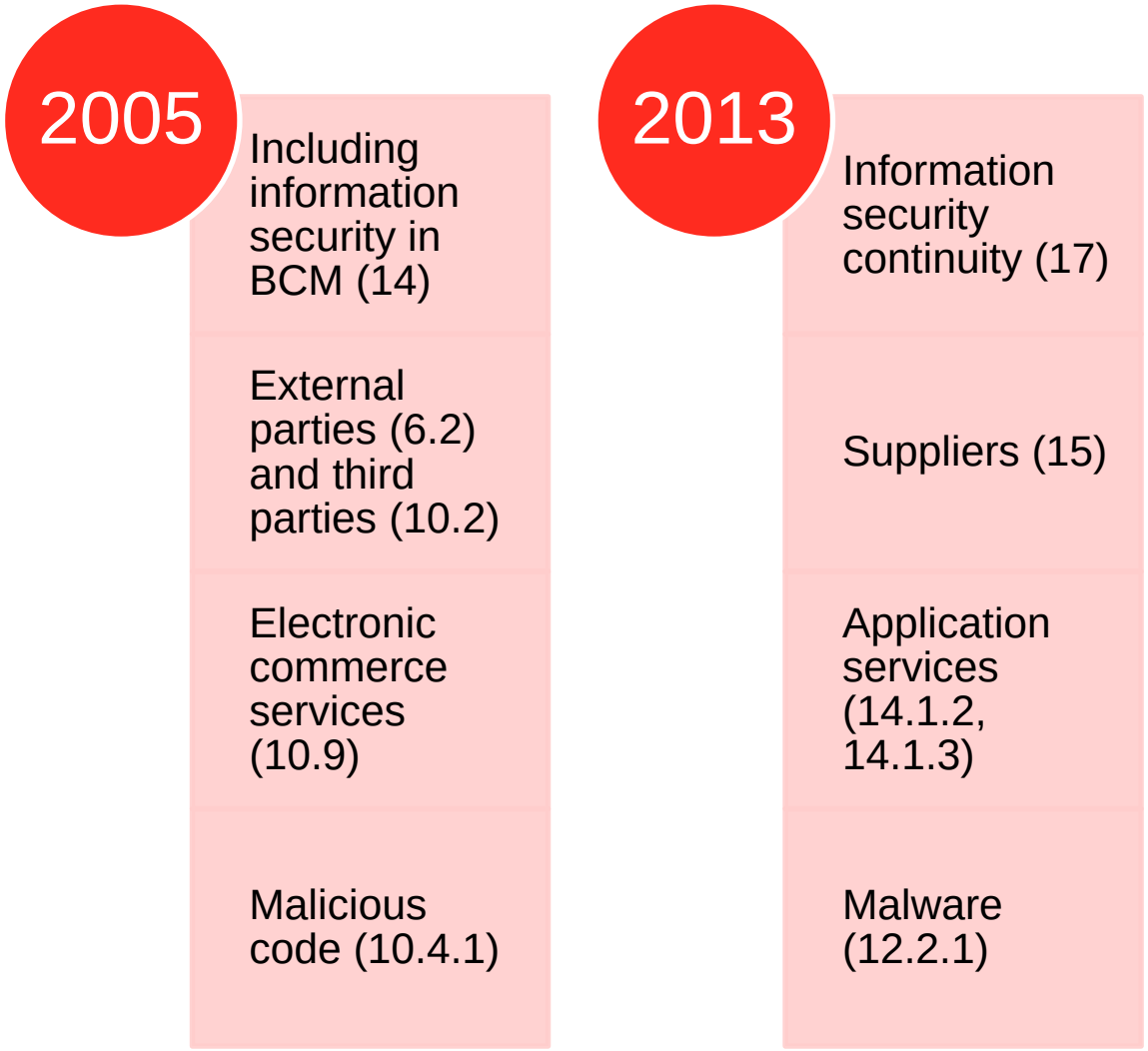
- Does not emphasise Plan-Do-Check-Act cycle in same way as ISO/IEC 27001:2005 did
- There have been changes to the terminology used
- The term "preventive action" has been replaced with "actions to address, risks and opportunities" and features earlier in the standard
- SOA requirements are similar 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

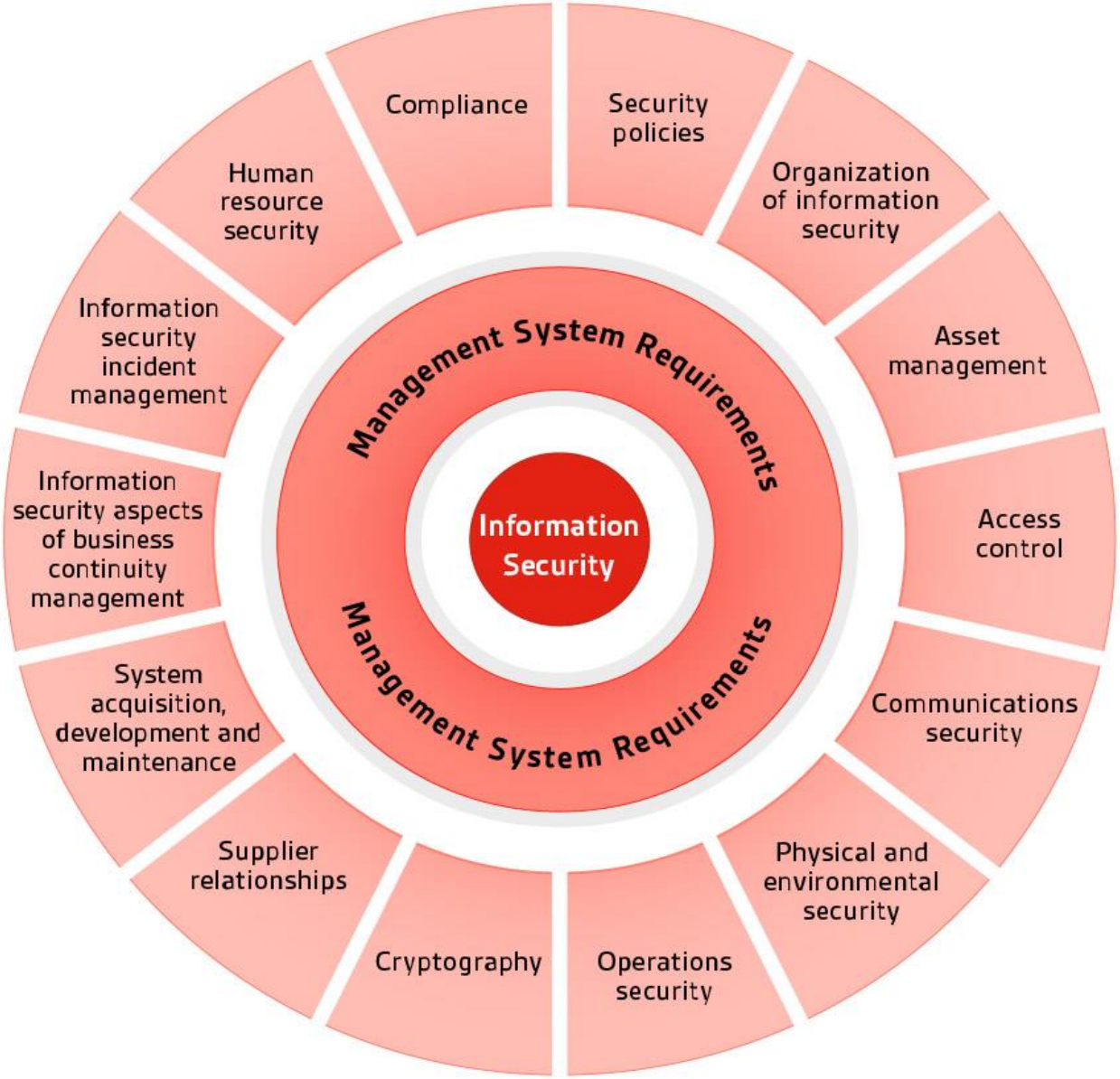
- New title - code of practice for information security controls
- Revised structure – more logical grouping of controls
- Changes to terminology to reflect industry changes
- Additional controls to reflect changes in security technology and advances in IT
- Some similar existing controls combined together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

Changes in emphasis and terminology



Supported by:

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, will be urgently updated
  - Again
  - Will contain a single set of definitions used by all 270xx Standards
- Inspection and audit standards will be updated
  - Update of ISO/IEC 27006 has already started
  - Important for supply chain inspection requirements
- 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
- Developing additional (free) information on changes and transition
- Copyright issues
- Payment issues
- Within ISO, overview and vocabulary standards are sometimes free-of-charge for download

Questions?

Supported by:

Dr. David Brewer
IMS-Smart Limited

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

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

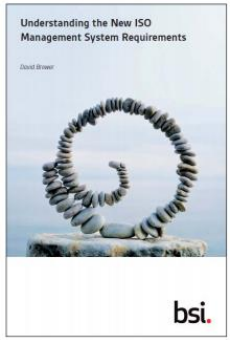
- Introductory remarks
- The new ISO directives
- Understanding the new requirements
- Transitioning to the new management system standards
- Summary

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:

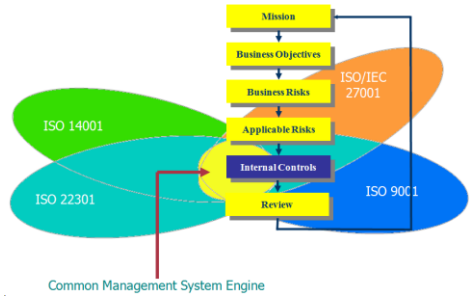


The new ISO directives

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

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

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:

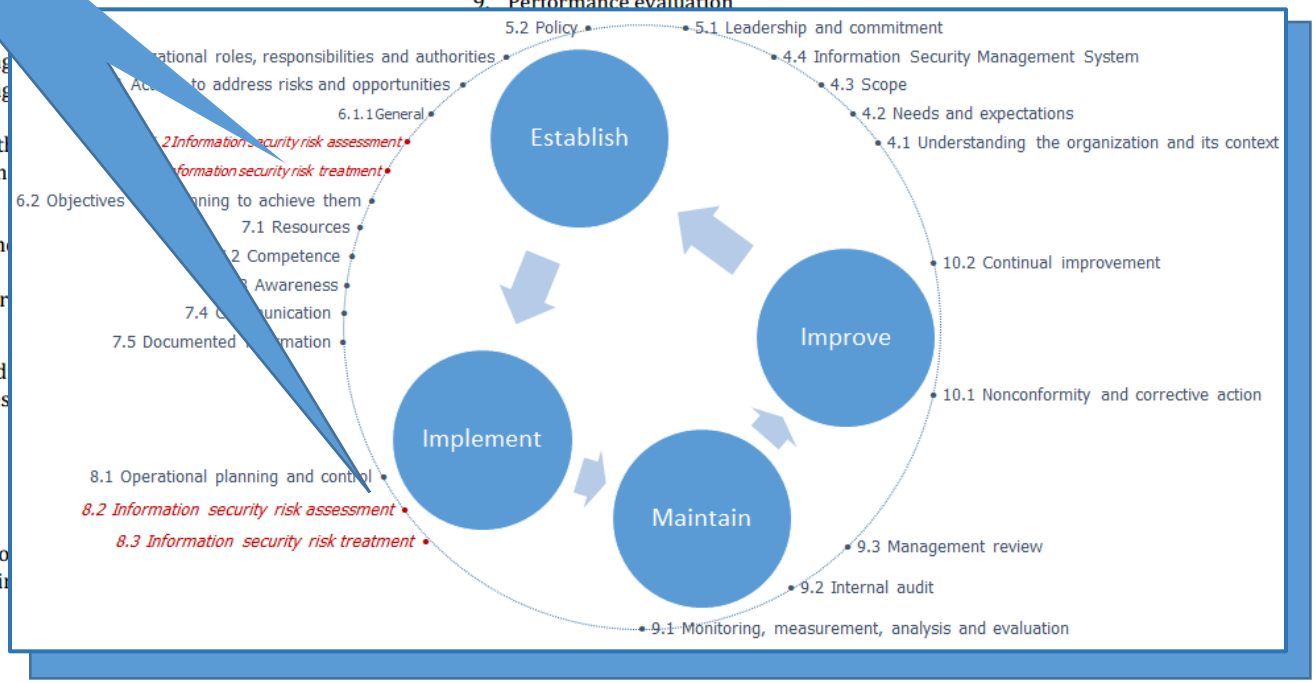
4.3	Scope of the ISMS	8.1	Operational planning and control
5.2	Information security policy	8.2	Results of the information security risk assessments
6.1.2	Information security risk assessment process	8.3	Results of the information security risk treatment
6.1.3	Information security risk treatment process	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 th
   - 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.

