Deloitte.

Information Security ISO Standards

Feb 11, 2015

Glen Bruce
Director, Enterprise Risk
Security & Privacy

Agenda

1. Introduction
   - Information security risks and requirements
2. Information Security Management System
   - ISO Directives for management system standards
3. ISO 27000 family of standards
   - Structure of the standards
   - Library of ISO 27000 standards available and under development
4. ISO 27001 certification
   - Certification approach
   - Certification Audit process
   - Benefits of ISMS certification
5. ISO standards involving service providers
6. Cloud security considerations
   - Cloud security requirements
   - Cloud service provider security certifications
7. Questions

A formal system is required to meet the information security risks

Information Security has generally evolved into a collection of measures to counter identified threats but not into a cohesive system that can be easily managed.

Why is it a problem?

- Information Security has traditionally grown up as a multiple technology responses to different threats leading to large and varied array of technology and vendors.
- Many times the technical response is reactive and not planned.
- Overall effectiveness of the security measures can be difficult to determine.
- The focus is increasingly on people as the weak point not the technology.
- Good security tends to be an opinion rather than a supportable fact

Implications

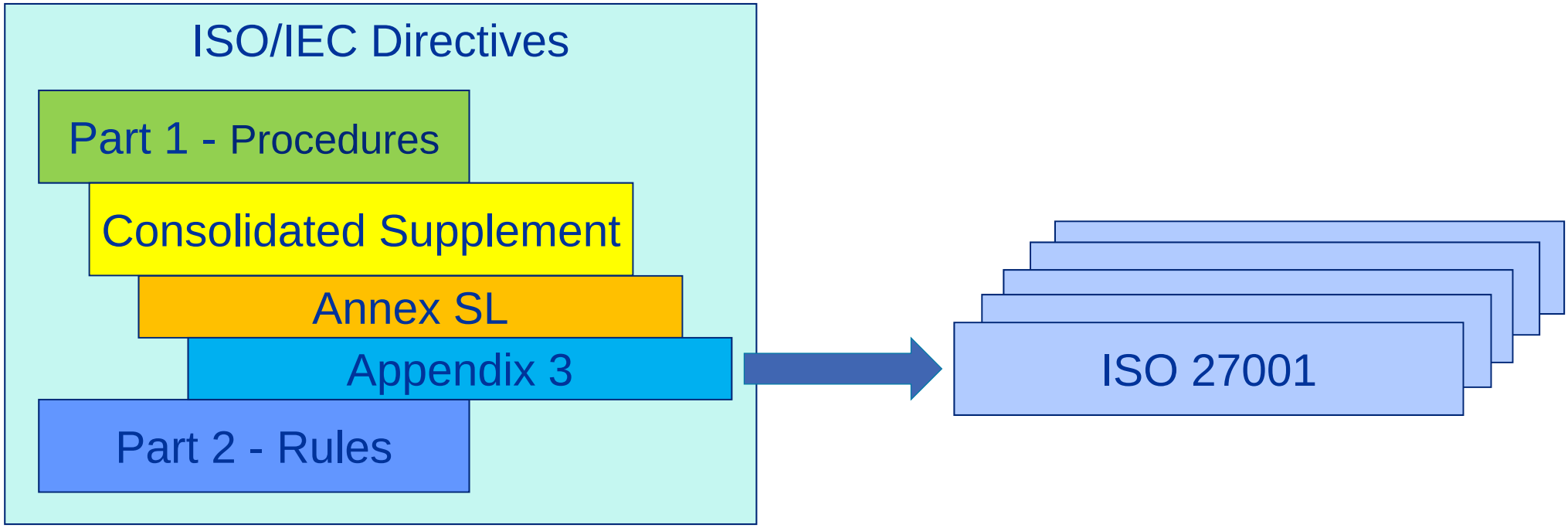
- Increased cost due to multiple technical controls and/or duplication.
- Increased complexity to manage an ever increasing technology base.
- Susceptible to new threats
- Security can get in the way of the business
- Maintenance is challenging.
- It is easy to loose sight of the big picture.

What does an organization need to effectively manage information security risk?

1. Corporate decisions on how risk must be managed (strategy, principles, policies, standards etc.);
2. Knowing how much risk the organization is willing to accept (risk tolerance/appetite);
3. An understanding of who accepts risk on behalf of the organization (understanding and adherence);
4. A method or process to understand the risk and how to deal with it (risk assessments, risk treatment);
5. Knowing what needs to be protected (inventory, information classification);
6. A method to effectively communicate responsibilities and obligations (escalate risks and decisions);
7. A comprehensive and balanced set of requirements;
8. A method and process for managing everyone's expectations (sign off); and
9. A common framework to put it all together.

Information security needs to be a continuously operating management system

The ISO / IEC Directives - define the basic procedures to be followed in the development of International Standards and other publications.



