AST

Audit de Sécurité Technique

Chapter 1.2

Regulatory framework and certification process

Jean-Marc Bost

jean-marc.bost@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

- Standards and regulatory framework
- ISO 27001 standard
- Other ISO 2700x standards
- ISO 27001 certification process

- **Standards and regulatory framework**
- ISO 27001 standard
- Other ISO 2700x standards
- ISO 27001 certification process

What is ISO ?

- International Standards Organisation
  - Independent, non-governmental
  - Central secretariat in Geneva
- Network of national bodies from 160+ countries
  - Fund the central secretariat + standards and technical projects
  - Coordination of international standardisation activities
- Final results of ISO activities are published as international standards
- Since 1947 over 19’000 standards have been published

ISO Standards

1. Equal representation: 1 vote per country

2. Voluntary membership: ISO does not have the authority to force adoption of its standards

3. Business orientation: ISO only develops standards for which a market demand exists

4. Consensus approach: looking for a large consensus among the different stakeholders

5. International cooperation: over 160 member countries

8 ISO Management Principles

1. **Customer focus**: Organisations depend on their customers and therefore should understand current and future needs, meet customer requirements and exceed customer expectations.
2. **Leadership**: Leaders establish unity of purpose and direction of the organisation. They should create and maintain the internal environment in which people can become fully involved in achieving organisation's objectives.
3. **Involvement of people**: People at all levels are the essence of the organisation and their full involvement enables their abilities to be used for the organisation's benefit.
4. **Process approach**: A desired result is achieved more efficiently when activities and related resources are managed as a process.
5. **System approach to management**: Identifying, understanding and managing interdependent processes as a system contributes to the effectiveness and efficiency in achieving its objective.
6. **Continual improvement**: continual improvement of the overall performance should be a permanent objective of the organisation.
7. **Factual approach to decision making**: Effective decisions are based on the analysis of data and information.
8. **Mutually beneficial supplier relationship**: Organisation and its suppliers are interdependent and a mutually beneficial relationship enhances the ability of both to create value.

Management system standards

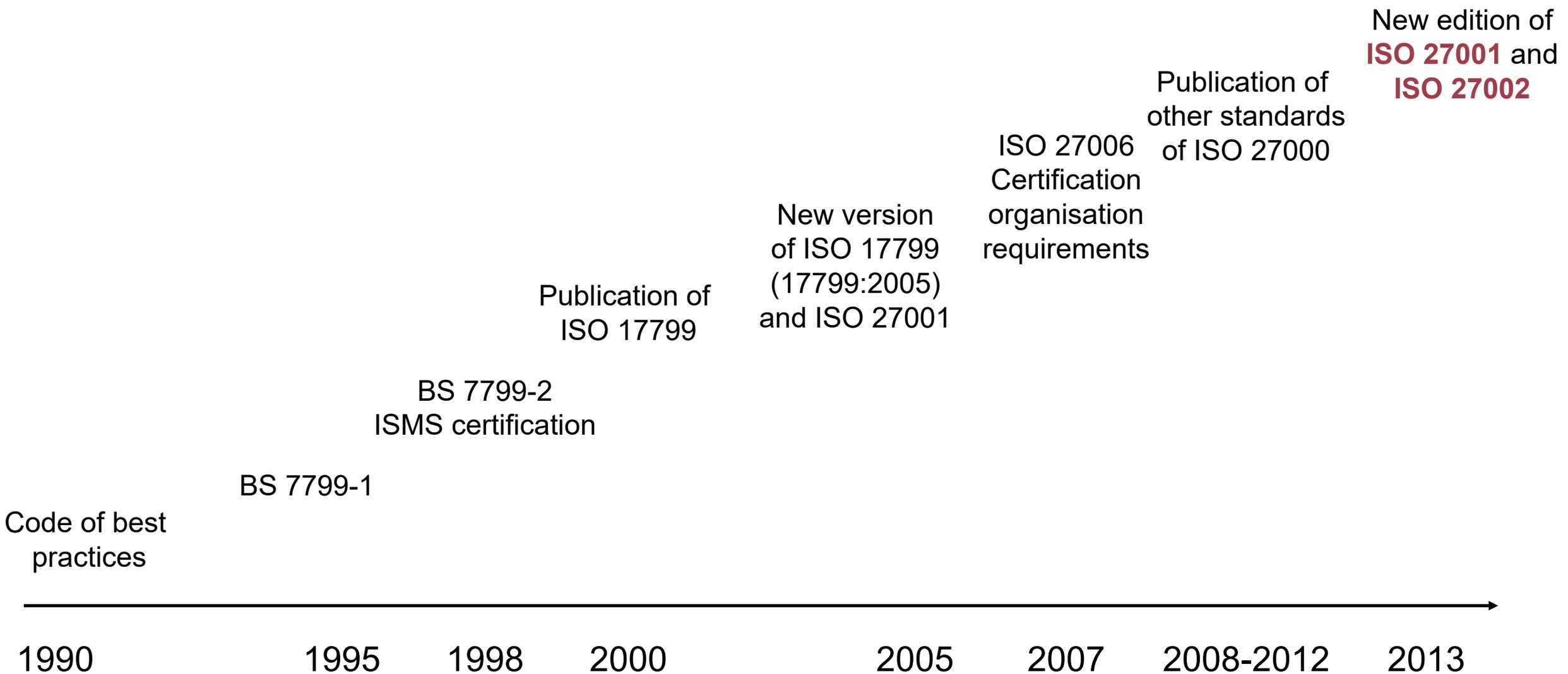
- ISO 9001 - Quality management. Good practices aimed at improving customer satisfaction, achievement of customer requirements and regulatory requirements as well as continuous improvement in those fields.
- ISO 14001 - Environmental management. Actions that the organisation can implement for the maximum reduction of negative impacts of its activities on the environment and for the continuous improvement of its environmental performance.
- ISO 18001 - Health and Safety at the organisation.
- ISO 20000-1 - Requirements for provision of IT services.
- ISO 22000 - Food safety. Applies to all organisations involved in the food supply chain and want to implement a system to continuously provide safe food.
- ISO 22301 - Business Continuity Management Process. Resilience of organisation in case of disaster.
- ISO 27001 - Information Security Management.
- ISO 28000 - Security management of the supply chain.

