Information Security Management System (ISMS) Overview

Arhnel Klyde S. Terroza

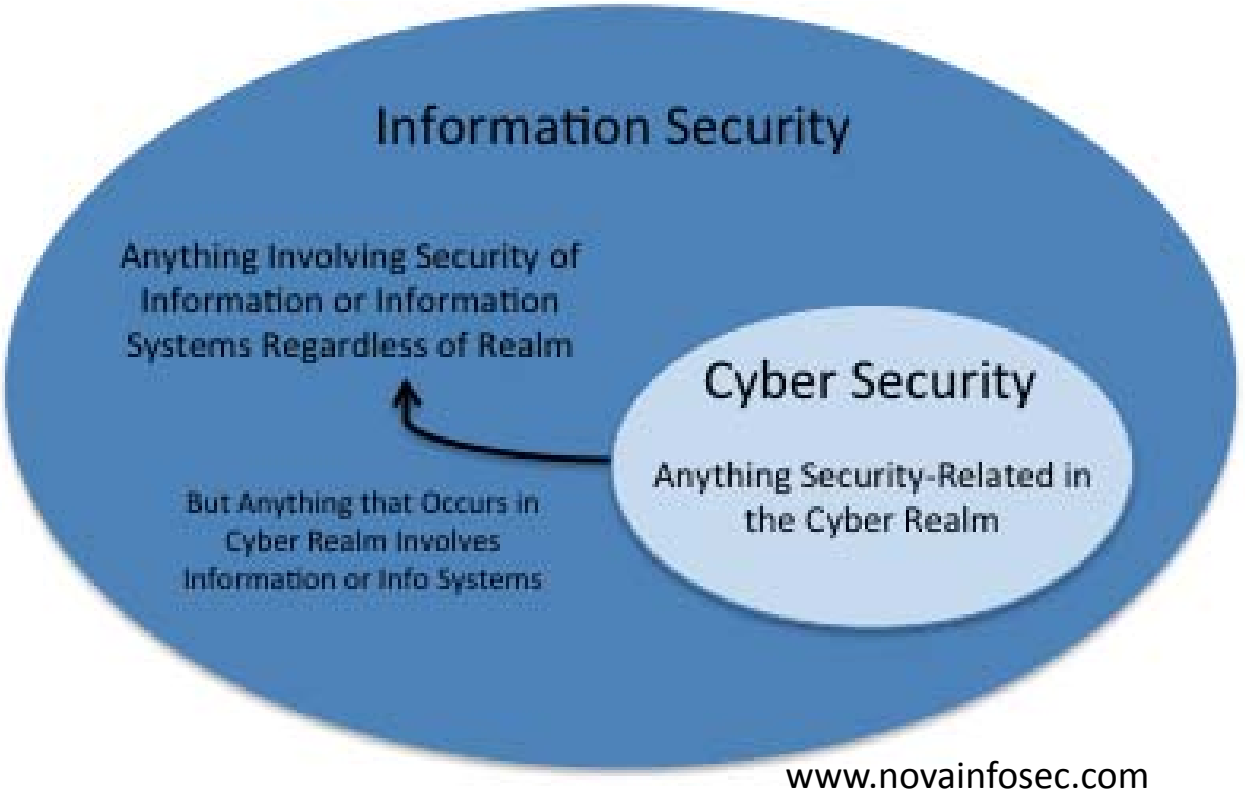
May 12, 2015

Arhnel Klyde S. Terroza
CPA, CISA, CISM, CRISC, ISO 27001 Provisional Auditor

- Internal Auditor at Clarien Bank Limited
- Former IT Risk and Assurance Manager with Ernst & Young – Financial Services Organization (FSO) – Hamilton, Bermuda and San Antonio, TX
- Certified Public Accountant (CPA - Philippines), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and ISO 27001 Provisional Auditor
- Bachelor of Science in Accountancy from Silliman University (Philippines)

AGENDA

- What is Information Security Management System (ISMS)?
- What are the standards, laws, and regulations out there that will help you build or assess your InfoSec Management Program?
- What is ISO/IEC 27001:2013?
- What are the ISO/IEC 27001 Controls?
- What are the benefits of adopting ISO 27001?
- Why do you need to conduct an InfoSec awareness survey?



www.novainfosec.com

What is ISMS?

- Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (ISO definition)
  - Note: A management system is a set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.
- Influenced by the organization's needs and objectives, security requirements, the processes employed and the size and structure of the organization.
- Expected to change over time.
- A holistic approach to managing information security – confidentiality, integrity, and availability of information and data.

What are the InfoSec-related standards, laws and regulations?

ISO 27000 Family of International Standards

Provides the best practice recommendations on InfoSec management, risks and controls within the context of an overall ISMS.

ISO 27000: Overview and Vocabulary (2014)

ISO 27001: ISMS Requirements (2013)

ISO 27002: Code of Practice (2013)

ISO 27003: ISMS Implementation Guidance (2010)

ISO 27004: ISM Measurement (2009)

ISO 27005: InfoSec Risk Management (2011)

ISO 27006: Requirements for Bodies Providing Audit and Certification of ISMS (2011)

ISO 27007 – 27008: Guidelines for Auditing InfoSec Controls (2011)

ISO 27014: Governance of InfoSec (2013)

ISO 27015: ISM Guidelines for Financial Services (2012)

- www.iso.org

Other Standards

Payment Card Industry Data Security Standard (PCI DSS)

US National Institute of Standards and Technology (NIST)

- Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53)
- Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)

ISACA Cybersecurity Nexus

The IIA GTAG 15: Information Security Governance (2010)

What are the InfoSec-related standards, laws and regulations?

Governmental laws and regulations with (or will have) a significant effect on InfoSec

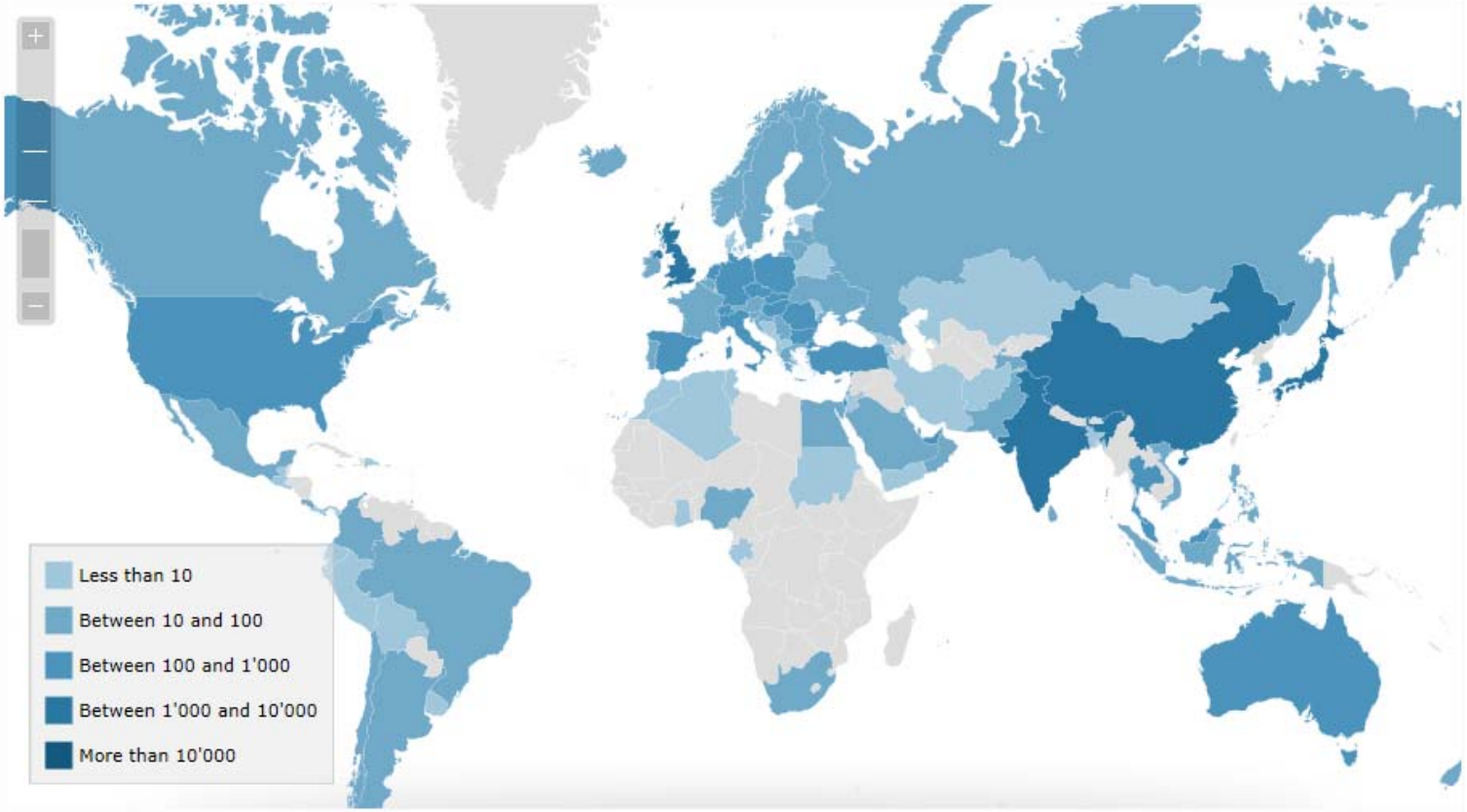
- UK Data Protection Act 1998
- The Computer Misuse Act 1990 (UK)
- Federal Information Security Management Act 2001 (US)
- Gramm-Leach-Bliley Act (GLBA) 1999 (US)
- Federal Financial Institutions Examination Council's (FFIEC) security guidelines (US)
- Sarbanes-Oxley Act (SOX) 2002 (US)
- State security breach notification laws (e.g. California) (US)
- Family Educational Rights and Privacy Act (US)
- Health Insurance Portability and Accountability Act (HIPAA) 1996 (US)
- Bermuda Laws???