The ISO Directives provide guidance for the development of **all** ISO management system standards including;

- ISO 30301:2011, *Information and documentation – Management systems for records*
- ISO 22301:2012, *Societal security – Business continuity*
- ISO 20121:2012, *Event sustainability management systems*
- ISO 39001, *Road-traffic safety (RTS) management systems*
- **ISO/IEC 27001– *Information security management systems***
- ISO 55001, *Asset management*
- ISO 16125, *Fraud countermeasures and controls – Security management system*

The “Plan-Do-Check-Act’ model guides all ISO Management System Standards

Act
Implement the identified Improvements in ISMS
Continuous feedback and improvement
Communication with interested parties
Ensure improvements achieve intended results

Check
Execute monitoring procedures and controls
Undertake regular reviews of ISMS
Review residual risk and acceptable risk

Interested Parties

Enterprise Security Architecture Requirements

Business Strategy

ISO Directives

Interested Parties

Established ISMS

Qualitative ROI

Regulatory / Legislative Compliance

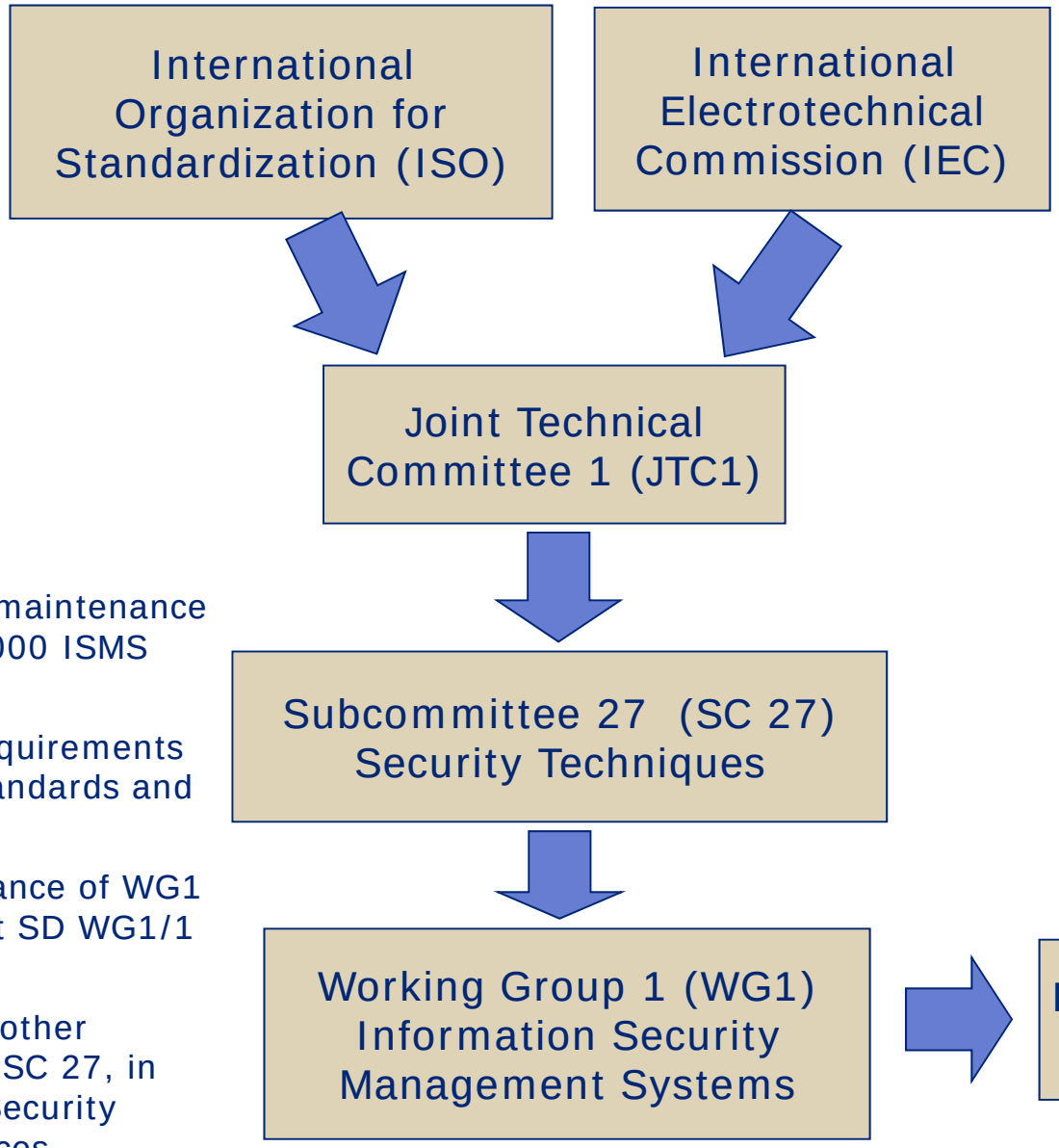
Plan
Define Scope of ISMS
Define ISMS Policy
Define Systematic approach to risk assessment
Identify and assess Risk
Identify and evaluate risk treatment options
Select controls for risk treatment
Prepare Statement of Applicability

Do
Formulate Risk Treatment Plan
Implement Risk Treatment Plan
Implement controls
Implement training and awareness
Manage Operations
Manage Resources
Implement detective and reactive controls for security incidents