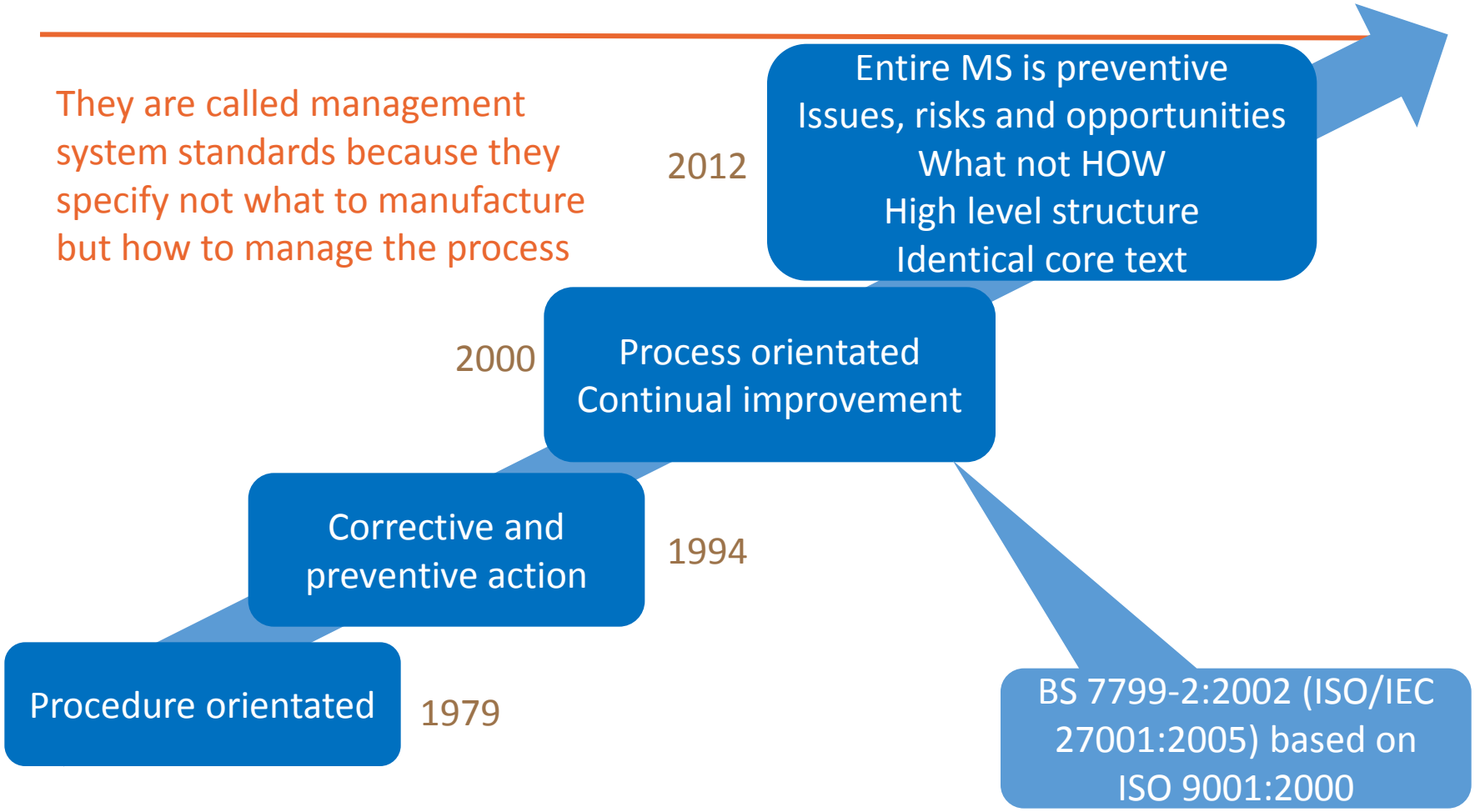
> **3.04**
> **management system**
> set of interrelated or interacting elements of an **organization** (3.01) to establish **policies** (3.07) and **objectives** (3.08) and **processes** (3.12) to achieve those objectives

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

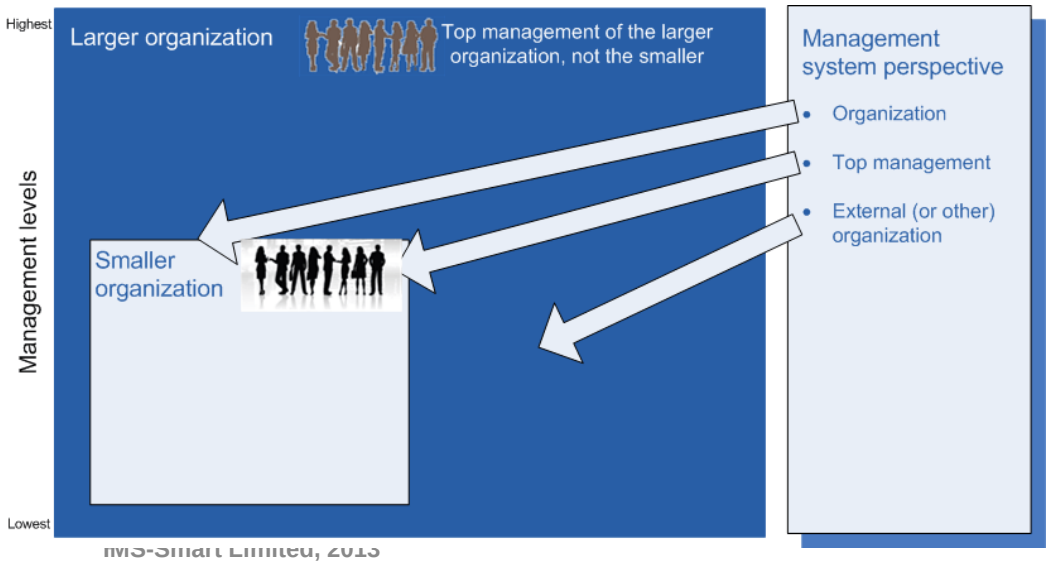
Scope of the management system

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

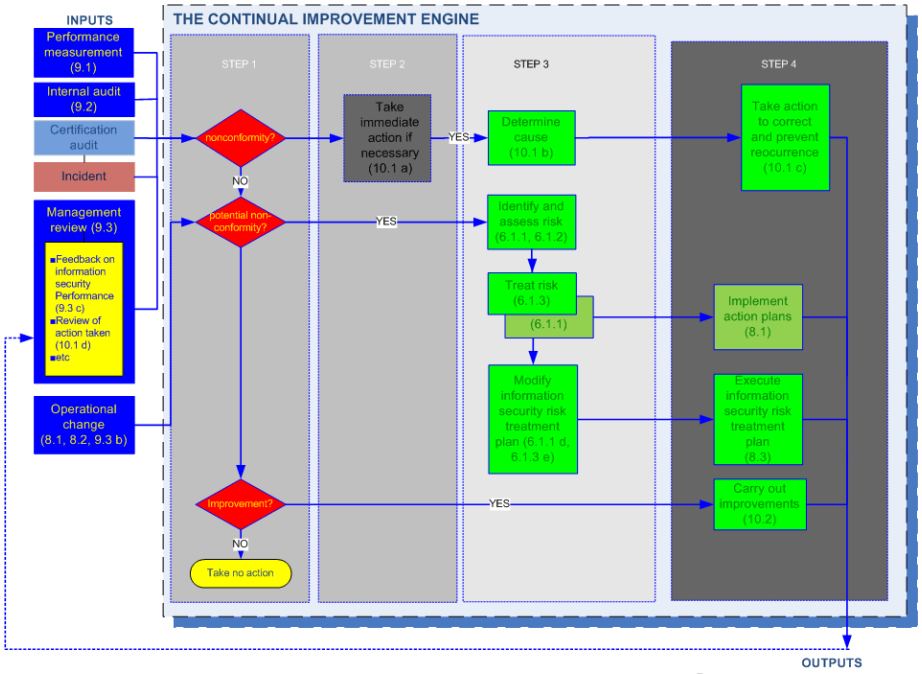
Actions to address risks and opportunities

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



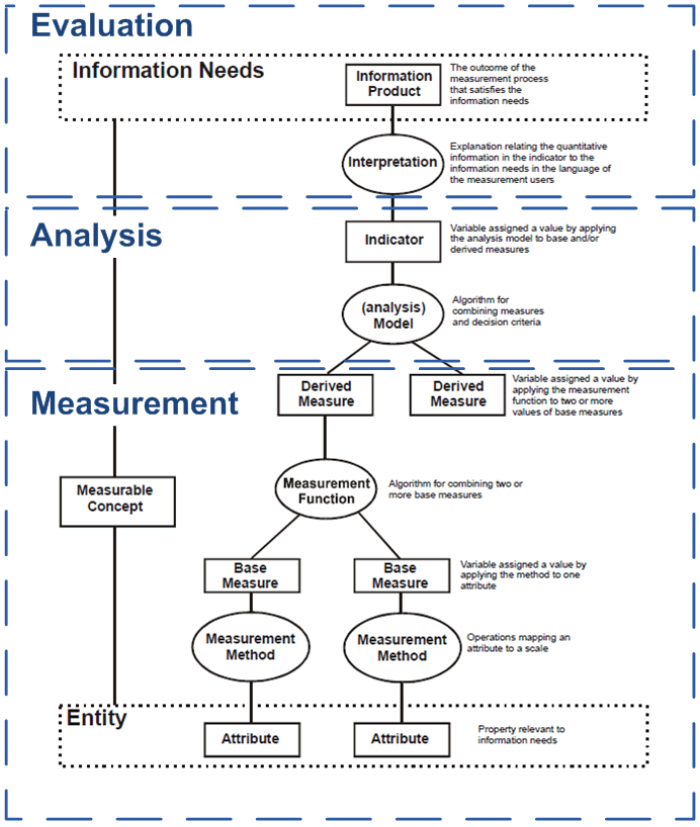
New requirements that may present a challenge

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

Questions?

Supported by:

ISO/IEC 27001:2005 to 2013 transition arrangements

Tim Sparey
UK Training Manager
British Standards Institution (BSI)

Transition arrangements

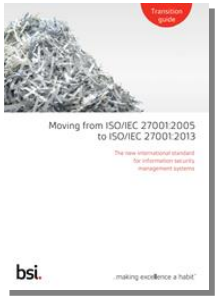
- Transition arrangements in the UK will be determined by UKAS and elsewhere by the national accreditation body
- A transition period of 24 months from the date of publication has been agreed
- Registrations to the old standard are permitted for a period of 12 months after the 2013 version publication date, after which all new accredited certifications issued will be to ISO/IEC 27001:2013
- Organizations working towards compliance with ISO/IEC 27001 can choose to either:
  - Be assessed against the 2005 version and transition at continuing assessment visits, 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

- Transitions will be conducted during planned assessment or re-assessment visits and will not incur the client any additional expenditure from an assessment perspective.

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

Supported by:

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?

Supported by:

Robert Christian

BSI / IST 33/ WG4 Network Security Lead and Editor ISO 27044: Guide to SIEM

ISO 27001 and SIEM

Robert Christian

BSI / IST 33/ WG4

Network Security Lead

&

Editor ISO 27044: Guide to SIEM

robert.christian@mac.com

07545 819560

AGENDA

- What is SIEM
- How does SIEM relate to ISO 27001
- How does SIEM relate to the ISO 27x (extended series)
- Summary

What is SIEM

- SIEM :

  Security Information and Event Management (System)

- ISO 27044 Guide to SIEM
  - Currently 2nd work draft

  " security information and event management

  SIEM *process in which electronic data is first aggregated, sorted according to specific categories and subsequently correlated*

  Note 1 to entry: The intent is to both reveal information security relevant incidents and to prioritize such information for further action." (ISO 27044, 2nd WD, 3.1)

What is SIEM


Data Collection
Normalistation
Analysis & Correlation
Alerting
Reporting
Storage

How does SIEM relate to ISO 27001

Information Security Management System (ISMS):

" …. The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. ….. "

(ISO/IEC FDIS 27001:2013(E))

How does SIEM relate to ISO 27001

" *A.16.1.4*

Assessment of and decision on information security events

Control

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. "

(ISO/IEC FDIS 27001:2013(E))

How does SIEM relate to ISO 27001

"A.16.1.6

Learning from information security incidents

Control

Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents."