What is ISO/IEC 27001:2013?

- Leading International Standard for ISMS. Specifies the requirements for establishing, implementing, maintaining, monitoring, reviewing and continually improving the ISMS within the context of the organization. Includes assessment and treatment of InfoSec risks.
- Best framework for complying with information security legislation.
- Not a technical standard that describes the ISMS in technical detail.
- Does not focus on information technology alone, but also other important business assets, resources, and processes in the organization.

What is ISO/IEC 27001:2013?

World distribution of ISO/IEC 27001 certificates in 2013



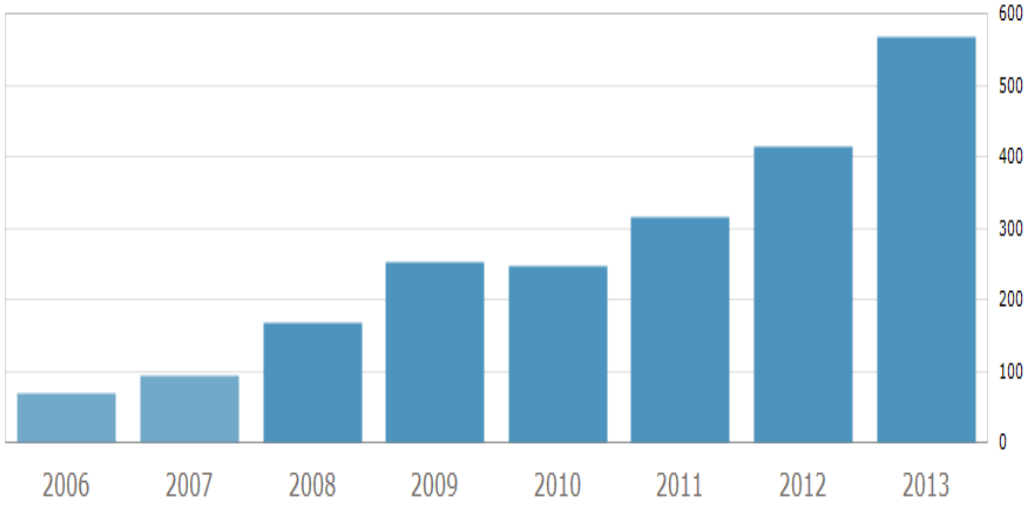
2013 – 22,293 (up 14%)
2012 – 19,620

Japan – 7,084
India – 1,931
United Kingdom – 1,923
China – 1,710
Spain – 799
United States – 566
Australia - 138
Canada – 66