Other information security standards

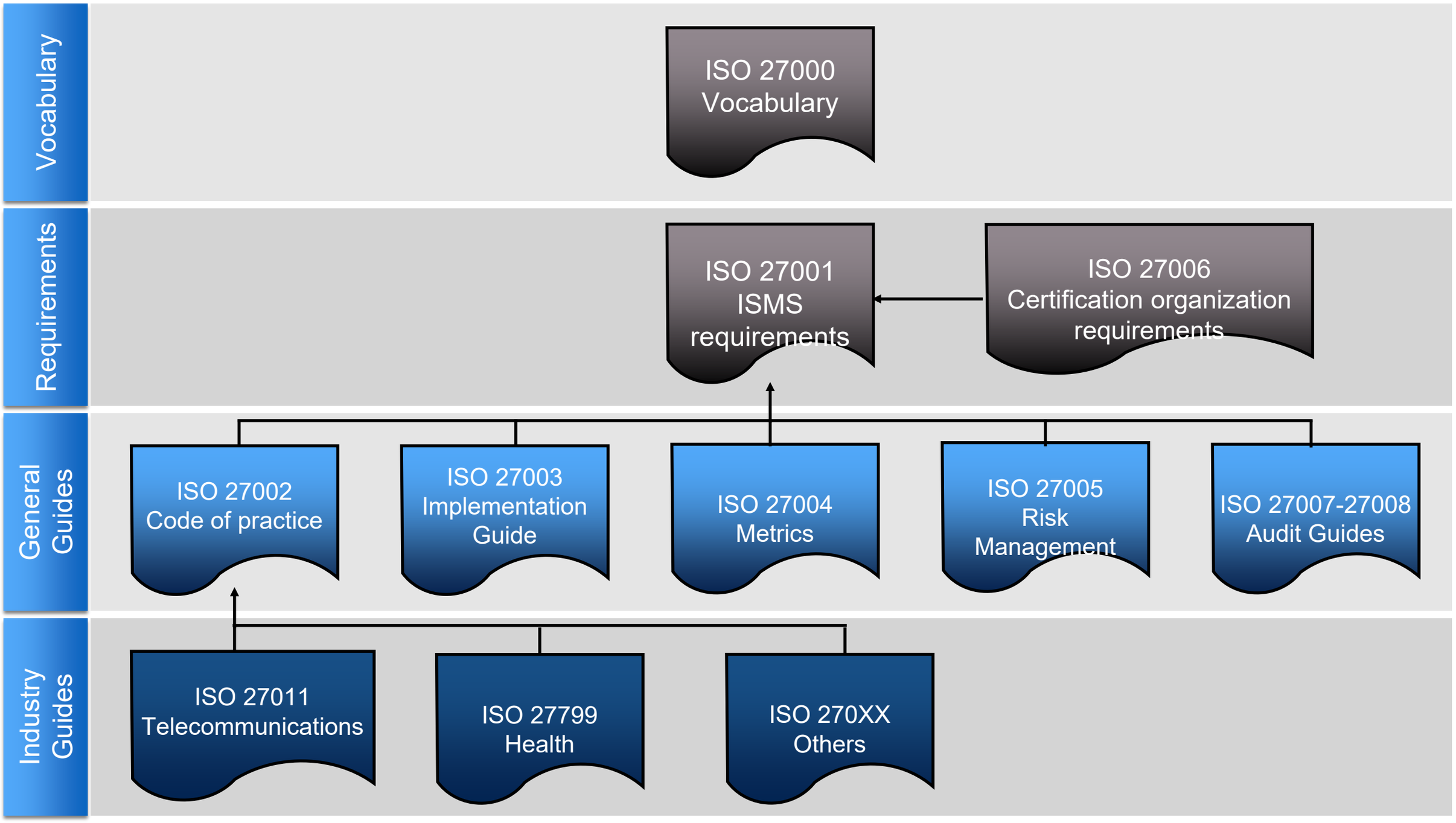
- ISO 9798 - Entity authentication. General model and requirements for the use of identity authentication mechanisms.
- ISO 11770 - Key management. General model for key management independent of cryptographic algorithm.
- ISO 15408 - Common Criteria. Evaluation of security properties of products and systems in IT.
- ISO 21827 - Capability maturity model. Essential characteristics fo an organisation’s security engineering process in order to ensure good security.
- ISO 24761 - Biometrics. Structure and elements for biometrics-based authentication.
- ISO 27033 - Network security. Defines and describes associated concepts.