How does SIEM relate to ISO 27001

" A.16.1.7

Collection of evidence

Control

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. "

(ISO/IEC FDIS 27001:2013(E))

How does SIEM relate to the the ISO 27x (extended series)

- ISO/IEC 27035 Security techniques – Information security incident management
  - Detecting and responding to information security events and incidents, as well as other phases of incident management

- ISO 27037: Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence
  - describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

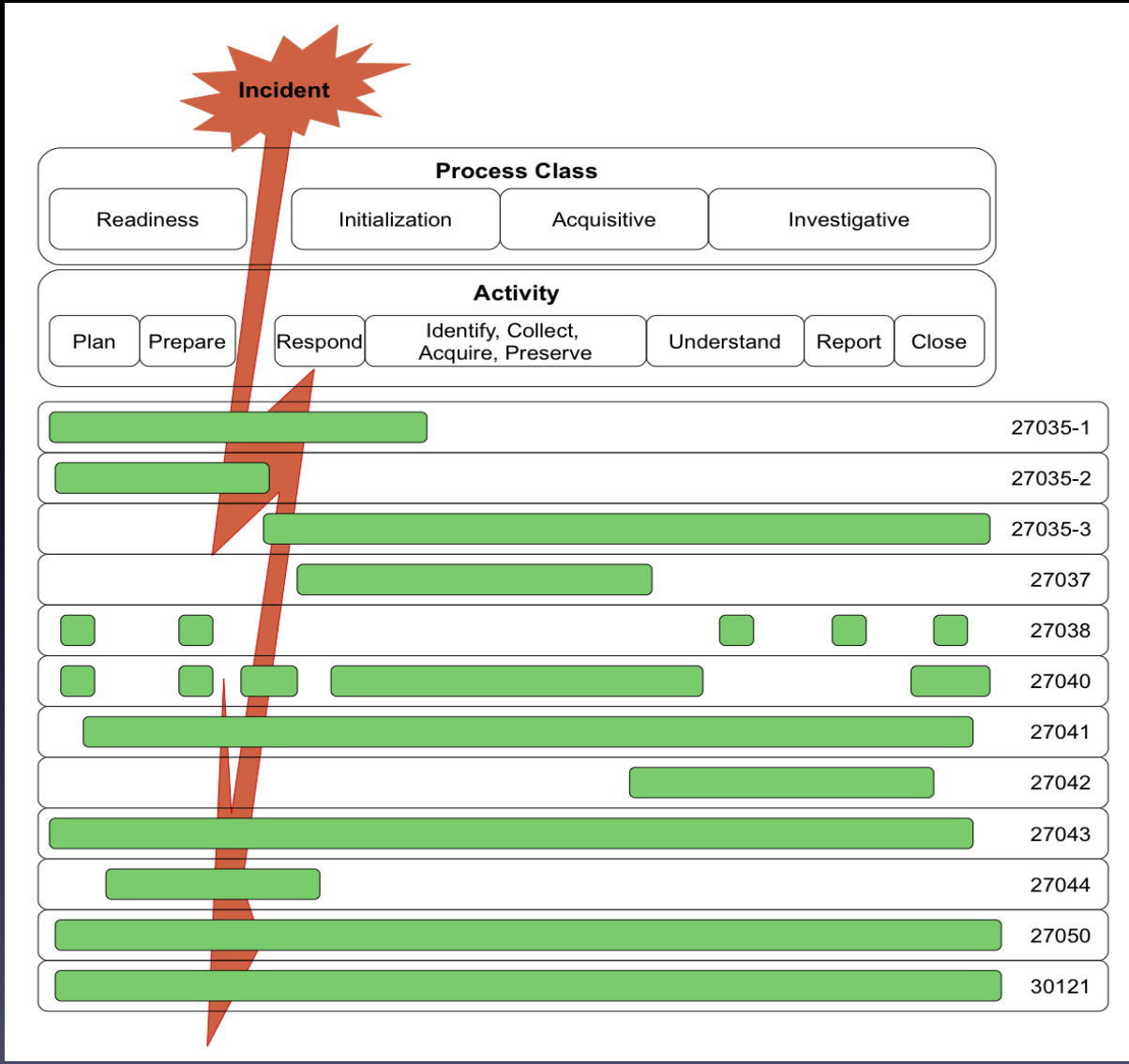
How does SIEM relate to the the ISO 27x (extended series)

- ISO 27033 Network security overview and concepts
- ISO 27039 Selection, deployment and operation of IDPS (Intrusion Detection & Prevention Systems)

How does SIEM relate to the the ISO 27x (extended series)

- ISO/IEC 27041: Guidance on Assuring the Suitability and Adequacy of Investigative Methods
- ISO/IEC 27042: Guidelines for the Analysis and Interpretation of Digital Evidence
- ISO/IEC 27043: Guidance on Investigation Principles and Processes

How does SIEM relate to the the ISO 27x (extended series)



Summary

- SIEM can be a very helpful element in creating and maintaining a ISMS
- SIEM compliments adjoining 27x standards
- SIEM selection, implementation and operation is a strategic element of information security

Questions?

Supported by:

Andrew Miller
PwC

Information Security Director

www.pwc.co.uk

Information Security Breaches Survey 2013

pwc

Agenda and contents

- **About the survey**
- **Security breaches increase**
- **External versus insider threats**
- **Understanding and communicating risks**
- **Implementation**
- **Key messages**

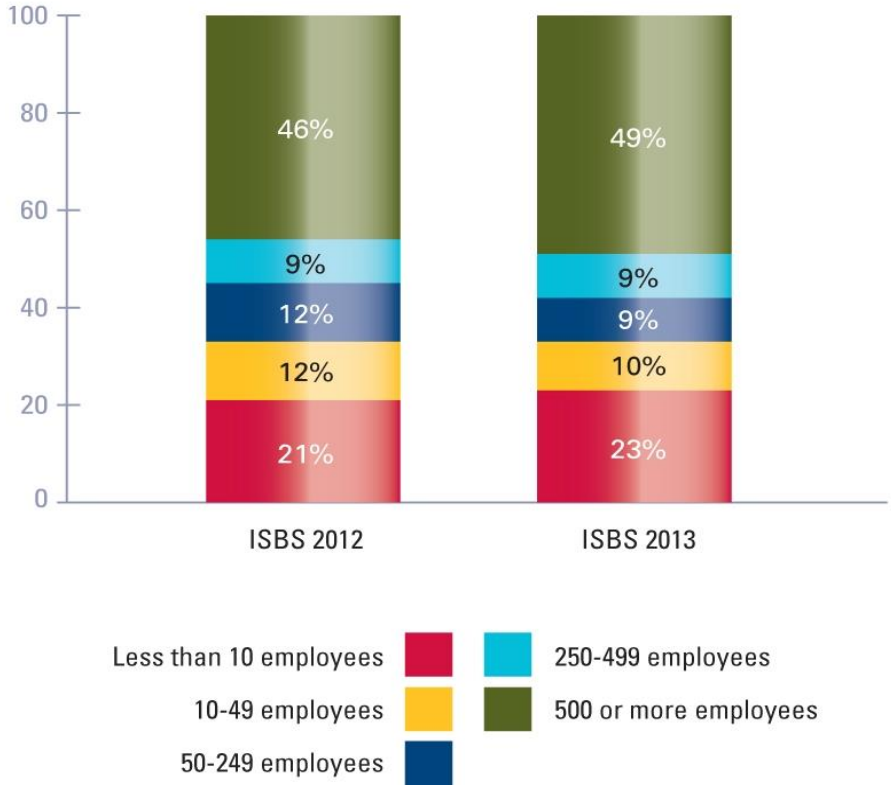
Andrew Miller

Information Security Director

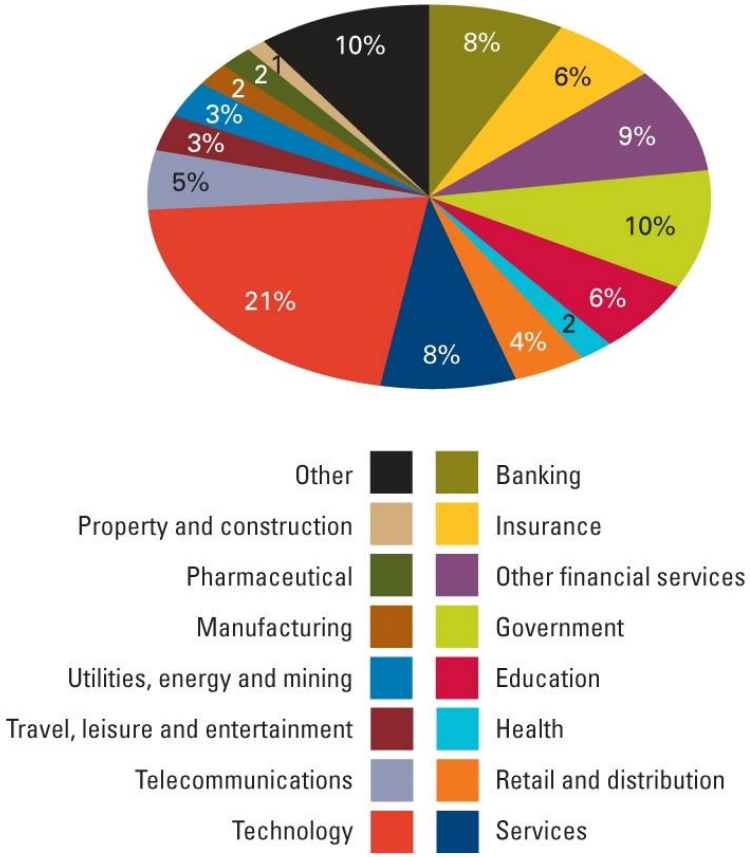
Full survey report is available from:
Department for Business, Innovation and Skills - www.gov.uk/bis
PricewaterhouseCoopers LLP - www.pwc.co.uk/informationsecurity
Infosecurity Europe – www.infosec.co.uk

- About the survey
- Security breaches increase
- External versus insider threats
- Understanding and communicating risks
- Implementation
- Key messages

Origin of data – Information Security Breaches Survey 2013?



(Based on 1,365 responses)



(Based on 1,402 responses)

Origin of data – Security Standards Survey?

Where is your organisation primarily located in the UK?

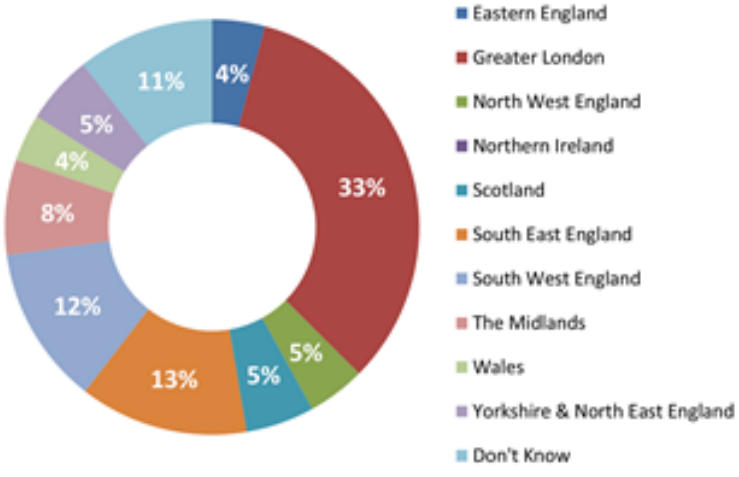


Figure 1 (based on 243 responses)

In which UK industry sector is your organisation?