Elements of a management system according to ISO

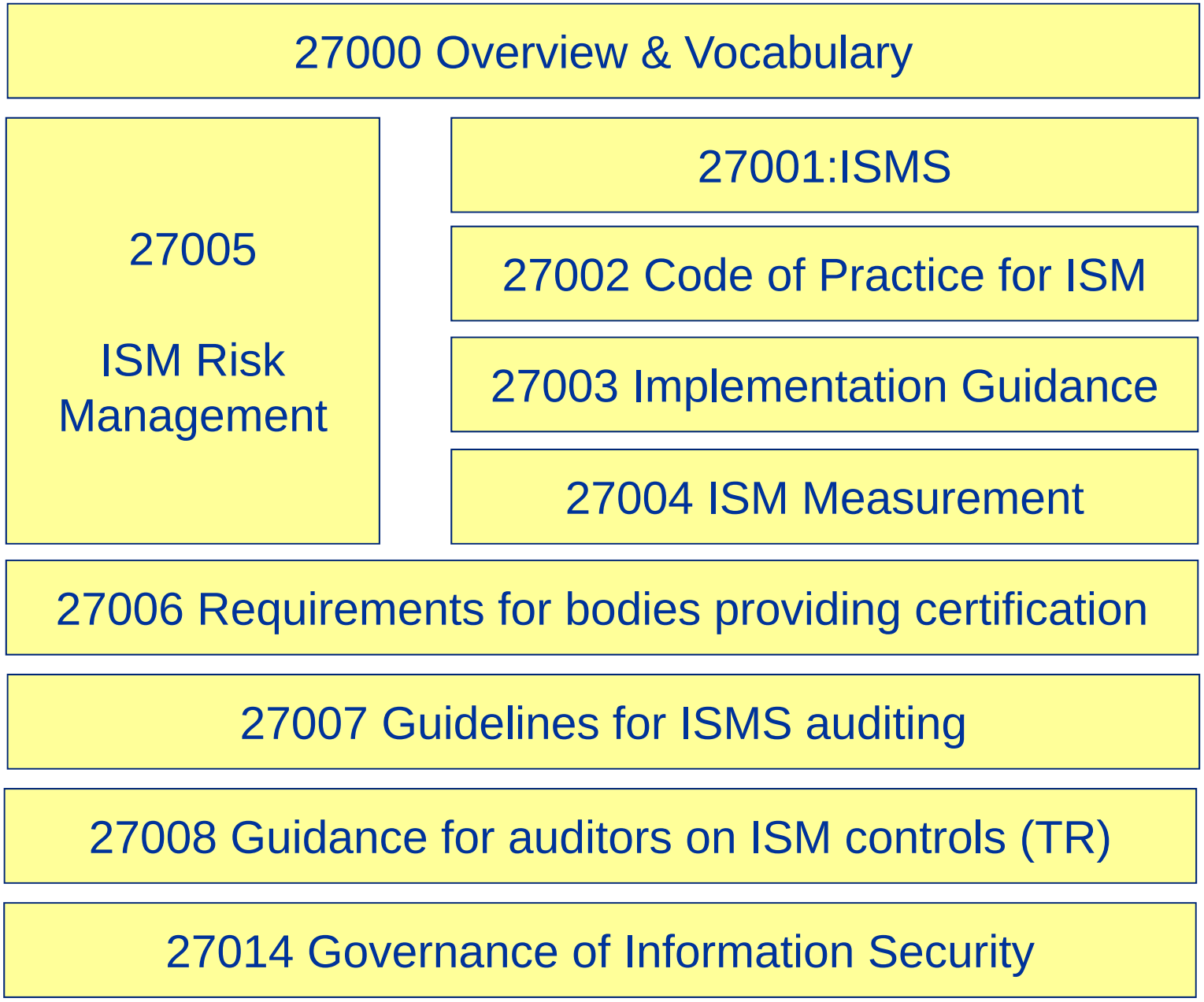
1. Scope
2. Normative References
3. Terms and Definitions
4. Context
   - Understanding the organization and its context
   - Understanding the needs and expectations of interested parties
   - Determining the scope of the management system
   - Security management system
5. Leadership
   - Leadership and commitment
   - Policy
   - Organization roles, responsibilities and authorities
6. Planning
   - Actions to address risks and opportunities
   - Objectives and planning to achieve them
7. Support
   - Resources
   - Competence
   - Awareness
   - Communication
   - Documented information
     - General
     - Creating and Updating
     - Control of documented information
8. Operation
   - Operational planning and control
9. Performance Evaluation
   - Monitoring, measurement, analysis and evaluation
   - Internal audit
   - Management review
10. Improvement
    - Nonconformity and corrective action
    - Continual improvement

ISO/IEC 27000 Family Standards Process



1. Development and maintenance of the ISO/IEC 27000 ISMS standards family
2. Identification of requirements for future ISMS standards and guidelines
3. On-going maintenance of WG1 standing document SD WG1/1 (WG1 Roadmap)
4. Collaboration with other working Groups in SC 27, in particular WG4 – Security Controls and Services

Structure of ISO 27000 standards



The ISO 27000 Standards Available Today

- **ISO 27000:2014** – ISM - Overview and vocabulary
- **ISO 27001:2013** – ISMS - Requirements
- **ISO 27002:2013** – Code of practice for information security controls
- **ISO 27003:2010** – ISMS - Implementation guidance
- **ISO 27004:2009** – Information security management - Measurement
- **ISO 27005:2011** – Information security risk management
- **ISO 27006:2011 –** Requirements for bodies providing audit and certification of the ISMS
- **ISO 27007:2011 –** Guidelines for ISMS auditing
- **ISO TR 27008:2011** – Guidelines for auditors on information security controls
- **ISO 27010:2012** – ISM for inter-sector and inter-organisational communications
- **ISO 27011:2008** – ISM Guidelines for telecommunications based on ISO/IEC 27002
- **ISO 27013:2012 –** Guidance on integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- **ISO 27014:2013 –** Governance of information security
- **ISO TR 27015:2012 –** Information security management guidelines for financial services
- **ISO TR 27016:2014 –** ISM **-** Organizational economics
- **ISO 27018:2014 –** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO TR 27019:2013 –** ISM Guidelines based on ISO/IEC 27002 for process control systems for the energy industry
- **ISO 27031:2011 –** Guidelines for ICT readiness for business continuity