Source: www.iso.org

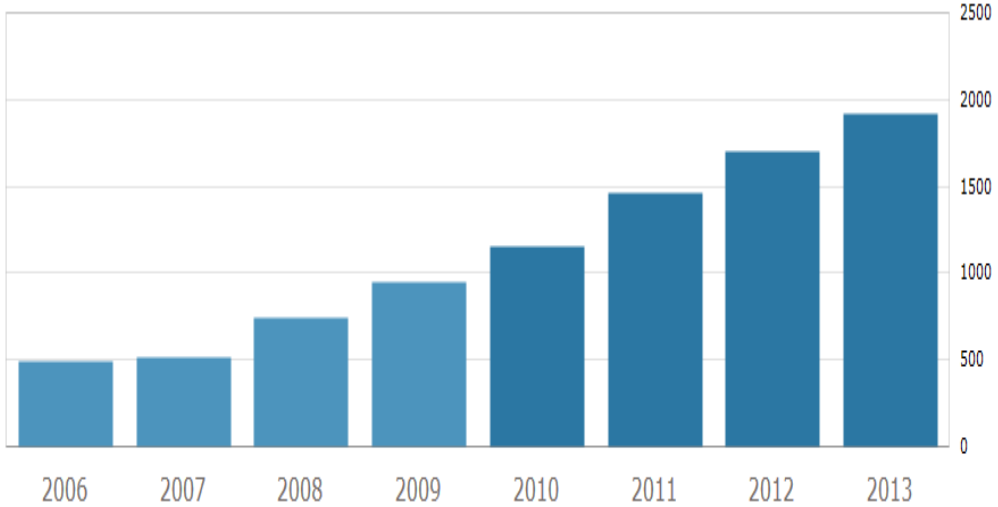
What is ISO/IEC 27001:2013?