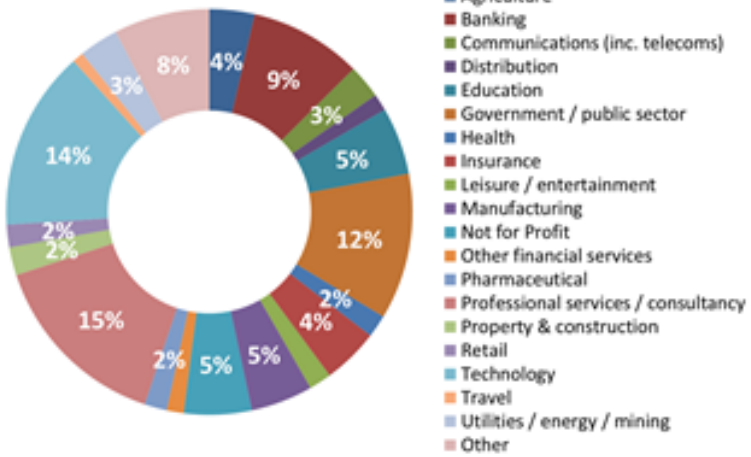


Figure 2 (based on 223 responses)

How many UK staff does your organisation comprise?

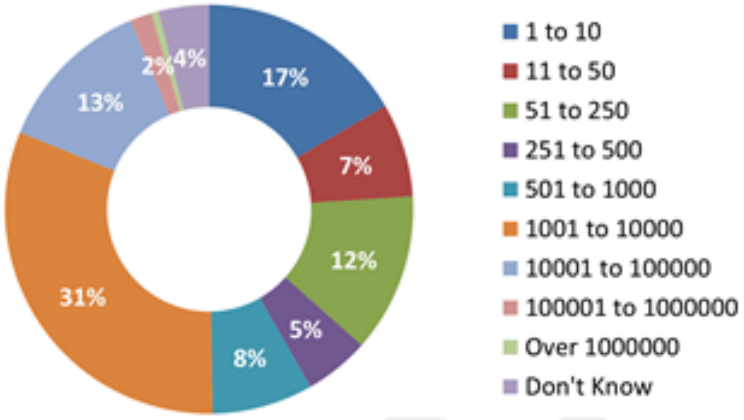


Figure 3 (based on 175 responses)

How old is your organisation in the UK?

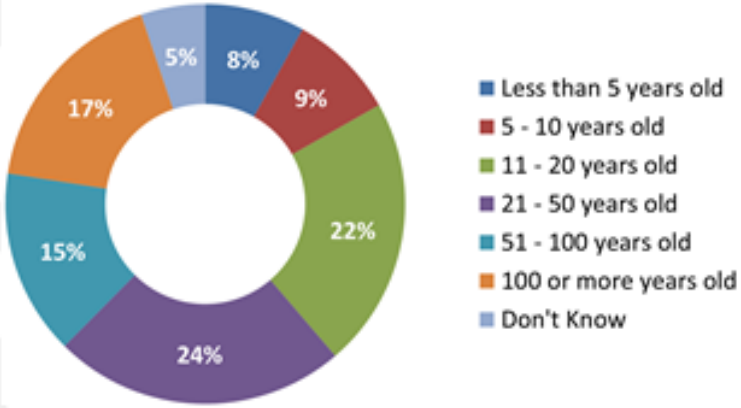


Figure 4 (based on 173 responses)

Thank you to all the organisations who supported this survey

- About the survey
- **Security breaches increase**
- External versus insider threats
- Understanding and communicating risks
- Implementation
- Key messages

Security breaches reach highest ever levels

Trend since 2012	Large organisations (more than 250 staff)	Small businesses (less than 50 staff)
% of respondents that had a breach	⟷	↑
Average number of breaches in the year	↑	↑
Cost of worst breach of the year	↑ ↑	↑ ↑
Overall cost of security breaches	↑ ↑	↑ ↑ ↑

Breaches and risks have never been higher

113	Median number of breaches suffered by a large organisation in the last year (71 a year ago)
17	Median number of breaches suffered by a small business in the last year (11 a year ago)
£450k-850k	Average cost to a large organisation of its worst security breach of the year
£35k-65k	Average cost to a small business of its worst security breach of the year
Billions	Estimated total cost to UK plc

Three times more than 2012

Breakdown of breaches - Median number suffered last year

93% large organisations had a security breach last year

87% small businesses had a security breach last year (76% a year ago)

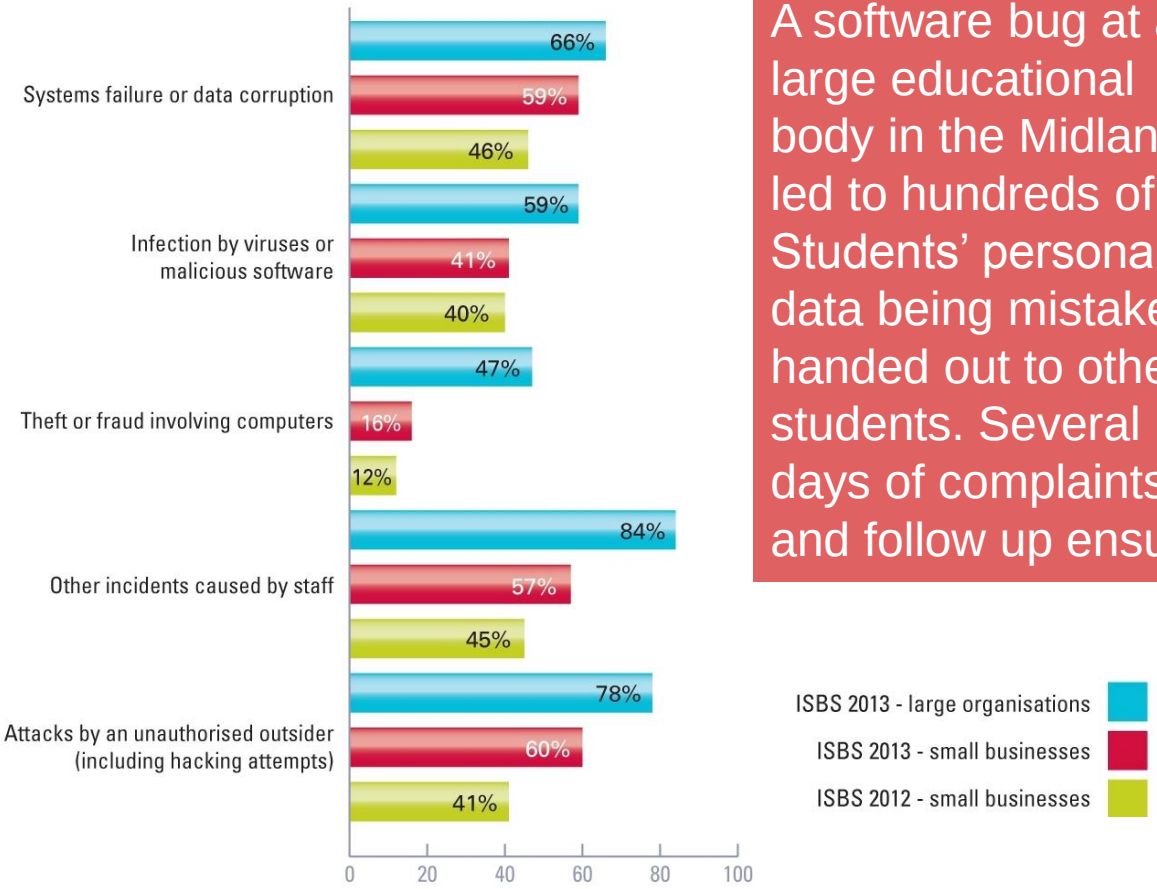
	Large organisations	Small businesses
Systems failure or data corruption	3 (3)	2 (2)
Infection by viruses or other malicious software	3 (3)	3 (1)
Theft or fraud involving computers	5 (5)	2 (3)
Other incidents caused by staff	18 (24)	11 (8)
Attacks by an unauthorised outsider (including hacking attempts)	106 (54)	10 (8)
Any security incident	113 (71)	17 (11)

(Based on 686 responses)

(Equivalent comparative statistics from ISBS 2012 shown in brackets)

Variations in type of breach witnessed last year

Failure to patch systems at a large bank led to an infection by the Poison Ivy backdoor. There was an effective contingency plan in place, but it still took several man-months of effort to eliminate the infection from systems. After the breach, procedures, (in particular for rolling out operating system patches) were improved.



A software bug at a large educational body in the Midlands led to hundreds of Students' personal data being mistakenly handed out to other students. Several days of complaints and follow up ensued.

(Based on 686 responses)

Impacts of breaches – Business disruption and financial loss

	ISBS 2013 small businesses	ISBS 2013 large organisations
Business disruption	£30,000 - £50,000 *over 3-5 days*	£300,000 - £600,000 *over 3-6 days*
Time spent responding to incident	£2,000 - £5,000 *6-12 man-days*	£6,000 - £13,000 *25-45 man-days*
Lost business	£300 - £600	£10,000 - £15,000
Direct cash spent responding to incident	£500 - £1,500	£35,000 - £60,000
Regulatory fines and compensation payments	£0	£750 - £1,500
Lost assets (including lost intellectual property)	£150 - £300	£30,000 - £40,000
Damage to reputation	£1,500 - £8,000	£25,000 - £115,000

- About the survey
- Security breaches increase
- **External versus insider threats**
- Understanding and communicating risks
- Implementation
- Key messages

Small businesses become an increasing target for internal and external threats

63%	Of small businesses were attacked by an unauthorised outsider in the last year (41% a year ago)
23%	Of small businesses were hit by denial-of-service attacks in the last year (15% a year go)
15%	Of small businesses detected that outsiders has successfully penetrated their network in the last year (7% a year ago)
9%	Of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year

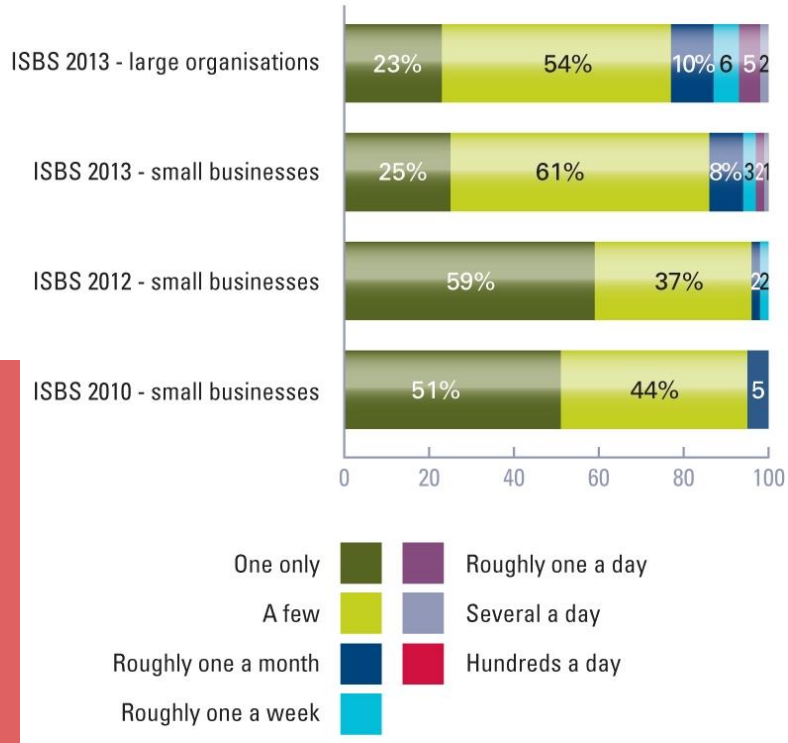
Internal and external threats remain a concern in large organisations

78%	Of large organisations were attacked by an unauthorised outsider in the last year (71% previous year)
39%	Of large organisations were hit by denial of service attacks in the last year (30% previous year)
20%	Of large organisations detected that outsiders had successfully penetrated their network in the last year (15% previous year)
14%	Of large organisations know that outsiders have stolen their intellectual property confidential data in the last year (12% previous year)

Infection by viruses and malicious software

Virus infection rate stabilised; but many businesses still catching themselves out.