The ISO 27000 Standards Available Today

- **ISO 27032:2012 –** Guidelines for cybersecurity
- **ISO 27033-1:2009 –** Network security – Part 1: Overview and concepts
- **ISO 27033-2:2012 –** Network security – Part 2: Guidelines for the design and implementation of network security
- **ISO 27033-3:2010 –** Network security – Part 3: Referencing network scenarios - threats, design techniques and control issues
- **ISO 27033-4:2014 –** Network security – Part 4: Securing communication between networks using security gateways
- **ISO 27033-5:2013 –** Network security – Part 5: Securing communication across networks using Virtual Private Networks (VPNs)
- **ISO 27034-1:2011 -** Application security - Overview and concepts
- **ISO 27035:2011 –** Information security incident management
- **ISO 27036-1:2014 –** Information security for suppler relationships – Part 1: Overview and concepts
- **ISO 27036-2:2014 –** Information security for suppler relationships – Part 2: Requirements
- **ISO 27036-3:2013 –** Information security for suppler relationships – Part 3: Guidelines for ICT supply chain security
- **ISO 27037:2012 –** Guidelines for identification, collection, acquisition and preservation of digital evidence
- **ISO 27038:2014** – Specification of digital redaction
- **ISO 27040:2015** – Storage security
- **ISO 27799:2008 –** Security management in health using ISO/IEC 27002

The Remaining ISO 27000 ISMS Family (in development)

- **ISO 27009** – Application of ISO/IEC 27001 - Requirements
- **ISO 27017 -** Security in cloud computing
- **ISO TR 27021** – Competence requirements for information security management professionals
- **ISO TR 27023** – Mapping the revised editions of ISO 27001 and ISO 27002
- **ISO 27033-6 -** Network Security – Part 6: Security wireless IP network access
- **ISO 27034 (Parts 2-8) –** Application Security
- **ISO 27036-4 –** Information security for supplier relationships – Part 4: Guidelines for security of cloud services
- **ISO 27038** – Specification for Digital Redaction
- **ISO 27039** - Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)
- **ISO 27041** - Guidance on assuring suitability and adequacy of incident investigative methods
- **ISO 27042** - Guidelines for the analysis and interpretation of digital evidence
- **ISO 27043** – Incident investigation principles and processes
- **ISO 27044** – Guidelines for security incident and event management (SIEM)
- **ISO 27050 (Parts 1-4) -** Electronic discovery

ISO 27001:2013 ISMS Requirements

Standard	High-Level Overview	High-Level Limitations
ISO 27001:2013	• Built on the same premise of any quality management ISO standard -continually improving performance. • Specifies the requirements for establishing, implementing and documenting an ISMS. • Specifies requirements for security controls to be implemented according to the business requirements, risk, and legal and contractual obligations. • Two Main Components of ISO: Clauses 4-10 and Annex A (Controls)	• Compliance with, or certification against ISO 27001:2013 does not, itself, guarantee that an organization is secure.

ISO 27001:2013 (clauses 4-10)

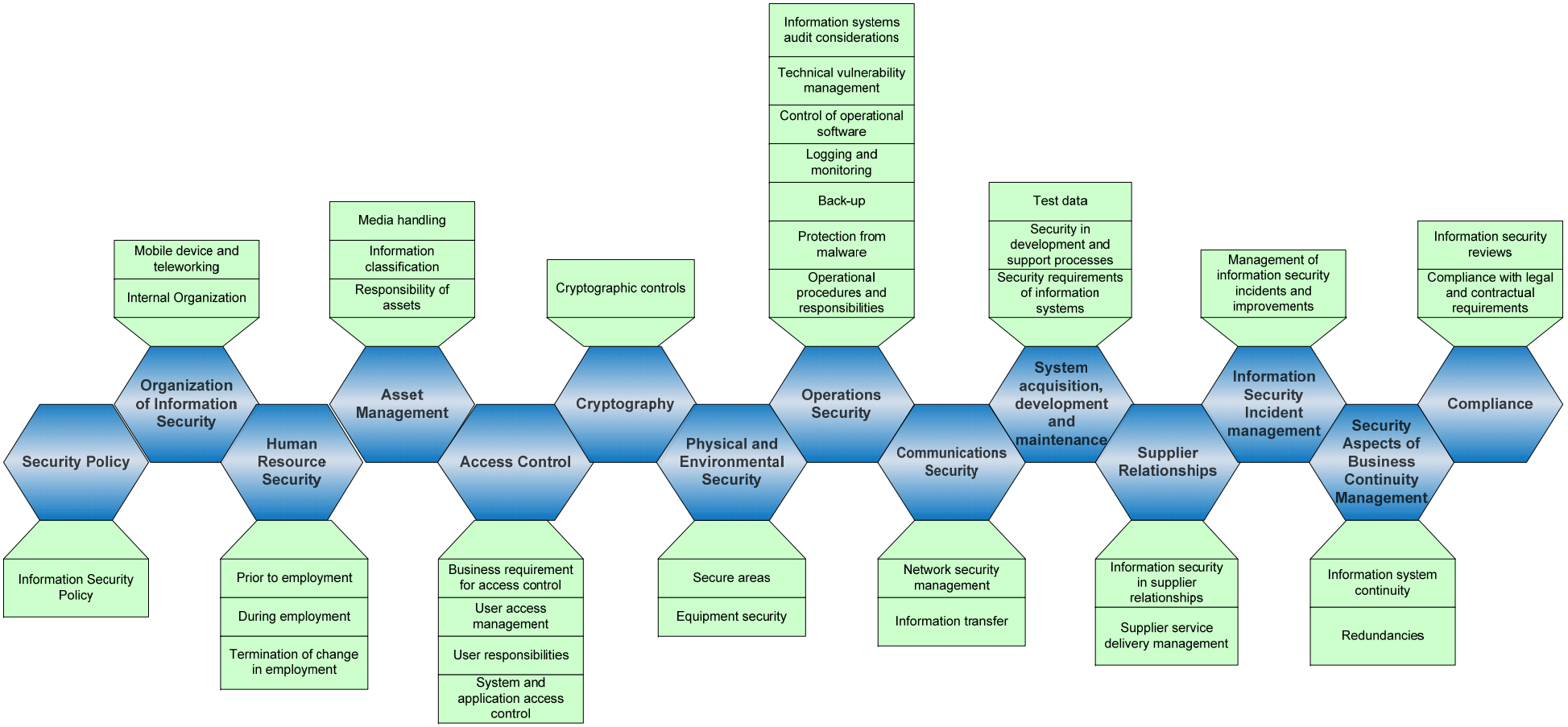
- 4. Context of the organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10. Improvement