- Standards and regulatory framework
- **ISO 27001 standard**
- Other ISO 2700x standards
- ISO 27001 certification process

History of ISO 27001



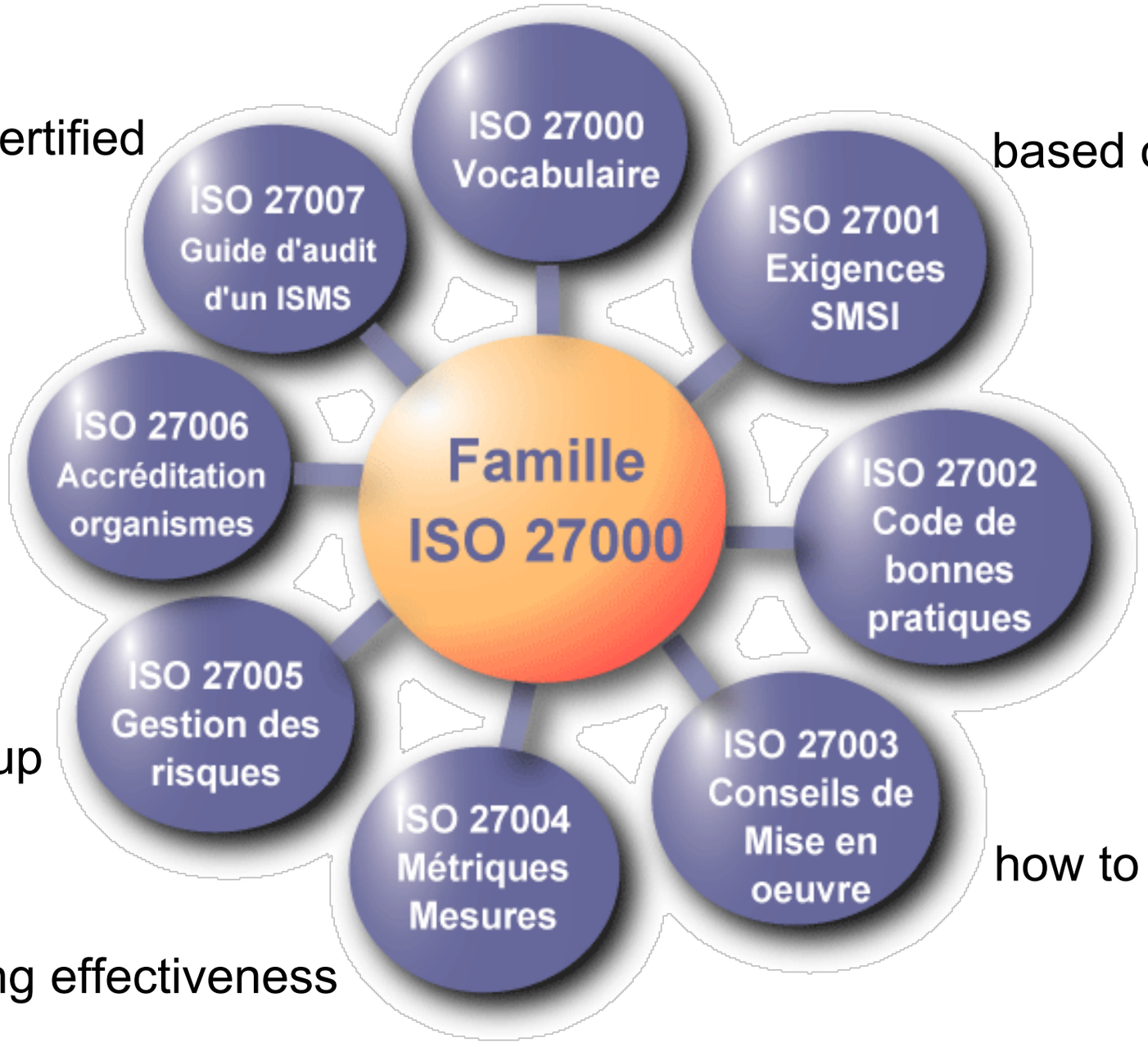
ISO 27000 Family



ISO 27000 Family

- ISO 27001:2013 is the only certifiable standard of the ISO 27000 family. Other standards are guidelines.