Evolution of ISO/IEC 27001 certificates



United States

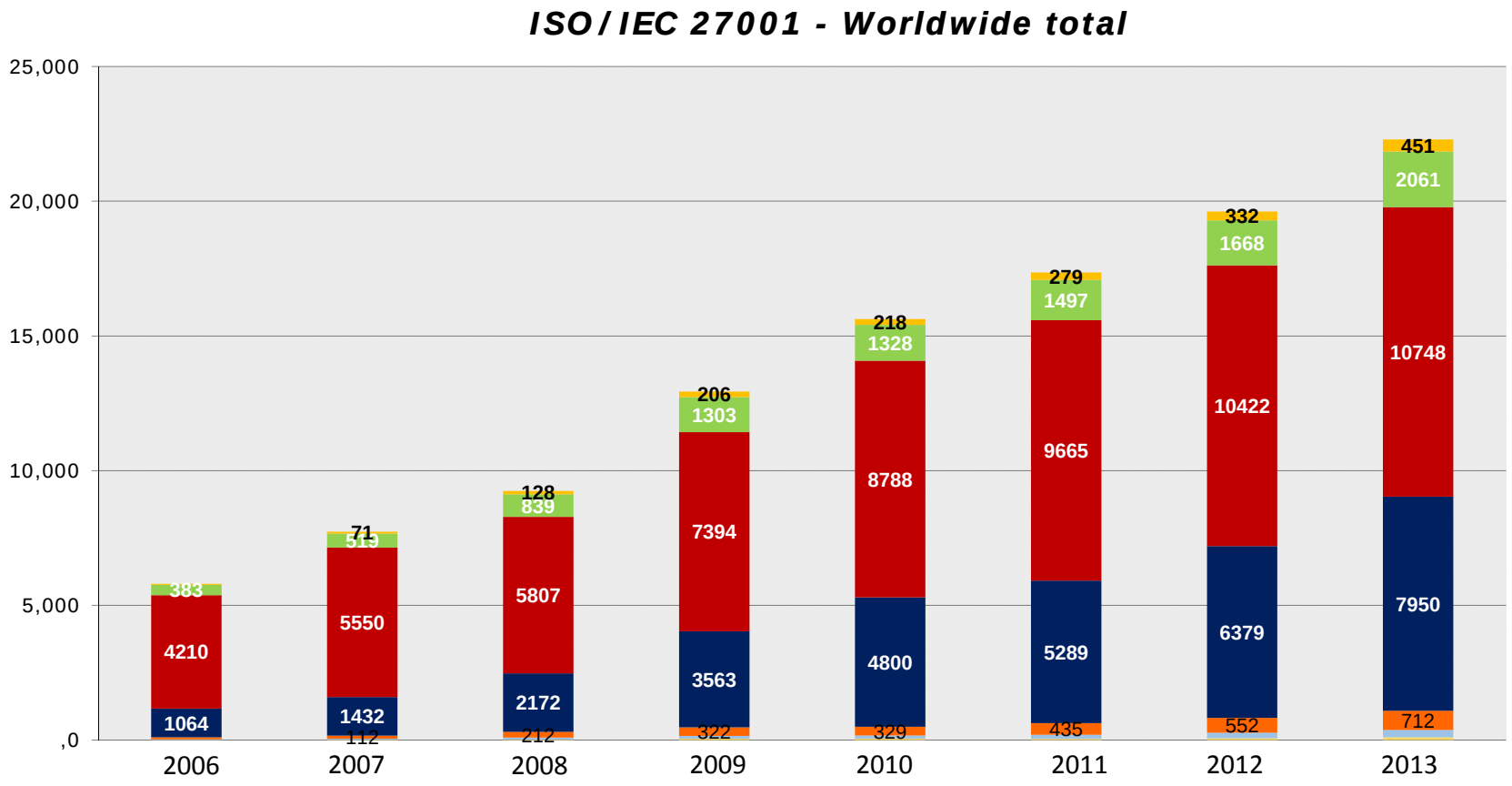
Source: www.iso.org



United Kingdom

- ISO does not perform certification. Organizations looking to get certified to an ISO standard must contact an independent certification body. Certification bodies muse use the ISO's Committee on Conformity Assessment (CASCO) standards related to the certification process.

What is ISO/IEC 27001:2013?



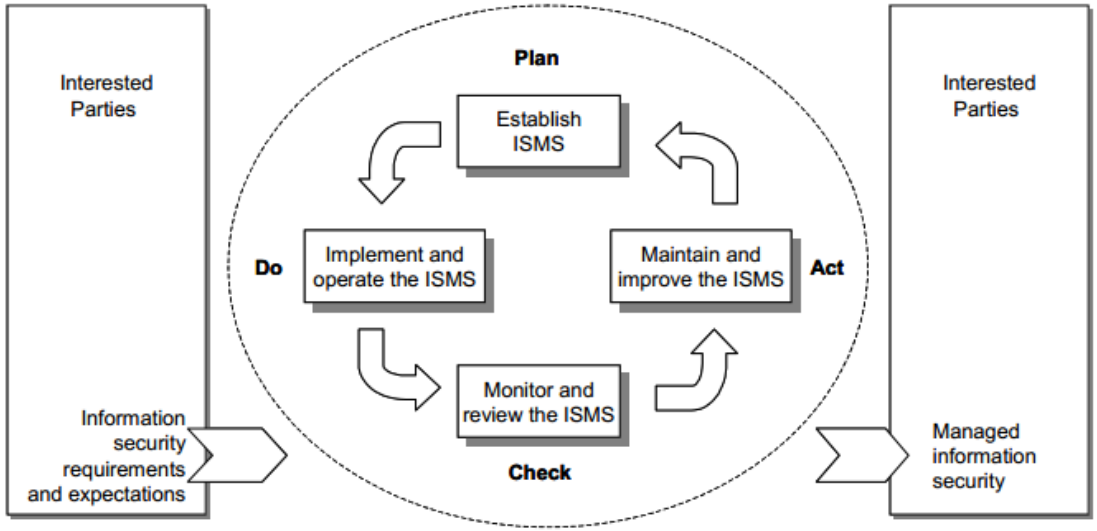
Source: www.iso.org

What is ISO/IEC 27001:2013?

Sources:
http://iaardirectory.jadianonline.com/Directory
http://www.bsiamerica.com

What is ISO/IEC 27001:2013?

Process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS:



PDCA model applied to ISMS processes

What are the ISO/IEC 27001 Controls?

Eight (8) mandatory clauses (controls/control objectives) for organizations claiming conformance to ISO/IEC 27001 standard:

- **Clause 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 information security management system
  - 4.4 Information security management system
- **Clause 5 Leadership**
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- **Clause 6 Planning**
  - 6.1 Actions to address risks and opportunities
  - 6.2 Information security objectives and planning to achieve them

What are the ISO/IEC 27001 Controls?