ISO 27001:2013 (Annex A Controls)

- 5. Information security policies
- 6. Organisation of information security
- 7. Human resources security
- 8. Asset management
- 9. Access control
- 10. Cryptography
- 11. Physical and environmental security
- 12. Operations security
- 13. Communications security
- 14. Systems acquisition development & maintenance
- 15. Supplier relationships
- 16. Information security incident management
- 17. Information security aspects of business continuity management
- 18. Compliance

ISO 27001:2013 contents (aligned to ISO Directives)

ISO 27002:2013 – Code of practice for information security controls



- Definition of control objectives, controls and implementation guidance under 14 security domains
- Included as Annex A in ISO 27001:2013

Example ISO 27001 Certification Implementation Approach

ISO 27001:2013 Certification Roadmap

Phase	Phase I Scoping & Planning	Phase II Gap Assessment & Roadmap	Phase III ISMS Implementation	Phase IV Internal & External Audit
Aim	Determine scope, organisational objectives, interested parties, stakeholders	Assess scope against current state compliance to ISO27001:2013 Clauses and Annex A Controls	Develop and implement requirements in compliance to ISO27001:2013	Monitoring, Internal and External Audit of the ISMS for compliance to ISO27001:2013 mandatory requirements
Activities	• Hi-level project plan • ISMS Scoping workshop • Approved ISMS Scope statement	• ISO27001: 2013 Clause 4 to 10 Conformance assessment • ISO27001:2013 Annex A Gap assessment • Develop ISMS Implementation Roadmap	• Review and update Information Security Policy • Definition of role, responsibilities and authorities • Risk Assessment • Risk Treatment Plans • Statement of Applicability • Documentation Controls • KPI's, KRI's and RACI	• Management Review • Internal Audit • Op. Readiness Assessment Stage 1 Certification Audit Stage 2 Certification Audit
			Risk Treatment	
Ongoing Streams	Project Management			
	Knowledge Transfer			

Mandatory documented information required for certification

1. ISMS scope (as per clause 4.3)
2. Information security policy (clause 5.2)
3. Information security risk assessment *process* (clause 6.1.2)
4. Information security risk treatment *process* (clause 6.1.3)
5. Information security objectives (clause 6.2)
6. Evidence of the competence of the people working in information security (clause 7.2)
7. Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
8. Operational planning and control documents (clause 8.1)
9. The *results* of the risk assessments (clause 8.2)
10. The *decisions* regarding risk treatment (clause 8.3)
11. Evidence of the monitoring and measurement of information security (clause 9.1)
12. The ISMS internal audit program and the results of audits conducted (clause 9.2)
13. Evidence of top management reviews of the ISMS (clause 9.3)
14. Evidence of nonconformities identified and corrective actions arising (clause 10.1)
15. Various others subject to specific control in Annex A.

ISO27001 Certification Audit Process

OPTIONAL: Readiness Assessment

- Onsite pre-assessment that covers both Stage 1 and Stage 2 audits
- Results of pre-assessment are not "official" but are akin to gap analysis

Stage 1: ISMS Documentation Review

- Desktop review of documentation (can be offsite)
- Objective: To provide focus for planning the audit by gaining and understanding the ISMS in the context of the organizations security policy, policy and preparedness for the audit
- Scope of ISMS
- Risk assessment report and risk treatment plan
- Documented procedures
- Records
- Statement of Applicability

Stage 2: Complete On-site Audit

- Determine that the ISMS is functioning effectively
- Interviews conducted with staff within the ISMS

Ongoing: Surveillance Audits

- Conducted on an ongoing (e.g. six months – one year) basis rotating through all ISMS and Annex A controls during a 2-year period
- Reassessed at year 3

Non-conformities

Definition

- Condition adverse to the requirements of ISO 27001
- Non-fulfilment of a specified requirement:
- Relating directly to the security policy
- Against the ISMS
- Against legal or regulatory requirements