getting certified



based on risk, shall

certifying

according to best practives, should

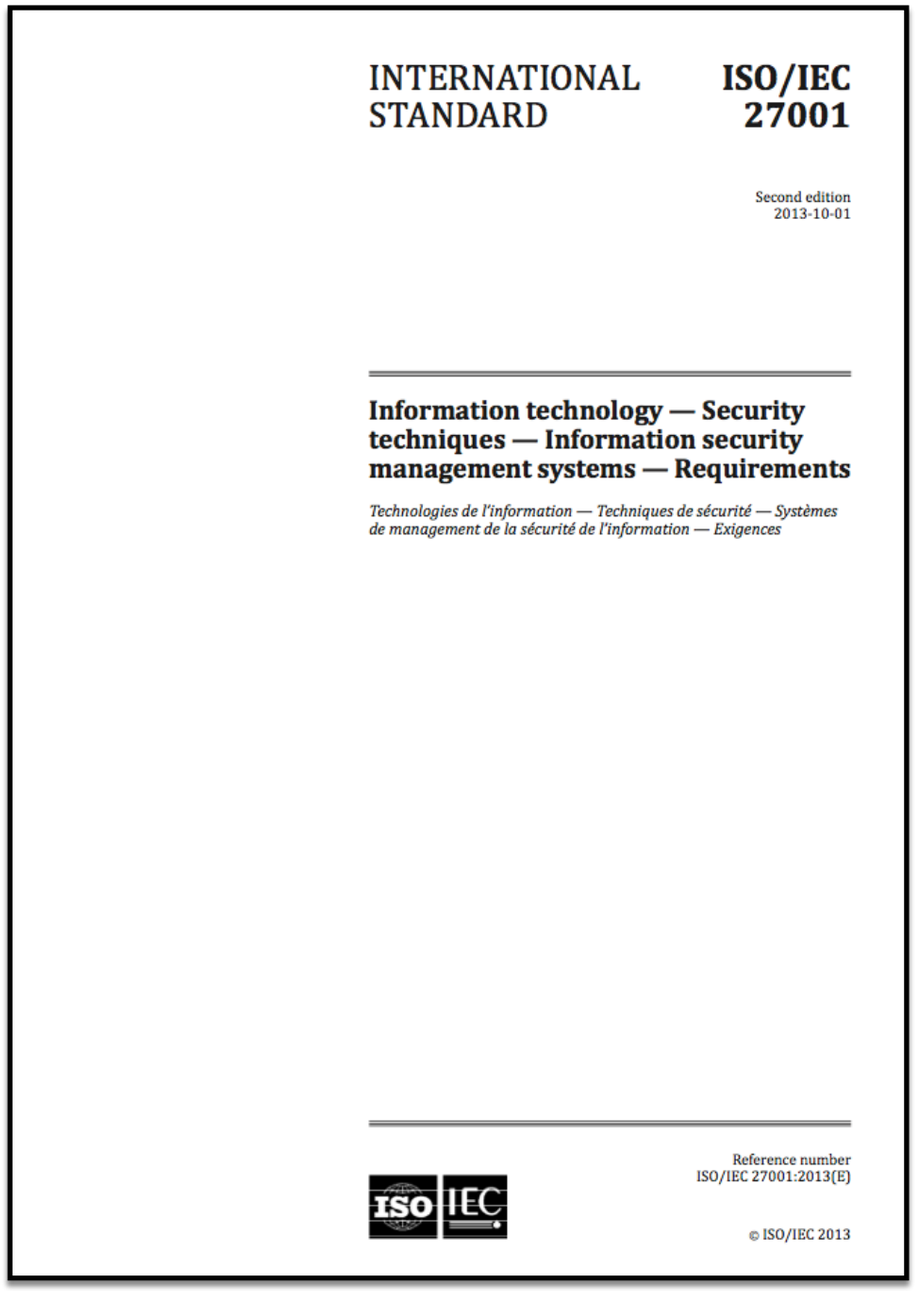
risk follow up

how to

evaluating effectiveness

ISO 27001

- Specifies requirements for ISMS management (*Clauses 4-10*)
- Requirements (clauses) are written using the imperative verb « shall »
- Annex A: 14 clauses containing 35 controls objectives and 114 controls
- Organisations can obtain certification against this standard
- An international standard to suit all types of organisations (e.g. commercial, government, nonprofit)


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

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

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

ISO 27001 – Annexe A

ISO27k Statement of Applicability

ISO 27001 security

Déclaration d'applicabilité

À jour au: JJ/MM/AAAA

Légende (pour les mesures sélectionnées et raisons de sélection des mesures)
LR: exigences légales, **CO**: obligations contractuelles, **BR/BP**: exigences opérationnelles/meilleures pratiques adoptées, **RRA**: résultats d'appréciation des risques, **TSE**: jusqu'à un certain point

ISO/IEC 27001:2013 Annexe A mesure de sécurité			mesures actuelles	Remarques (avec justification des exclusions)	mesures sélectionnées et raisons de sélection				Remarques (aperçu de la mise en œuvre)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
5 Politiques de sécurité	5.1	Orientations de la direction en matière de sécurité de l'information							
	5.1.1	Politiques de sécurité de l'information							
	5.1.2	Revue des politiques de sécurité de l'information							
6 Organisation de la sécurité de l'information	6.1	Organisation interne							
	6.1.1	Fonctions et responsabilités liées à la sécurité de l'information							
	6.1.2	Relations avec les autorités							
	6.1.3	Relations avec des groupes de travail spécialisés							
	6.1.4	La sécurité de l'information dans la gestion de projet							
	6.1.5	Séparation des tâches							
	6.2	Appareils mobiles et télétravail							
	6.2.1	Politique en matière d'appareils mobiles							
	6.2.2	Télétravail							
7 Sécurité des ressources humaines	7.1	Avant l'embauche							
	7.1.1	Sélection des candidats							
	7.1.2	Termes et conditions d'embauche							
	7.2	Pendant la durée du contrat							
	7.2.1	Responsabilités de la direction							
	7.2.2	Sensibilisation, apprentissage et formation à la sécurité de l'information							
	7.2.3	Processus disciplinaire							
	7.3	Rupture, terme ou modification du contrat de travail							
	7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail							

ISO 27001 – Annexe A

	8.1	Responsabilités relatives aux actifs							
	8.1.1	Inventaire des actifs							
	8.1.2	Propriété des actifs							
	8.1.3	Utilisation correcte des actifs							
	8.1.4	Restitution des actifs							
	8.2	Classification de l'information							
8 Gestion des actifs	8.2.1	Classification des informations							
	8.2.2	Marquage des informations							
	8.2.3	Manipulation des actifs							
	8.3	Manipulation des supports							
	8.3.1	Gestion des supports amovibles							
	8.3.2	Mise au rebut des supports							
	8.3.3	Transfert physique des supports							
	9.1	Exigences métier en matière de contrôle d'accès							
	9.1.1	Politique de contrôle d'accès							
	9.1.2	Politique relative à l'utilisation de services en réseau							
	9.2	Gestion de l'accès utilisateur							
	9.2.1	Enregistrement et désinscription des utilisateurs							
	9.2.2	Provisionnement des accès utilisateurs							
	9.2.3	Gestion des privilèges							
	9.2.4	Gestion des informations secrètes d'authentification des utilisateurs							
9 Contrôle d'accès	9.2.5	Revue des droits d'accès utilisateurs							
	9.2.6	Suppression ou adaptation des droits d'accès							
	9.3	Responsabilités des utilisateurs							
	9.3.1	Utilisation d'informations secrètes d'authentification							
	9.4	Contrôle de l'accès au système et à l'information							
	9.4.1	Restriction d'accès à l'information							
	9.4.2	Sécuriser les procédures de connexion							
	9.4.3	Système de gestion des mots de passe							
	9.4.4	Utilisation de programmes utilitaires à privilèges							
	9.4.5	Contrôle d'accès au code source du programme							
	10.1	Mesures cryptographiques							
10 Cryptographie	10.1.1	Politique d'utilisation des mesures cryptographiques							
	10.1.2	Gestion des clés							
	11.1	Zones sécurisées							
	11.1.1	Périmètre de sécurité physique							
	11.1.2	Contrôles physiques des accès							
	11.1.3	Sécurisation des bureaux, des salles et des équipements							