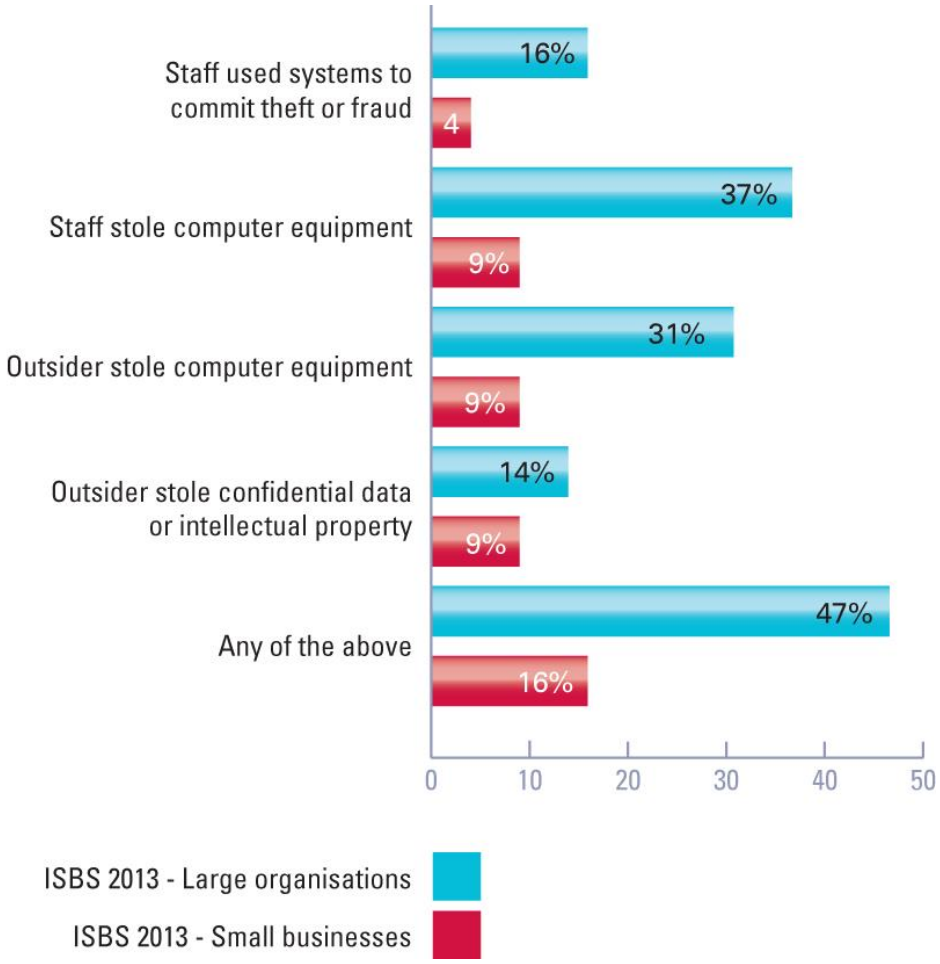
Many have left themselves vulnerable by not applying patches



An unpatched system at a large agricultural business in the South-East became infected by the Conficker worm. Routine security monitoring picked it up immediately and an effective contingency plan kicked in. As a result, the business disruption was minor and dealt with within a day.

(Based on 656 responses)

Internal risks are on the increase



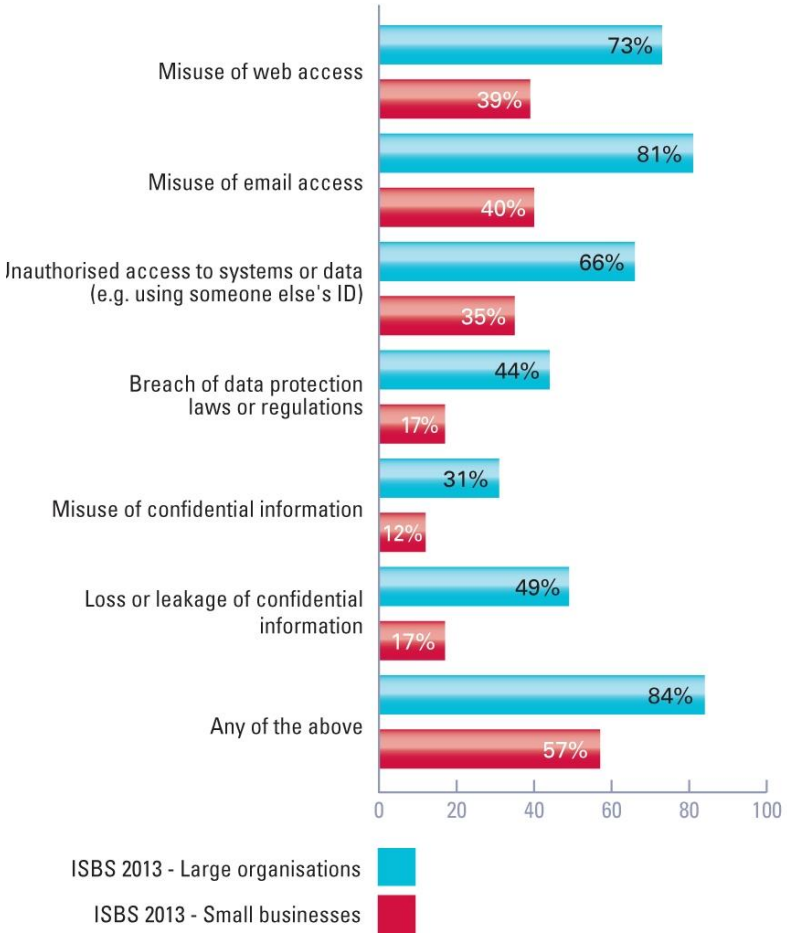
(Based on 551 responses)

A disgruntled employee at a large utility company stole some sensitive information which he had access to as part of his job and began selling this. The breach was discovered by accident, over a month after it started. The value of the lost data was several thousand pounds, but the impact on the business of the investigation and aftermath was even greater. The lack of contingency plan contributed to this cost. After the breach, the company deployed new systems, changed its procedures and introduced a formalised post-incident review process.

Staff related incidents increase significantly in the last year

Staff related breaches remains relatively high levels with particular increases in small businesses reporting staff misuse of the Internet or email. The average affected company had about one breach a month

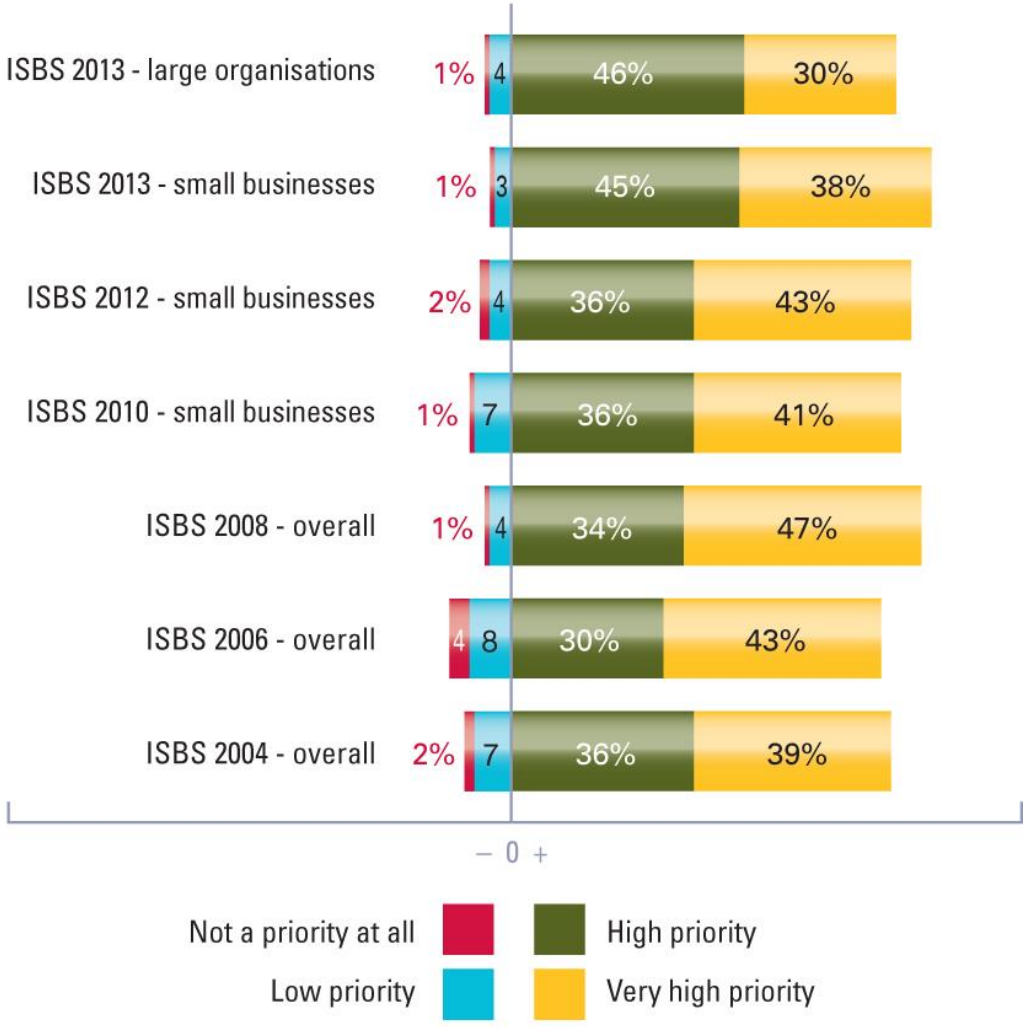
A member of staff at a small security consultancy firm accidentally replied to all recipients of an email with an inappropriate response. This small mistake resulted in several thousand pounds of lost business, and consumed several days of management time dealing with the complaints from customers. The employee was disciplined and additional staff training was implemented.



(Based on 528 responses)

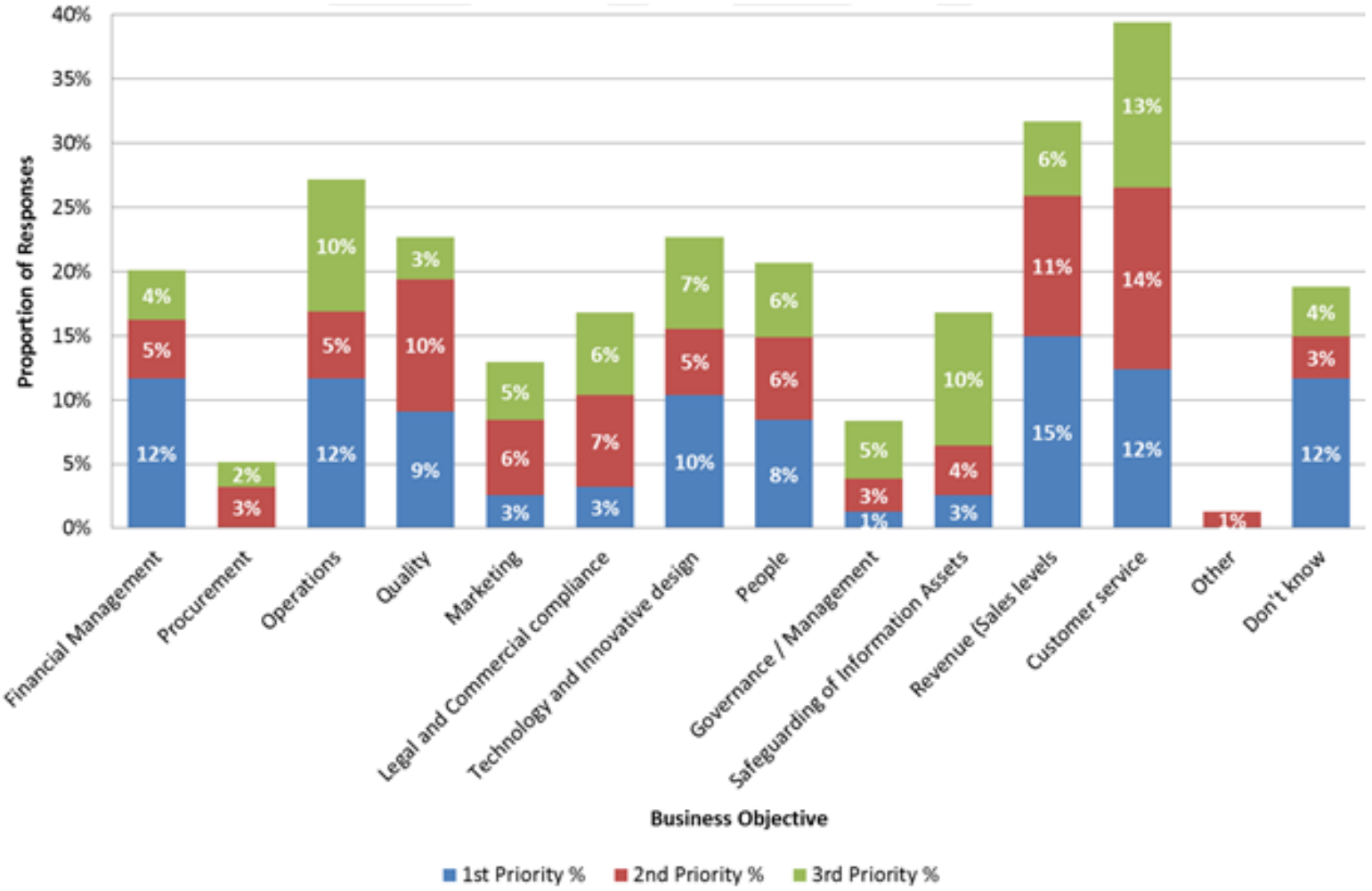
- About the survey
- Security breaches increase
- External versus insider threats
- **Understanding and communicating risks**
- Implementation
- Key messages