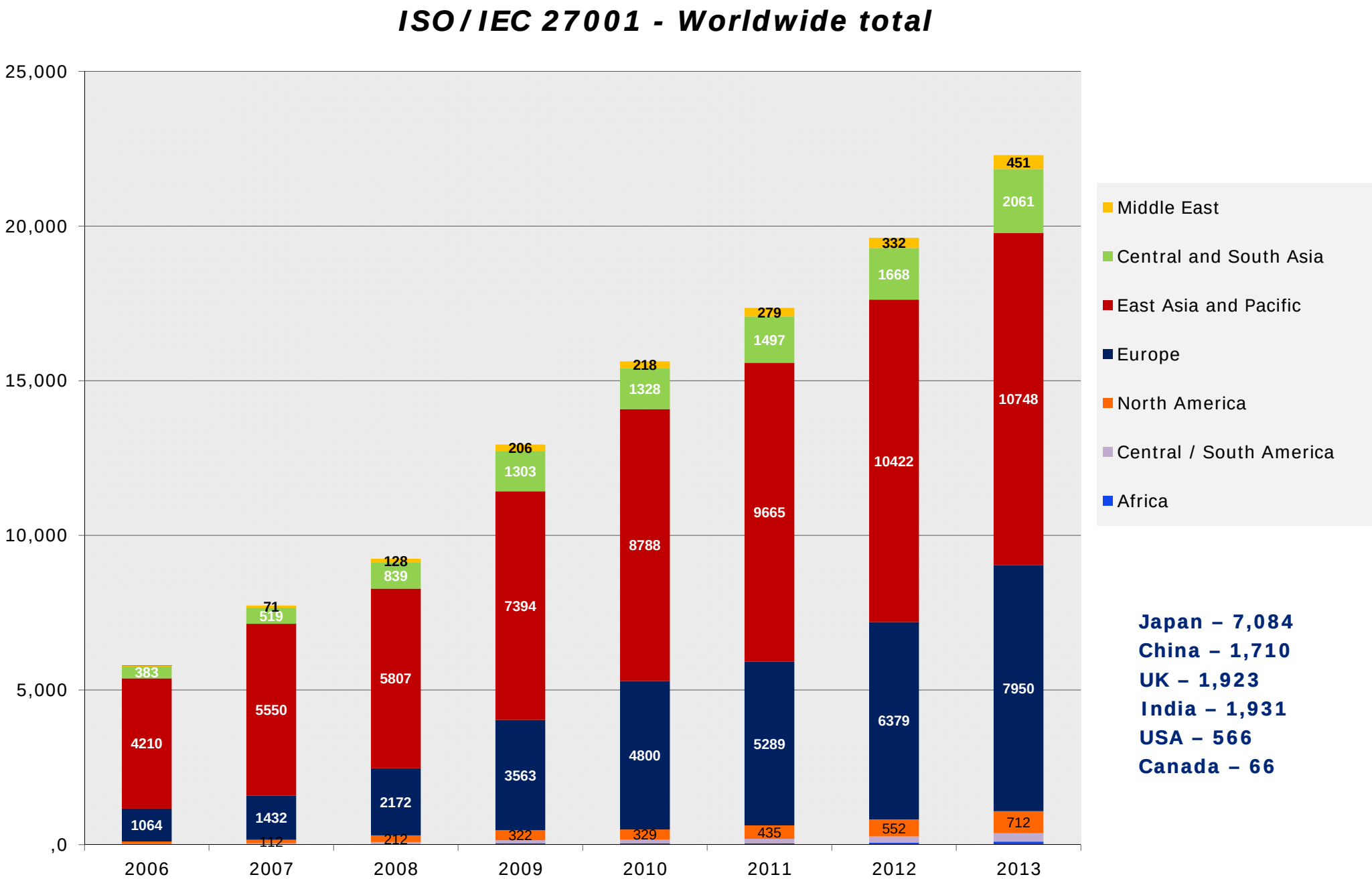
Possible Causes

- Documented system (defined process) does not conform with the ISMS standard (intent)
- Practice is not in line with intent (implementation)
- Action is not achieving planned results (effectiveness)

Non-conformity examples

- Observed non-compliance with clear desk policy
- Visitors not signed out of the building on one occasion
- Training record not available
- Observed non-compliance to policies