Eight (8) mandatory clauses (cont…):

- **Clause 7 Support**
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- **Clause 8 Operation**
  - 8.1 Operational planning and control
  - 8.2 Information security risk assessment
  - 8.3 Information security risk treatment
- **Clause 9 Performance Evaluation**
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review

What are the ISO/IEC 27001 Controls?

Eight (8) mandatory clauses (cont…):

- **Clause 10 Improvement**
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement

ISO/IEC 27001:2013 ISMS Control Point and Control Objective Summary			
Reference		**Description**	**Control Total**
Mandatory	**Clause 4**	**Context of the organization**	**8**
	Clause 5	**Leadership**	**19**
	Clause 6	**Planning**	**39**
	Clause 7	**Support**	**28**
	Clause 8	**Operation**	**9**
	Clause 9	**Performance evaluation**	**29**
	Clause 10	**Improvement**	**16**
		Total Control Points:	**148**

Source: www.slideshare.net by Mark E.S. Bernard (2013)

What are the ISO/IEC 27001 Controls?

14 Control Categories (Domain/Control Area) - Discretionary Controls (Annex A)

- **A.5 Information security policies**
  - A.5.1 Management direction for information security
- **A.6 Organization of information security**
  - A.6.1 Internal organization
  - A.6.2 Mobile devices and teleworking
- **A.7 Human resource security**
  - A.7.1 Prior to employment
  - A.7.2 During employment
  - A.7.3 Termination and change of employment

What are the ISO/IEC 27001 Controls?

14 Control Categories (Domain/Control Area) - Discretionary Controls (Annex A)

- **A.8 Asset management**
  - A.8.1 Responsibility for assets
  - A.8.2 Information classification
  - A.8.3 Media Handling
- **A.9 Access control**
  - A.9.1 Business requirements of access control
  - A.9.2 User access management
  - A.9.3 User responsibilities
  - A.9.4 System and application access control
- **A.10 Cryptography**
  - A.10.1 Cryptographic controls

What are the ISO/IEC 27001 Controls?

14 Control Categories (Domain/Control Area) - Discretionary Controls (Annex A)

- **A.11 Physical and environmental security**
  - A.11.1 Secure areas
  - A.11.2 Equipment
- **A.12 Operations security**
  - A.12.1 Operational procedures and responsibilities
  - A.12.2 Protection from malware
  - A.12.3 Backup
  - A.12.4 Logging and monitoring
  - A.12.5 Control of operational software
  - A.12.6 Technical vulnerability management
  - A.12.7 Information systems audit considerations

What are the ISO/IEC 27001 Controls?

14 Control Categories (Domain/Control Area) - Discretionary Controls (Annex A)

- **A.13 Communications security**
  - A.13.1 Network security management
  - A.13.2 Information transfer
- **A.14 System acquisition, development and maintenance**
  - A.14.1 Security requirements of information systems
  - A.14.2 Security in development and support processes
  - A.14.3 Test data
- **A.15 Supplier relationships**
  - A.15.1 Information security in supplier relationships
  - A.15.2 Supplier service delivery management
- **A.16 Information security incident management**
  - A.16.1 Management of information security incidents and improvements

What are the ISO/IEC 27001 Controls?

14 Control Categories (Domain/Control Area) - Discretionary Controls (Annex A)

- **A.17 Information security aspects of business continuity management**
  - A.17.1 Information security continuity
  - A.17.2 Redundancies
    - Note: A comprehensive BCMS standard was published by ISO in 2012 – ISO 22301:2012
- **A.18 Compliance**
  - A.18.1 Compliance with legal and contractual requirements
  - A.18.2 Information security reviews

ISO/IEC 27002:2013 is a better reference for selecting controls when implementing an ISMS based on ISO/IEC 27001:2013, either for certification purposes or alignment to a leading standard. Or it could simply be used as a guidance document for implementing commonly accepted information security controls.

What are the ISO/IEC 27001 Controls?

ISO/IEC 27001:2013 ISMS Control Point and Control Objective Summary			
Reference		**Description**	**Control Total**
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8
Source: www.slideshare.net by Mark E.S. Bernard (2013)		**Total Control Points:**	113

What are the benefits of ISO/IEC 27001:2013?