Priority given to security by senior management



(Based on 1,204 responses)

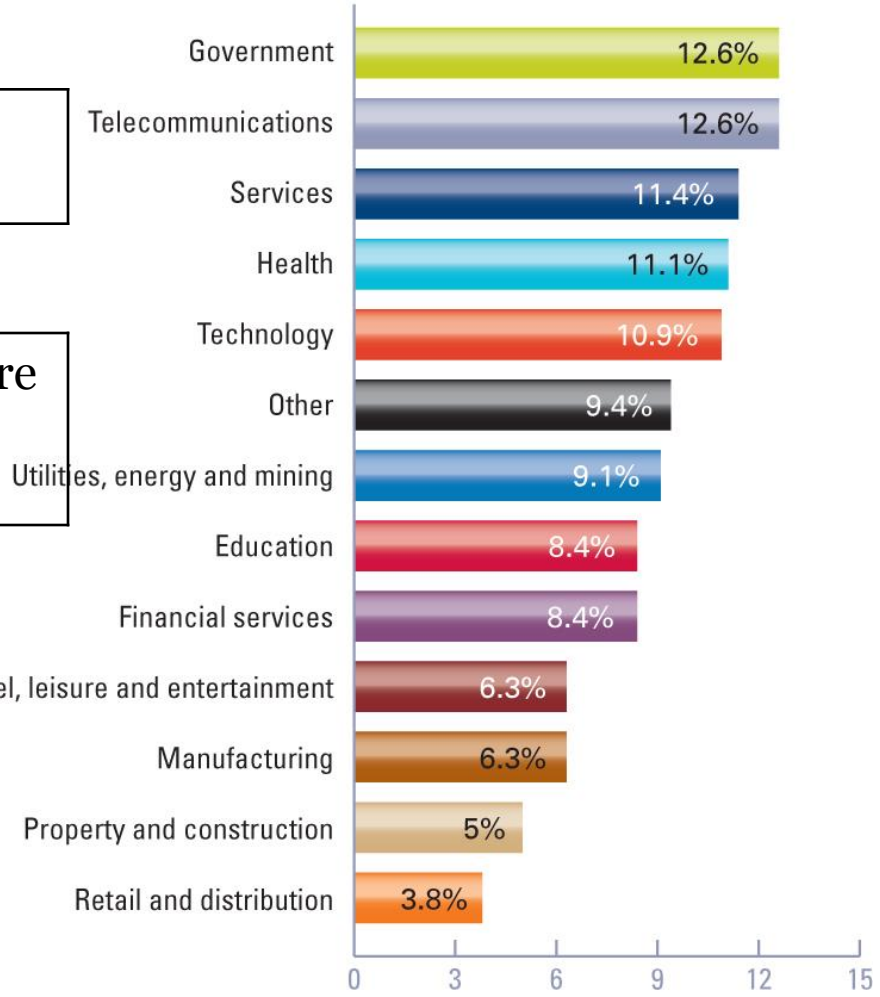
Prioritisation of protecting information assets



Security expenditure by sector

10%	is the average spent on security up from 8% a year ago.

16%	is the average spent on security where security is a very high priority. Up from 11% a year ago



(Based on 845 responses)

Translation into effective security defences.

93% of companies where security policy was poorly understood had staff related breaches (versus 47% where policy was well understood)

42% of large organisations don't provide any ongoing security awareness training to their staff (10% don't even brief staff on induction)

26% of respondents haven't briefed their board on security risks in the last year (19% never done so)

33% of large organisations say responsibilities for ensuring data is protected aren't clear (only 22% say they are very clear)

32% of companies don't evaluate the effectiveness of their security expenditure at all.

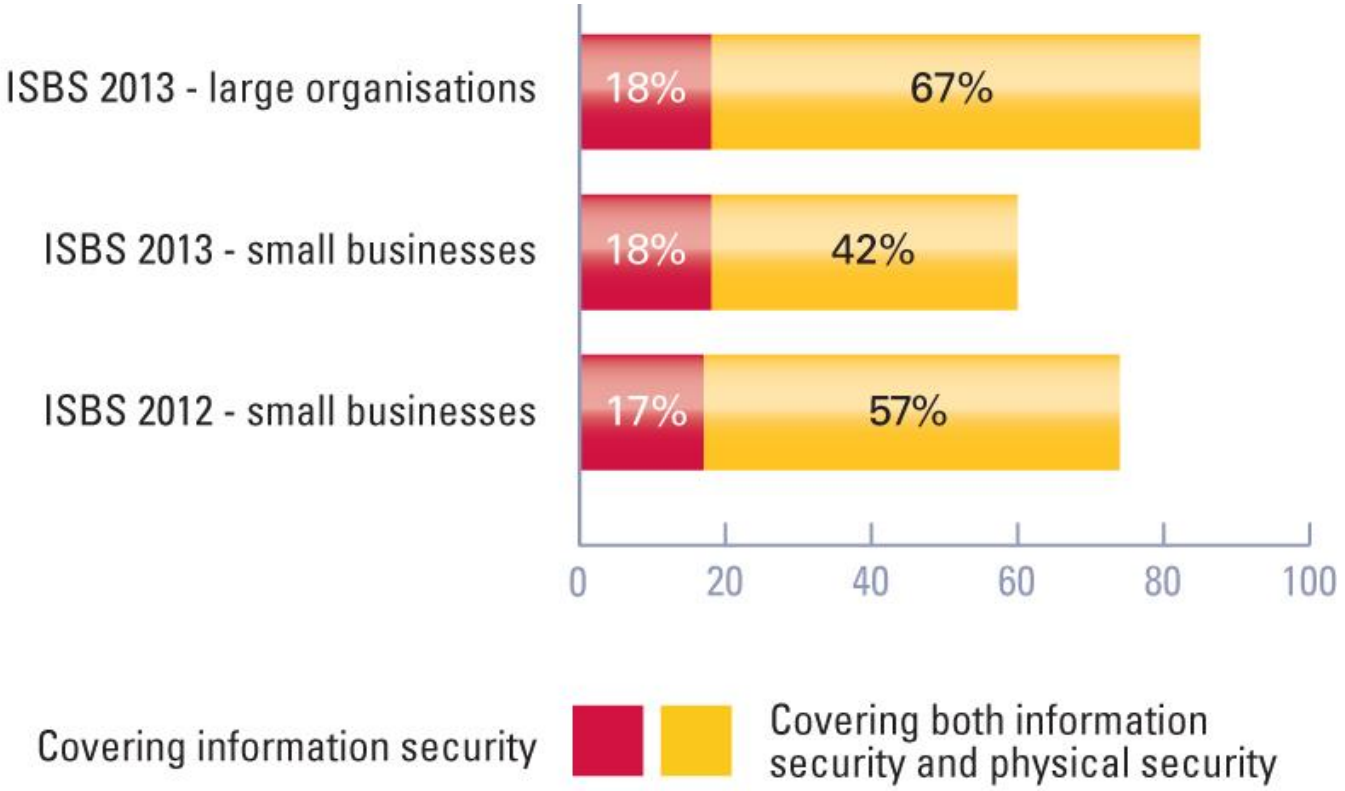
Investment versus overhead

(Based on 164 responses)

Lack of progress in treating security as an investment rather than overhead.

12% of organisations try to calculate return on investment on their security expenditure - worse than 2012 and significantly worse than 2004 (39%)

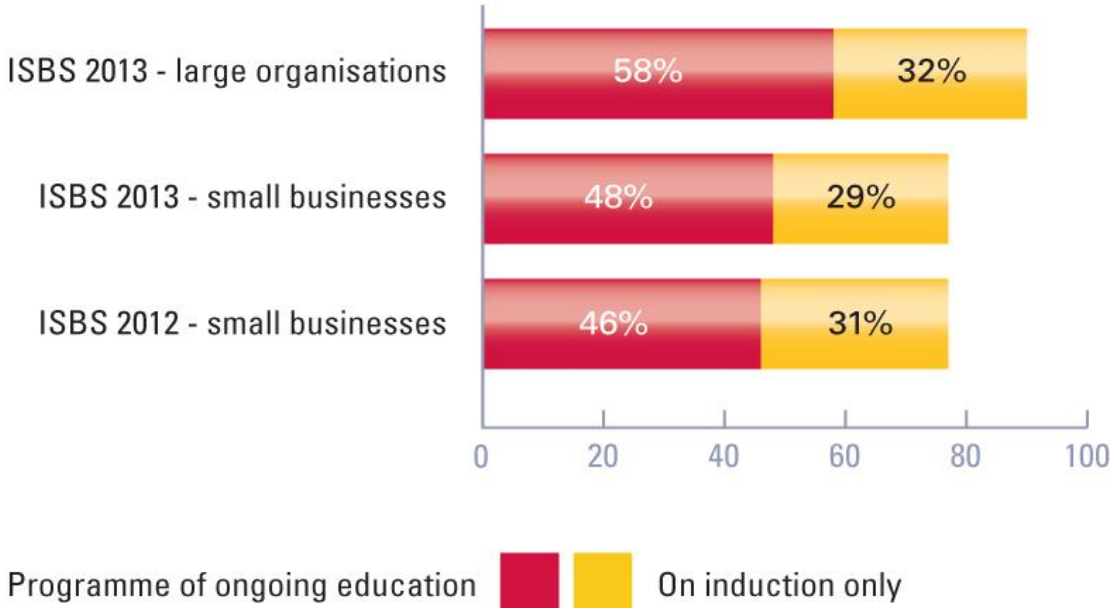
How many organisations carry out security risk assessment?



(Based on 146 responses)

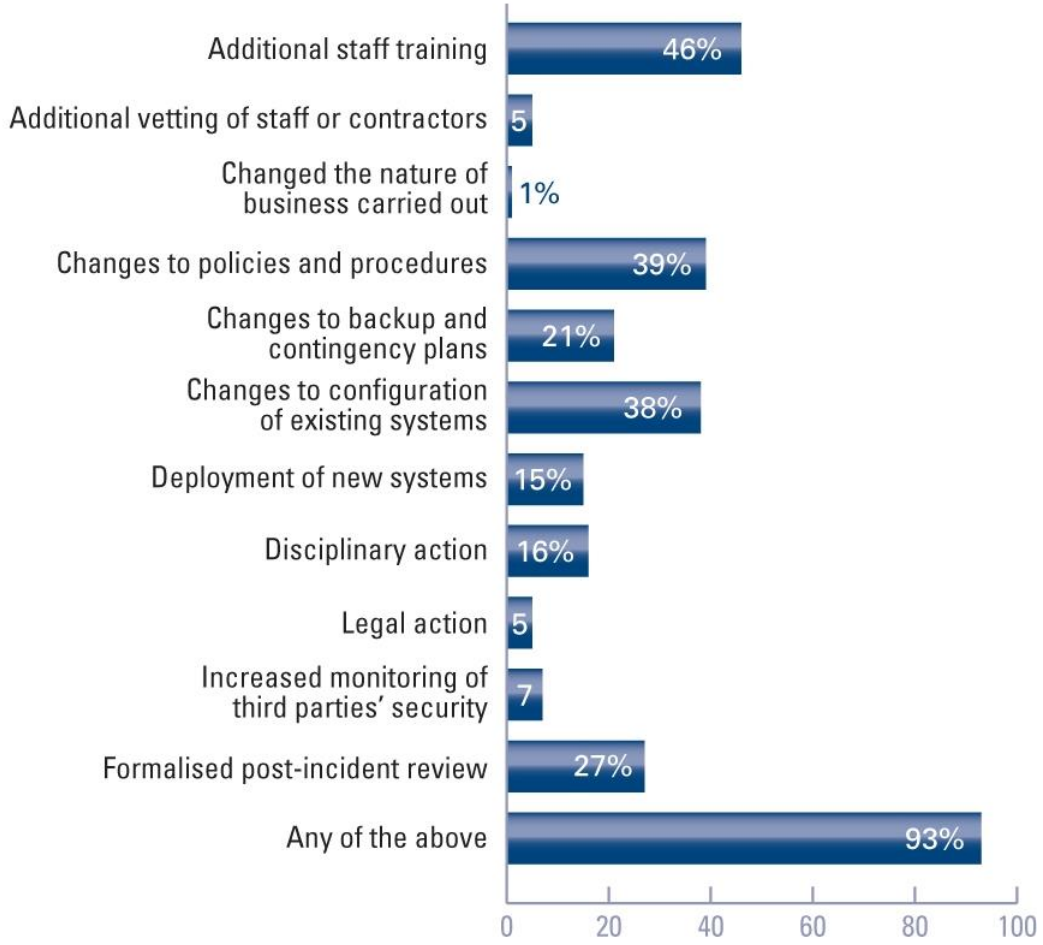
Communicating security risks to staff

A large technology company suffered when one of their customers decided to carry out an unauthorised destructive penetration test on their systems. This took down systems and led to customer complaints. Fortunately, the breach was identified and resolved immediately.