ISO 27001: ISMS Certificates



Japan – 7,084
China – 1,710
UK – 1,923
India – 1,931
USA – 566
Canada – 66

Certificates – 22,293 in 105 countries

Benefits of certification

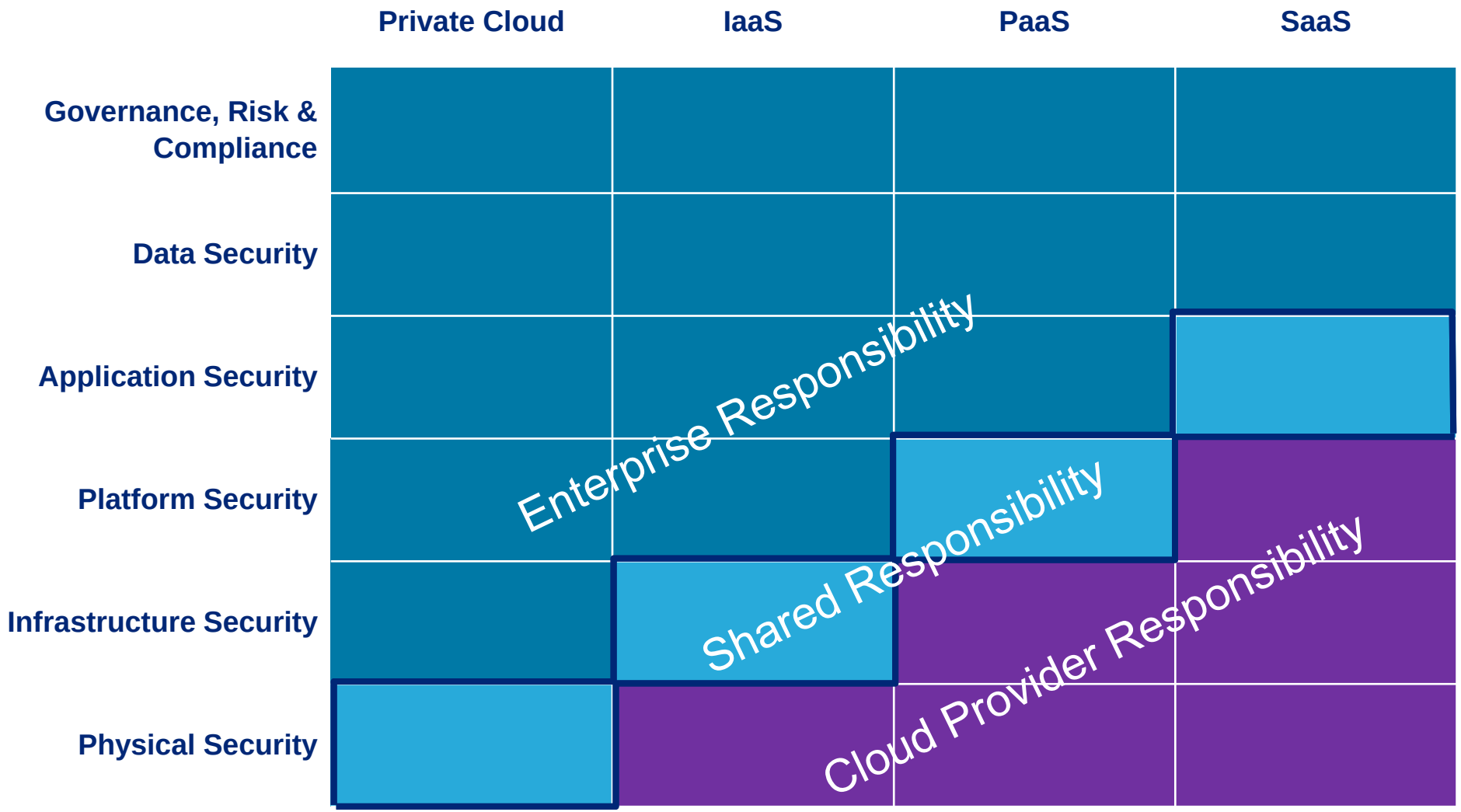
Management Commitment to Information Security	• Requirements of the standard hold management accountable for committing (time, effort, funding, resources, etc.) to information security • Management is accountable to select controls based on risk acceptance and enforce those controls within the organisation
Information Security Effectiveness	• Increase awareness of information security within the organisation • Appropriate protection of organisational assets • Effectiveness of controls are measured and reported
Compliance and Legal Requirements	• Demonstrates pro-active compliance with regulators • Can be used as the common framework for other standards, regulatory requirements • Reduced liability risk
Building and Maintaining Trust	• Used to validate security practices and provide confidence in the use of third parties • Operational efficiencies gained through repeatable processes for compliance monitoring
Continual Improvement	• Enables the development of an introspective, agile and resilient organization

ISO Standards Involving Suppliers and Service Providers

- ISO/IEC 17788:2014 - Information technology -- Cloud computing -- Overview and vocabulary
- ISO/IEC 17789:2014 - Information technology -- Cloud computing -- Reference architecture
- ISO/IEC 27017 – Security in cloud computing (in development)
- ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27036 – Information security for supplier relationships
  - Part 1 – Overview and concepts (published)
  - Part 2 – Requirements (published)
  - Part 3 – Guidelines for ICT supply chain security (published)
  - Part 4 – Guidelines for security of cloud services (in development)
- ISO/PAS 28000 - Specification for security management systems for the supply chain
- ISO /IEC 37500:2014 – Guidance on outsourcing

Cloud security is a shared responsibility

Shared between the enterprise and the cloud provider, with varying responsibilities depending on the nature of the (X)aaS type



Cloud Service Provider (CSP) Risk Exposure

The nature of the CSP relationship determines the risk exposure

1. **Risk Attributes**
   - Financial stability
   - Geography
   - Capability / capacity / service-levels
   - Corporate strategy and leadership

2. **Product / Service Profile**
   - Type of service / implementation
   - Nature / extent of customer interaction
   - Access to intellectual property
   - Sensitivity to regulatory requirements

3. **Level of Integration**
   - Integration into end products
   - Emerging technologies, and alignment of technology and processes

4. **Service Model affecting CSP Oversight**
   - Staff augmentation
   - Managed service

Potential Risk Exposures
Strategic / CSP Selection
Information Security
Reputation
Transaction / Operational
Financial
Legal / Compliance
Credit
Contractual
Geopolitical
Business Continuity

Cloud Service Provider Certifications

1. **Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)**
   - Leading cloud security certifications based on the Open Certification Framework