ISO 27001 – Annexe A

11 Sécurité physique et environnementale	11.1.4	Protection contre les menaces extérieures et environnementales							
	11.1.5	Travail dans les zones sécurisées							
	11.1.6	Zones de livraison et de chargement							
	11.2	Matériels							
	11.2.1	Emplacement et protection du matériel							
	11.2.2	Services généraux							
	11.2.3	Sécurité du câblage							
	11.2.4	Maintenance du matériel							
	11.2.5	Sortie des actifs							
	11.2.6	Sécurité du matériel et des actifs hors des locaux							
	11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel							
	11.2.8	Matériel utilisateur laissé sans surveillance							
	11.2.9	Politique du bureau propre et de l'écran vide							
12 Sécurité liée à l'exploitation	12.1	Procédures et responsabilités liées à l'exploitation							
	12.1.1	Procédures d'exploitation documentées							
	12.1.2	Gestion des changements							
	12.1.3	Dimensionnement							
	12.1.4	Séparation des environnements de développement, de test et d'exploitation							
	12.2	Protection contre les logiciels malveillants							
	12.2.1	Mesures contre les logiciels malveillants							
	12.3	Sauvegarde							
	12.3.1	Sauvegarde des informations							
	12.4	Journalisation et surveillance							
	12.4.1	Journalisation des événements							
	12.4.2	Protection de l'information journalisée							
	12.4.3	Journaux administrateur et opérateur							
	12.4.4	Synchronisation des horloges							
	12.5	Maîtrise des logiciels en exploitation							
	12.5.1	Installation de logiciels sur des systèmes en exploitation							
	12.6	Gestion des vulnérabilités techniques							
	12.6.1	Gestion des vulnérabilités techniques							
	12.6.2	Restrictions liées à l'installation de logiciels							
	12.7	Considérations sur l'audit des systèmes d'information							
	12.7.1	Mesures relatives à l'audit des systèmes d'information							
13 Sécurité des communications	13.1	Gestion de la sécurité des réseaux							
	13.1.1	Contrôle des réseaux							
	13.1.2	Sécurité des services de réseau							
	13.1.3	Cloisonnement des réseaux							
	13.2	Transfert de l'information							
	13.2.1	Politiques et procédures de transfert de l'information							

ISO 27001 – Annexe A

	13.2.2	Accords en matière de transfert d'information							
	13.2.3	Messagerie électronique							
	13.2.4	Engagements de confidentialité ou de non-divulgation							
	14.1	Exigences de sécurité applicables aux systèmes d'information							
	14.1.1	Analyse et spécification des exigences de sécurité							
	14.1.2	Sécurisation des services d'application sur les réseaux publics							
	14.1.3	Protection des transactions liées aux services d'application							
	14.2	Sécurité des processus de développement et d'assistance technique							
14 Acquisition, développement et maintenance des systèmes d'information	14.2.1	Politique de développement sécurisé							
	14.2.2	Procédures de contrôle des changements							
	14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation							
	14.2.4	Restrictions relatives aux changements apportés aux progiciels							
	14.2.5	Procédures de développement des systèmes							
	14.2.6	Environnement de développement sécurisé							
	14.2.7	Développement externalisé							
	14.2.8	Phase de test de la sécurité du système							
	14.2.9	Test de conformité du système							
	14.3	Données de test							
	14.3.1	Protection des données de test							
	15.1	Sécurité dans les relations avec les fournisseurs							
	15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs							
15 Relations avec les fournisseurs	15.1.2	Sécurité dans les accords conclus avec les fournisseurs							
	15.1.3	chaîne d'approvisionnement informatique							
	15.2	Gestion de la prestation du service							
	15.2.1	Surveillance et revue des services des fournisseurs							
	15.2.2	Gestion des changements apportés dans les services des fournisseurs							
	16.1	Gestion des incidents liés à la sécurité de l'information et améliorations							
	16.1.1	Responsabilités et procédures							
16 Gestion des incidents liés à la sécurité de l'information	16.1.2	Signalement des événements liés à la sécurité de l'information							
	16.1.3	Signalement des failles liées à la sécurité de l'information							
	16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision							