(Based on 159 responses)

Actions following worst security breach of the year



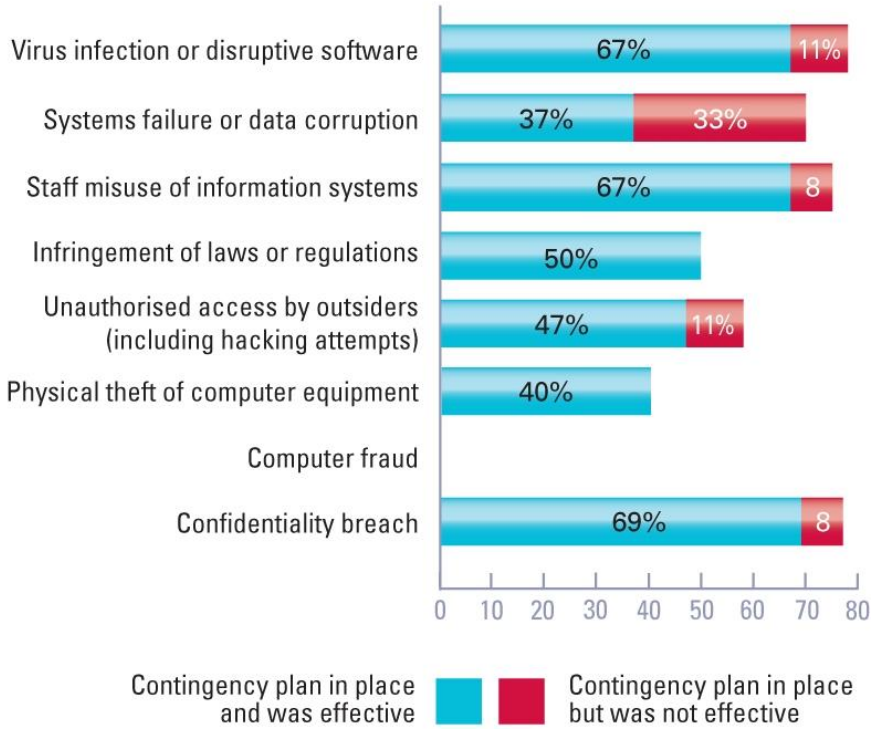
(Based on 122 responses)

- About the survey
- Security breaches increase
- External versus insider threats
- Understanding and communicating risks
- **Implementation**
- Key messages

Proactive versus reactive?

68% had contingency plans in place – but plans are not always effective

Following Superstorm Sandy, a mid sized technology company primarily based in London was forced to fail over from their primary servers in the USA to their backup server in the UK. Although the failover procedure was successful, a later power outage on either secondary site led to their client-facing systems being inaccessible. It took around several man- weeks of effort over a 24 hour period to restore service.



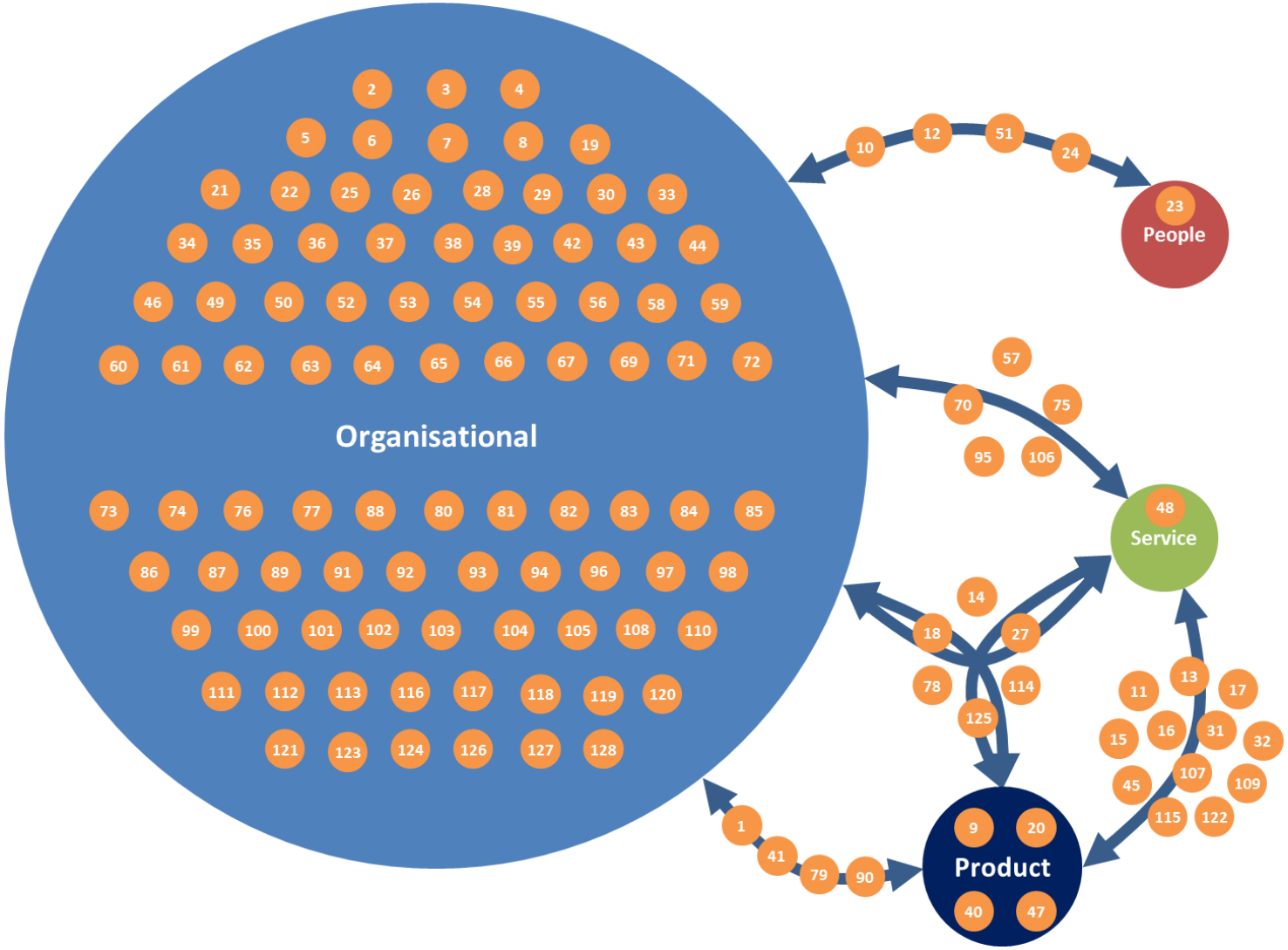
(Based on 99 responses)

"The Ten Steps"

The Ten Steps	Large organisations	Small businesses
Information risk management	Some good, some weak	Some good, some weak
User education and awareness	Some good, some weak	Generally weak
Home and mobile working	Some good, some weak	Generally weak
Incident management	Some good, some weak	Generally weak
Managing user privileges	Some good, some weak	Some good, some weak
Removable media controls	Some good, some weak	Generally weak
Monitoring	Some good, some weak	Generally weak
Secure configuration	Some good, some weak	Some good, some weak
Malware protection	Generally good	Some good, some weak
Network security	Generally weak	Generally weak

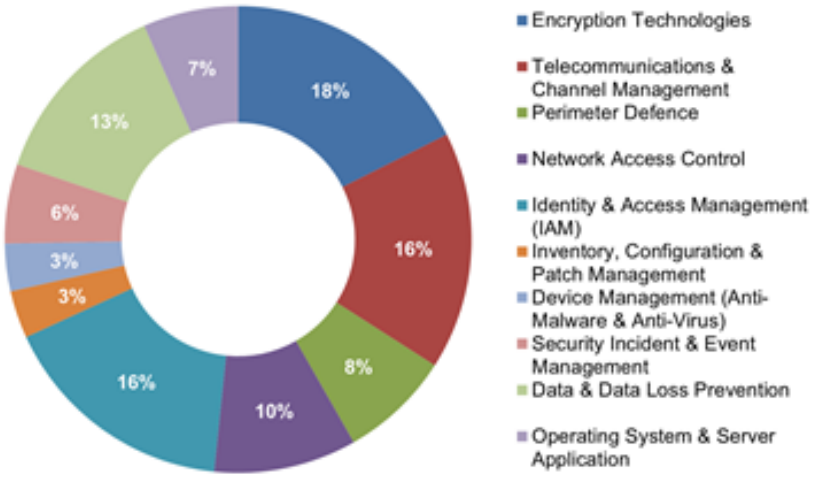
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Standards Landscape