2. **US FedRAMP - Secure Cloud Computing for Federal Government**
   - Cloud certification using a baseline of security controls to support low and moderate impact systems based NIST 800-53 V4

3. **UK GCloud**
   - Assertion-based using implementation guidance in support of 14 cloud security principles

4. **TRUSTed Cloud Privacy Certification**
   - Review of data privacy management practices. If practices are consistent with the TRUSTe Privacy Program Requirements will be granted the TRUSTe Certified Privacy Seal

5. **Service Organizational Control (SOC) 2 compliance.**
   - SOC 2 certification is designed for a technology and cloud computing organizations. It provides the assurance that a service provider delivers secure, reliable and effective systems for information storage, com

Cloud Service Provider Certifications – continued

6. **ISO 27001 Certification**
   - Certification of the ISMS supporting the Cloud Services

7. **ISO/IEC 20000-7: Application of ISO/IEC 20000-1 to the cloud.**
   - Currently being developed.
   - To provide guidance on application of ISO/IEC 20000 Part 1 to the cloud.

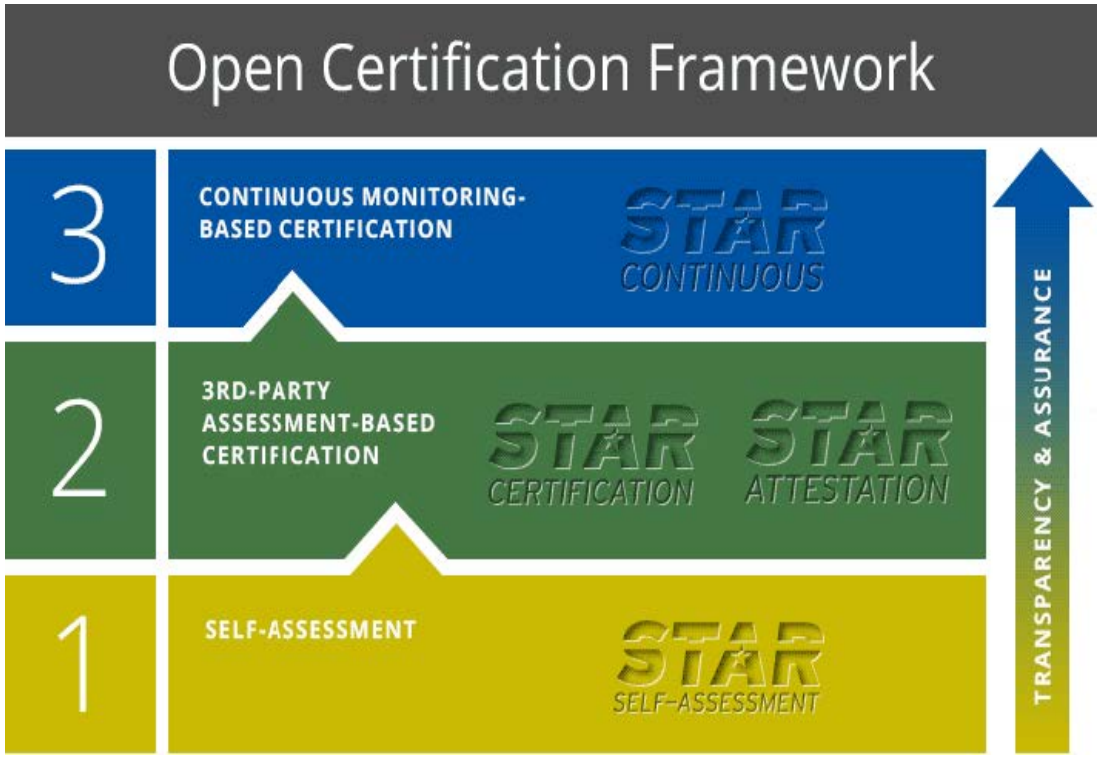
8. **Hybrid Certification (externally certified and audited)**
   - Service Organization Controls 1 (SOC 1) Type II report
   - Service Organization Controls 2 (SOC 2) Type II report
   - ISO 27001 certification
   - PCI DSS Level 1
   - US Federal Risk and Authorization Management Program (FedRamp)
   - Audits including; ITAR, FIPS 140-2, FISMA/DIACAP, HIPAA …
   - This approach is used by Amazon AWS, Rackspace and Microsoft Azure.

9. **CUMULUS - Certification infrastrUcture for MUlti-Layer cloUd Services**
   - EU-based project for development of certification models, processes and tools

10. **Geography Specific**
    - Hong Kong/Guangdong cloud security assessment and certification scheme
    - Multi-Tier Cloud Security Standard for Singapore (MTCS SS 584:2013)
    - Trusted Cloud Service Certification – China Cloud Computing Promotion and Policy Forum (CCCPPF)

CSA - Open Certification Framework

The STAR approach offers 3 different levels of certification that would align with different levels of required assurance.



- The 1st level, CSA STAR Self-Assessment level, is obtained by registering the results of the Consensus Assessments Initiative Questionnaire (CAIQ) completed by the Cloud Service Provider.
- The 2nd level can be CSA STAR Certification, obtained from an independent assessment from an accredited 3rd party or CSA STAR Attestation, obtained from a conducted SOC 2 report using the AICPA Trust Service Criteria and the CSA CCM.
- The 3rd level, CSA STAR Continuous Monitoring is under development.

- Certification is built upon the globally accepted standard for information security management systems (ISO 27001).

Deloitte.

Questions?