ISO 27001 – Annexe A

	16.1.5	Réponse aux incidents liés à la sécurité de l'information							
	16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information							
	16.1.7	Recueil de preuves							
	17.1	Continuité de la sécurité de l'information							
17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	17.1.1	Organisation de la continuité de la sécurité de l'information							
	17.1.2	Mise en oeuvre de la continuité de la sécurité de l'information							
	17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information							
	17.2	Redondances							
	17.2.1	Disponibilité des moyens de traitement de l'information							
	18.1	Conformité aux obligations légales et réglementaires							
	18.1.1	Identification de la législation et des exigences contractuelles applicables							
	18.1.2	Droits de propriété intellectuelle (DPI)							
	18.1.3	Protection de l'information documentée							
18 Conformité	18.1.4	Protection de la vie privée et protection des données à caractère personnel							
	18.1.5	Réglementation relative aux mesures cryptographiques							
	18.2	Revue de la sécurité de l'information							
	18.2.1	Revue indépendante de la sécurité de l'information							
	18.2.2	Conformité avec les politiques et les normes de sécurité							
	18.2.3	Examen de la conformité technique							

ISO 27001 Benefits

1. Improvement of security

- General improvement of the effectiveness of information security
- Several aspects covered: technology, corporate, physical
- Independent review of organisation's ISMS
- Better awareness to information security
- Mechanisms to measure the effectiveness of the management system

2. Good governance

- Awareness of personnel
- Decrease of lawsuit risks (due care and due diligence)
- Opportunity to identify weaknesses and provide corrections
- Accountability of top management for information security

3. Conformity

- To other ISO standards
- To industry standards (e.g. PCI-DSS)
- National laws and regulations

4. Cost reduction

- Justification of the profitability of projects and measurable return-benefit

5. Marketing

- Competitive advantage for the organisation
- Customer, suppliers and partners confidence

Legal conformity

- Organisations must comply with applicable laws and regulations.
- Implementation of an ISO standard is a voluntary decision of the organisation, not a legal requirement
- In all cases, laws take precedence over standards
- ISO 27001 can be used to comply to several laws and regulations
  - Clause 18.1: Compliance with legal and contractual requirements
    - Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
  - Clause 18.1.1: Identification of applicable legislation and contractual requirements
    - Control: All relevant legislative, statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organisation.

Legal Aspects

1. Data protection

- Aspects related to safeguarding confidentiality and data integrity of personal data.

2. Privacy

- Regulatory, legal and business requirements regarding the treatment and protection of personally identifiable information (PII)
- Enable the organisation to meet its commercial liability, legal and regulatory obligations in respect of PII

3. Identification and prosecution of computer crime

- Necessary awareness and adequate countermeasures in compliance with applicable laws
- Evidence collection must respect legislation
- Protective measures cannot themselves be crimes

4. Use of digital signature

- In some countries, electronic records must ensure the preservation of traces as evidence of integrity to be considered valid in case of litigation

5. Intellectual property (IP)

- IP is the cornerstone for the competition between companies
- Proper management of human IP can help smaller companies to compete with bigger ones