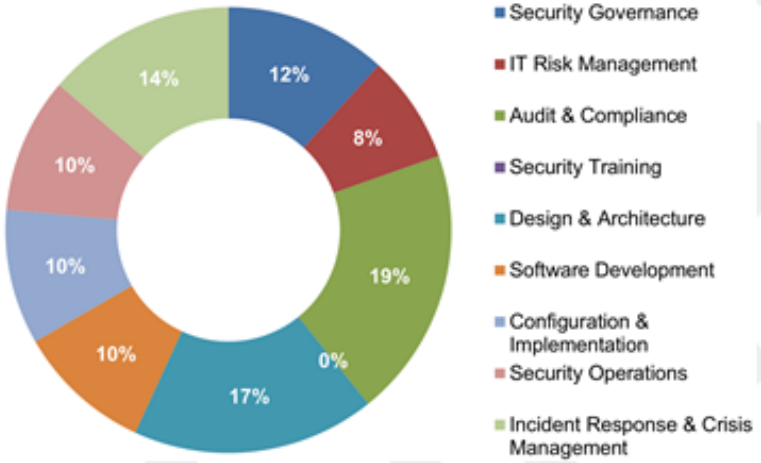


Standards Coverage

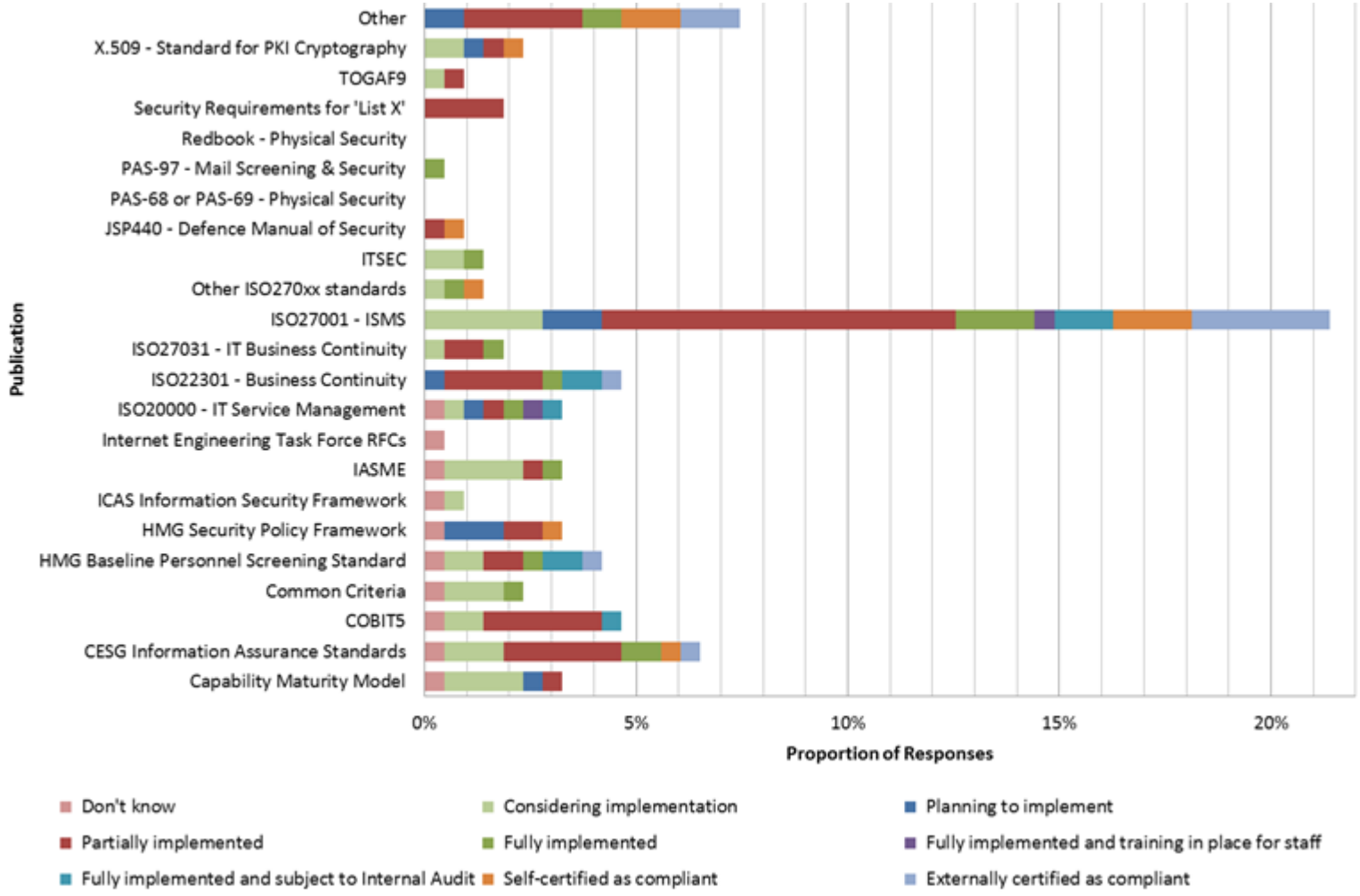
Product type coverage



Service type coverage



Level of standards adoption



- About the survey
- Security breaches increase
- External versus insider threats
- Understanding and communicating risks
- Implementation
- **Key messages**

Key messages in 2013

- **Small business are now getting targeted**
- **Need to measure ROI on security investment**
- **Get the basics in place (Ten Steps)**
- **Educating staff can halve insider breaches**

Questions?

Simon Schofield
BAE Systems Detica

Business Lead Cyber Security Consulting Services

Detica

BAE SYSTEMS

Social Engineering

How Cyber Criminals take advantage of lack Information security awareness, education and training to get what they need from your organisation

Simon Schofield Nov 2013

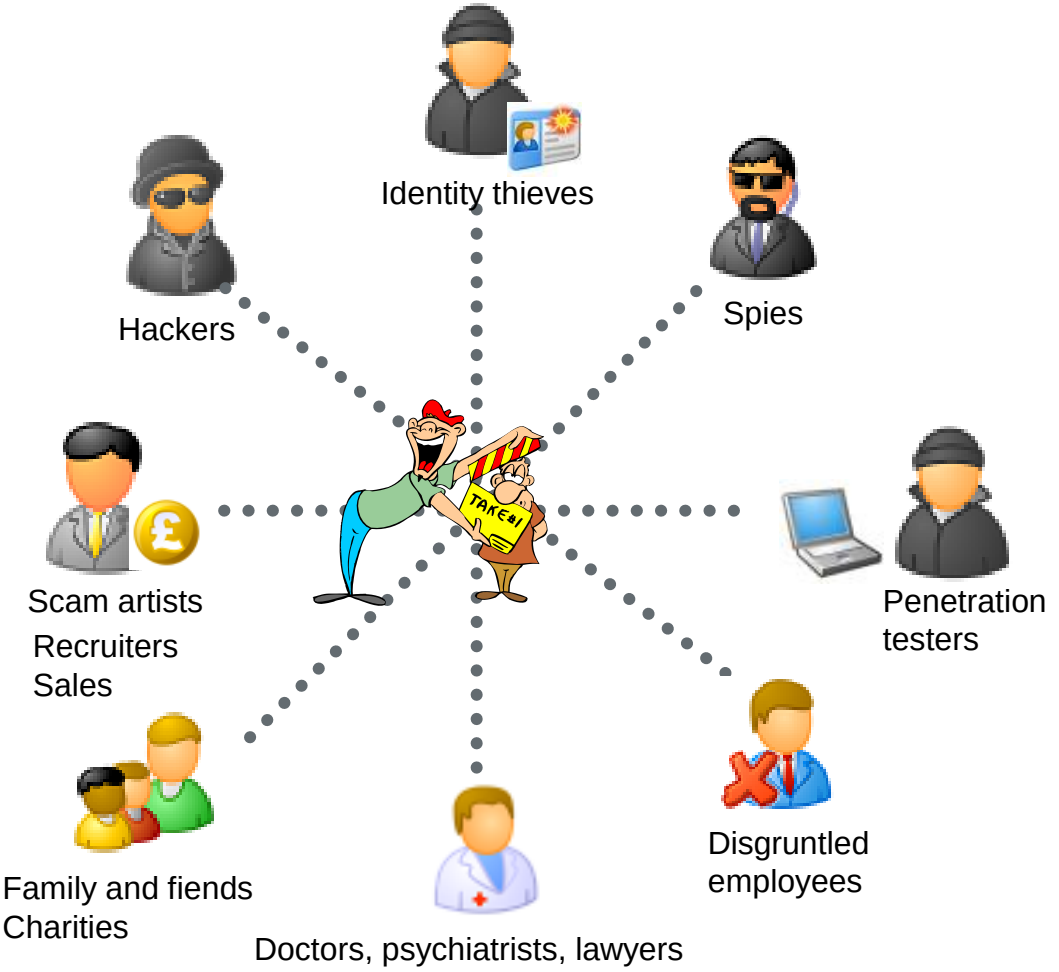
Detica

BAE SYSTEMS

What is Social Engineering

Social Engineering is:

The act of manipulating a person to take an action which may or may not be in the 'targets' best interest



Types of Social Engineering attacks

Physical		Technical
Interactive	**Non Interactive**	
Impersonation • Reverse Plant • Employee • Partner	Direct Assault • Physical Breach Assessment	Phishing • Email • Website
Employee • Desk Swiping • Piggy Back • Shoulder Surfing	Indirect Assault • Tailgating • Dumpster Diving • Eavesdropping	Cyber Baiting • Malicious Website • USB Key • DVD
Solicitation • Telephone • Mail • Social Media		Direct Attack • Rogue Wireless AP • Rogue Implant • Key Logging • Screen Grabbing

SparkyBlaze: “In my mind social engineering is the biggest issue today”.

SONY

Lockheed Martin

Google

HB Gary

PBS

Citibank

The Onion

Stratfor

David Kennedy:{SE attack}“success ratio is around 94%”

Impersonation

Pretexting : When was the last time you stopped or questioned someone with a mop?

To work pretexting needs to be:

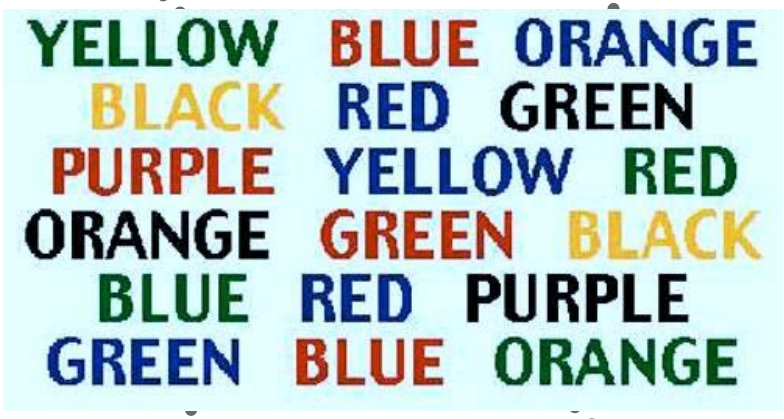
- Simple
- Be an outline not a script
- Have knowledge of the pretext
- Always close

Psychological factors

- **Framing:** Everything you are told evokes a frame. Telling you not to think of something evokes a frame; thinking about a frame reinforces that frame
- **Elicitation:** To stimulate or draw out a particular class of behaviour
- **Motivation:** The process that initiates, guides and maintains goal-oriented behaviours

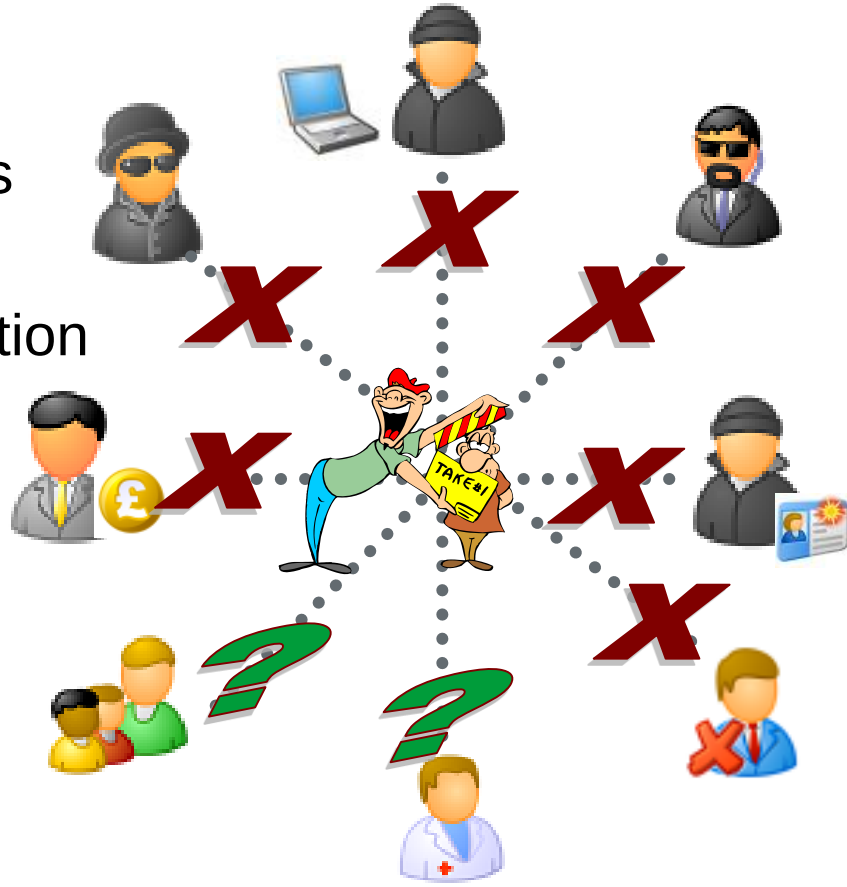
Manipulation

- **Scripting**: People go through life running scripts
- **Suggestibility**: Making people more suggestive through action or language
- **Conditioning**: Modifying fixed action pattern
- **Intimidation**: Frightening into compliance through coercion



How to defend you and your organisation

- **Critical thought**
  - As soon as someone asks why or disagrees Social Engineering fails
- **Policies & procedures**
  - Management direction for information security
  - Human Resource security
  - Business requirements of access control
- **Technical mitigations**
  - Logging and monitoring
  - Network segregation
  - Controls against malware



Where is the baby ?

Think it cannot happen to you?

Ogborn v McDonalds
Milligram experiment
Stanford prison experiment
Blue eye brown eye experiment

Questions?