- Best framework for complying with information security legal, regulatory and contractual requirements
- Better organizational image because of the certificate issued by a certification body
- Proves that senior management are committed to the security of the organization, including customer's information
- Focused on reducing the risks for information that is valuable for the organization
- Provides a common goal
- Optimized operations within the organization because of clearly defined responsibilities and business processes
- Builds a culture of security

What are the benefits of ISO/IEC 27001:2013?

BSI Study on ISO 27001

- 87% of respondents stated that implementing ISO/IEC 27001 had a positive or very positive outcome
- Ability to meet compliance requirements increased for 60% of organizations
- Number of security incidents decreased for 39%
- Down time of IT systems decreased for 39%
- Ability to respond to tenders increased for 43%
- Relative competitive position increased for 47%
- 51 % saw an increase in external customer satisfaction following the implementation of an ISMS
- 40% saw an increase in internal customer satisfaction
- 66% noted an increase in the quality control of information security processes and procedures and 40% decrease in risk

Sources: http://www.bsiamerica.com

Why do you need to conduct an InfoSec awareness survey?

- What is an information security awareness program?
  - Promotes risk and security aware culture.
  - Helps in managing security incidents, compliance risks, and financial losses.
    - e.g. Phishing exercises, newsletters, posters

- What are the benefits of conducting an information security awareness survey?
  - Provides visibility into organizational behavior with respect to information security.
  - Data collected can be used to identify areas of possible improvement and risk reduction.
  - Initial survey can provide a baseline of security awareness of the organization; when applied overtime, can indicate progress or challenges in the infosec awareness program.
  - Helps the InfoSec Team and Human Resources gain a degree of understanding of personnel's attitudes and habits related to information security within the context of their day-to-day activities

Why do you need to conduct an InfoSec awareness survey?

- Misconception of awareness survey
  - Information security awareness survey is not intended to assess the organization's ISMS
- How to deploy surveys
  - Online survey tools (e.g. Survey Monkey)
  - Traditional mail
- How to analyze data from the survey?
  - Quantitative – aggregate responses to a question.
  - Qualitative – open ended questions can provide qualitative data. Comparison of results across departments, roles, and demographics (e.g. tenure within the company)
    - Note: How you analyze date depends on what questions are included

Why do you need to conduct an InfoSec awareness survey?

- Can an overall risk be concluded from the survey?
  - Questions can be designed in such a manner that answers are assigned a risk score.
    - For example, each question response are assigned a risk value of one to five – one being lowest risk value and five as the highest risk value
  - Results of the survey can be sued to determine the overall risk score of the organization
    - For example:

Risk Score	Description
Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with the Organization's security policies and standards.
Elevated (40 – 59)	Users have already been trained on the Organization's security policies and standards, they are aware of threats, but may not follow good security principles and controls.
Moderate (60 – 79)	Users are aware of threats and know they should follow good security principles and controls, but need training on the Organization's security policies and standards. They also may not know how to identify or report a security event.
Significant (80 – 99)	Users are not aware of good security principles or threats nor are they aware of or compliant with the Organization's security policies and standards.
High (100 and higher)	Users are not aware of threats and disregard known security policies and standards or do not comply. They are likely to engage in activities or practices that are easily attacked and exploited.

SUMMARY

An organization needs to undertake the following steps in establishing, monitoring, maintaining and improving its ISMS:

- Identify information assets and their associated information security requirements
- Assess information security risks and treat information security risks [to an acceptable level]
- Select and implement relevant controls to manage unacceptable risks [or to reduce risks to acceptable levels]
- Monitor, maintain and improve the effectiveness of controls associated with the organization’s information assets

SUMMARY

- Adoption of an ISMS should be a strategic decision for an organization.
- ISMS is a holistic approach to managing information security – confidentiality, integrity, and availability of information and data.
- Laws and regulations are continuing to evolve to address information security risk and privacy. ISO/IEC 27001:2013 is the best framework for complying with information security legislation.
- ISO/IEC 27001:2013 is not a technical standard for IT only.
- Increasing trend in adopting a holistic approach (using ISO/IEC 27001:2013) in managing information security risks.
- Organizations need to conduct an information security awareness survey.

Questions