6. Commerce and electronic payments

- Proof of transaction

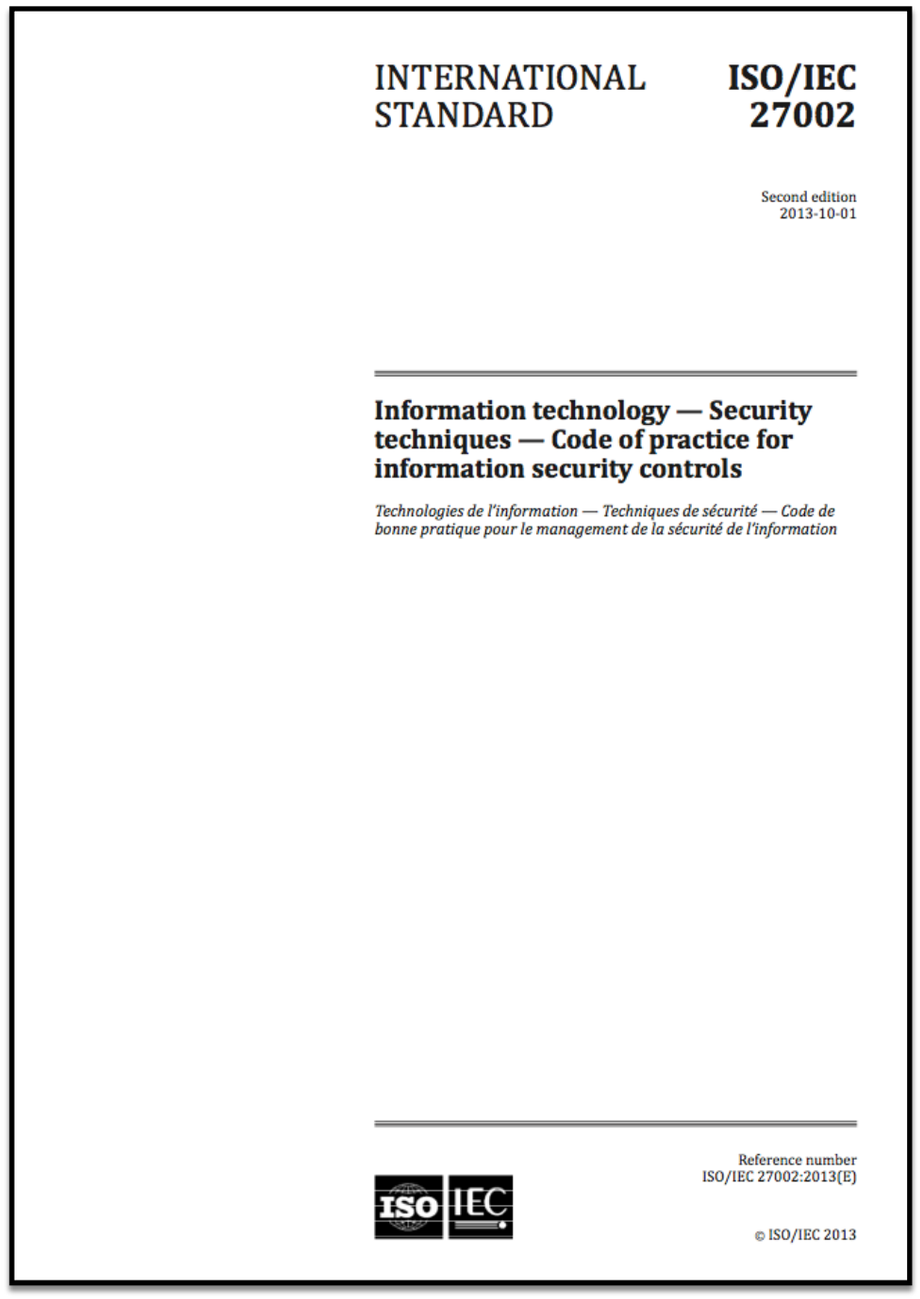
7. Records management

- Necessary for the annual financial audit

- Standards and regulatory framework
- ISO 27001 standard
- **Other ISO 2700x standards**
- ISO 27001 certification process

ISO 27002

- Guide for code of practice for information security controls (Reference document)
- Clause written using the verb « should »
- Composed of 14 clauses, 35 control objectives and 114 controls
- Organizations can not obtain certification against this standard
- Clauses 5 to 18 provide specific advice and an implementation guide related to the best practices to support the controls specified in Annex A of ISO 27001


INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

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

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

© ISO/IEC 2013

ISO 27000 Extended family

- ISO 27001:2013 is the only certifiable standard of the ISO 27000 family. Other standards are guidelines.
- ISO 27000: Basic concepts and vocabulary that applies to ISMS.
- ISO 27001: Requirements of the ISMS.
- ISO 27002: Best practices guide for management of information security.
- ISO 27003: Guide for implementing the ISMS
- ISO 27004: Metrics for ISMS management. Objectives for implementation and effectiveness criteria.
- ISO 27005: Guide for information security risk management compliant with the concepts, models and general processes of ISO 27001.
- ISO 27006: Guide for organisations auditing and certifying ISMS.
- ISO 27007: Guidelines for ISMS auditing.
- ISO 27008: Guidelines for auditors on information security controls.
- …
- ISO 27011: Guidelines for the use of ISO 27002 in Telecom industry.
- ISO 27031: Guidelines for information and communication technology readiness for business continuity.
- ISO 27799: Guidelines for the use of ISO 27002 in Health industry.

ISO 27009+

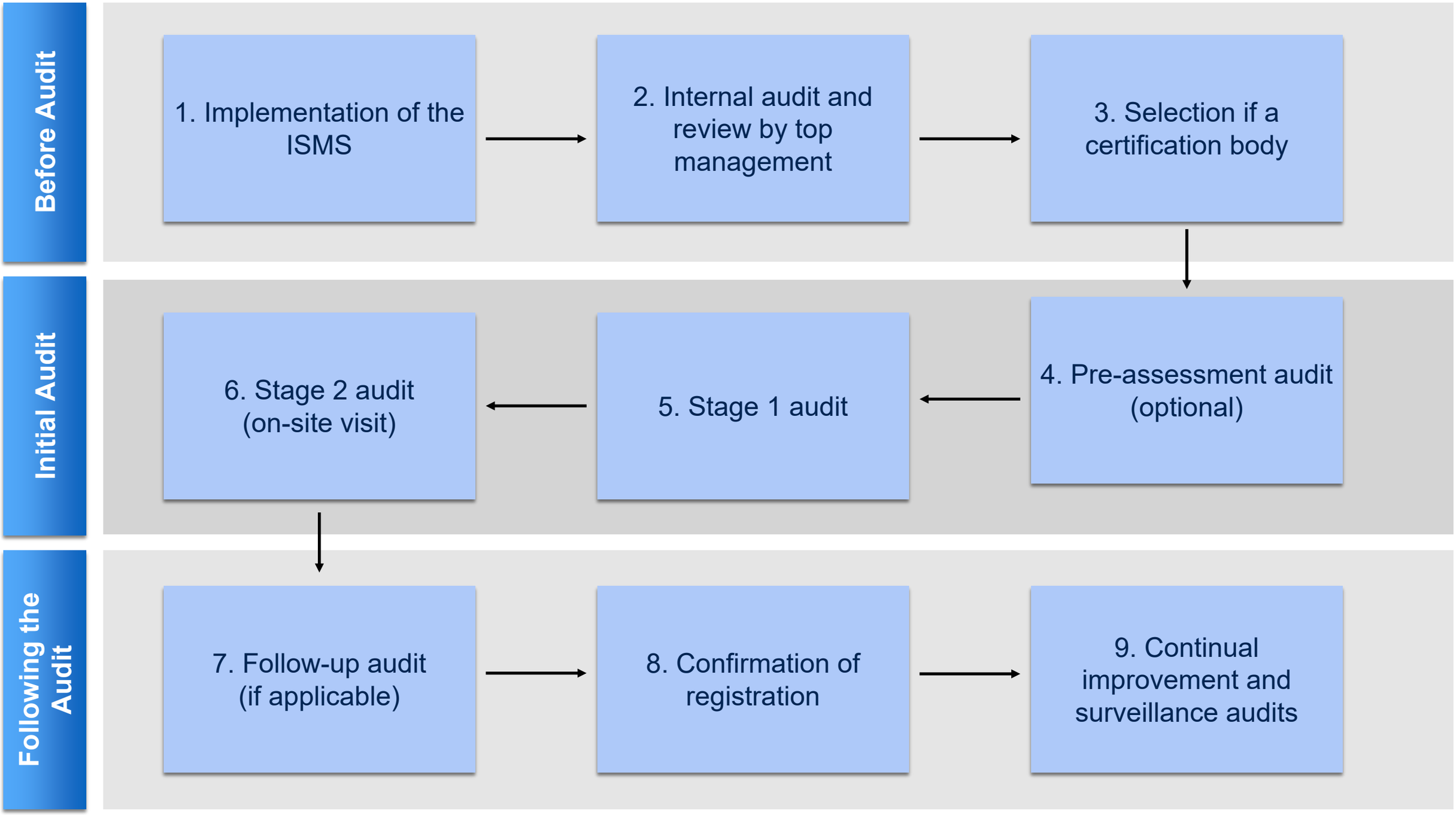
- Within ISO 27000 series, ISO 27009 and subsequent numbers are reserved for the creation of domain-specific standards

  - For industries:
    - Telecom
    - Health
    - Finance and insurance

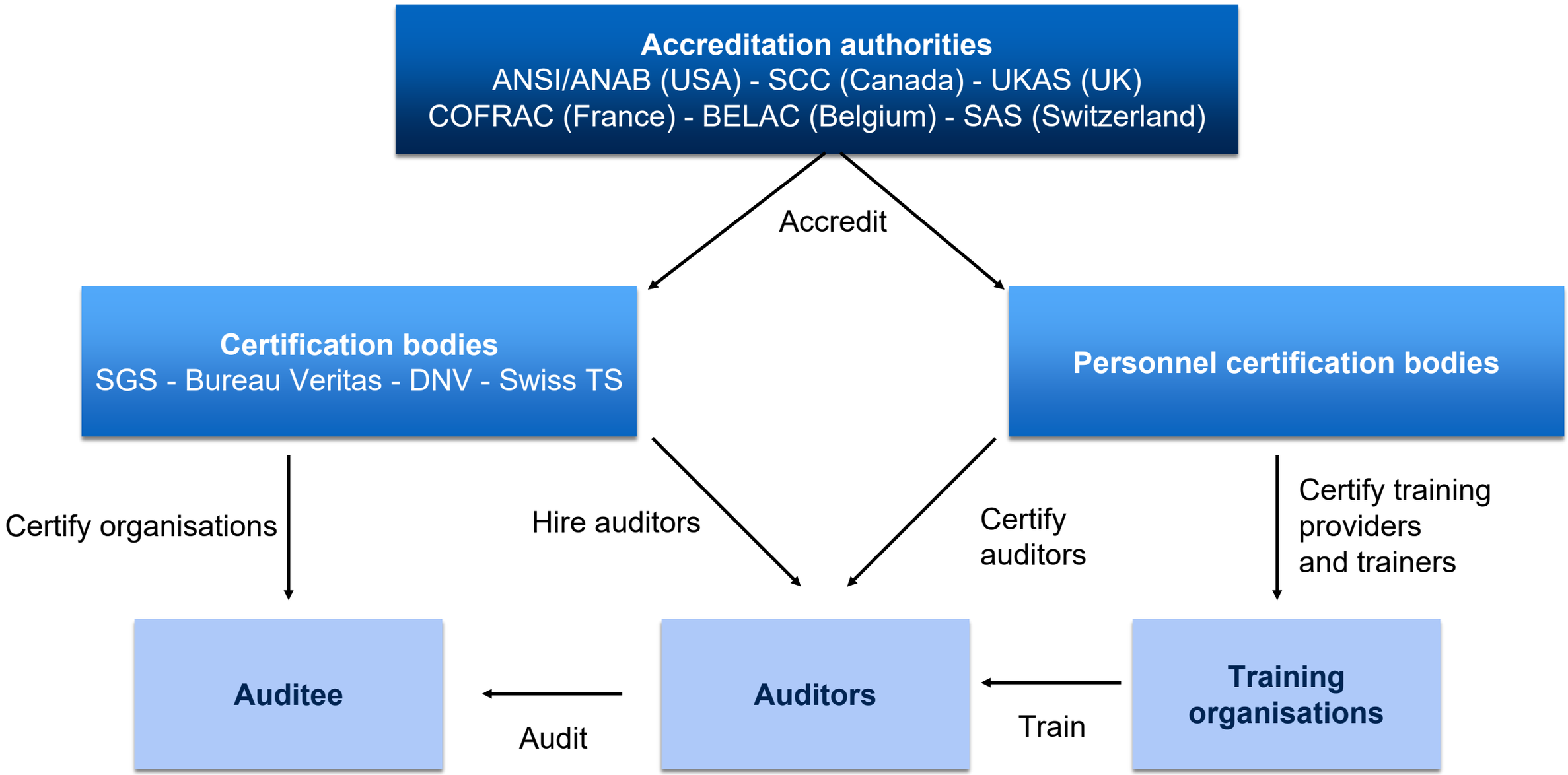
  - For specific sectors related to information security:
    - Application security
    - Security incident management
    - Privacy protection

- Standards and regulatory framework
- ISO 27001 standard
- Other ISO 2700x standards
- **ISO 27001 certification process**

Certification process



Certification Schema



Authorities and bodies

- **Accreditation authority**
  - National organisation which supervises certification programs and which makes sure that national or inter nation criteria are respected

- **Certification Body**
  - Third party which performs the assessment of conformity of management systems
  - Certification - procedure in which a third party attests in writing that a product, process, service or a person is conform ant to specified criteria

- **Personnel certification bodies**
  - Certify professionals