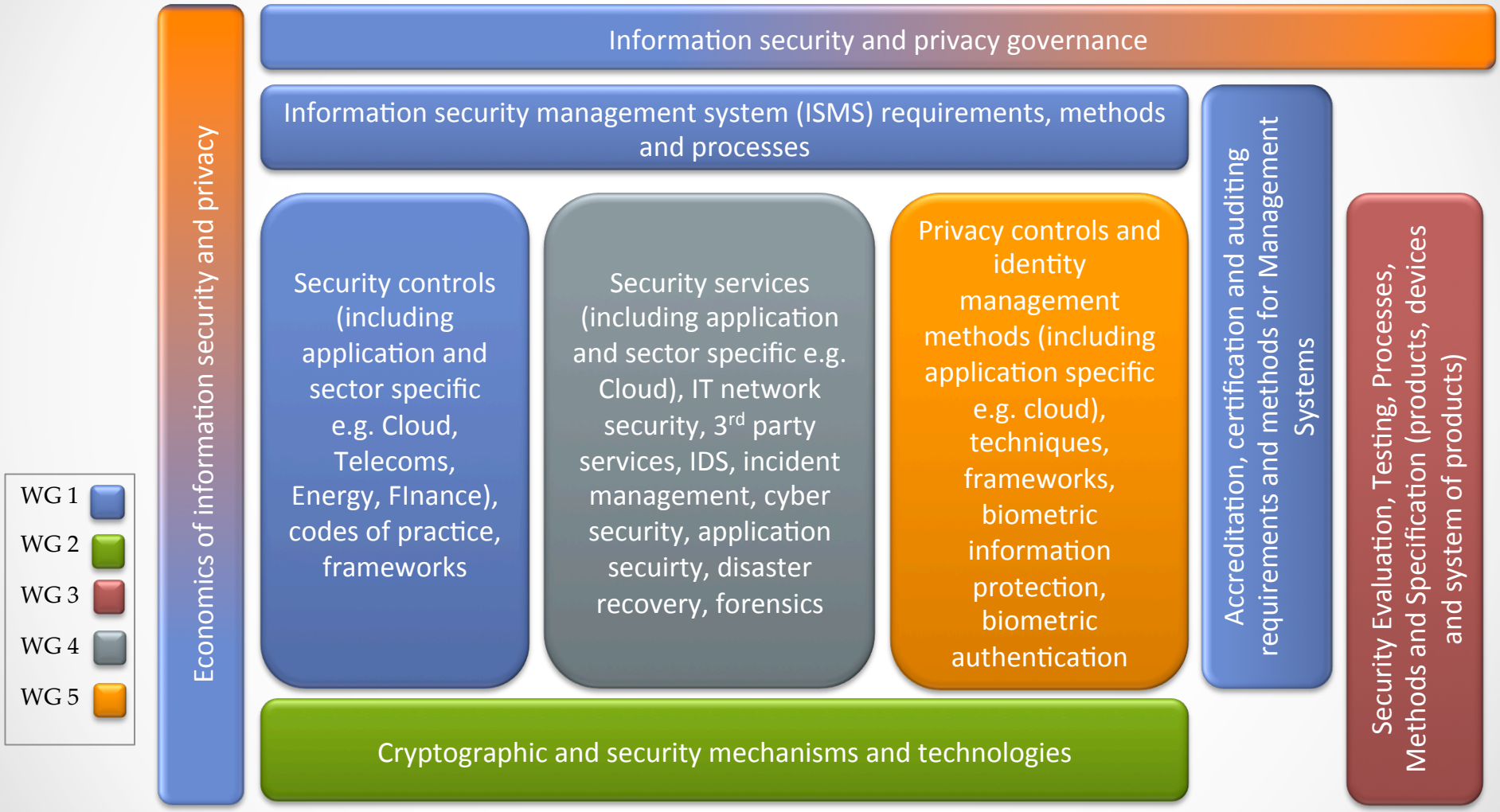
ISO/IEC JTC 1/ SC 27 WG1 ISMS Standards

Edward Humphreys
WG 1 Convenor
edwardj7@msn.com

Security and Privacy Topic Areas



SC27 WG1 Mission

Information Security Management Systems

The scope covers all aspects of standardisation related to information security management systems:

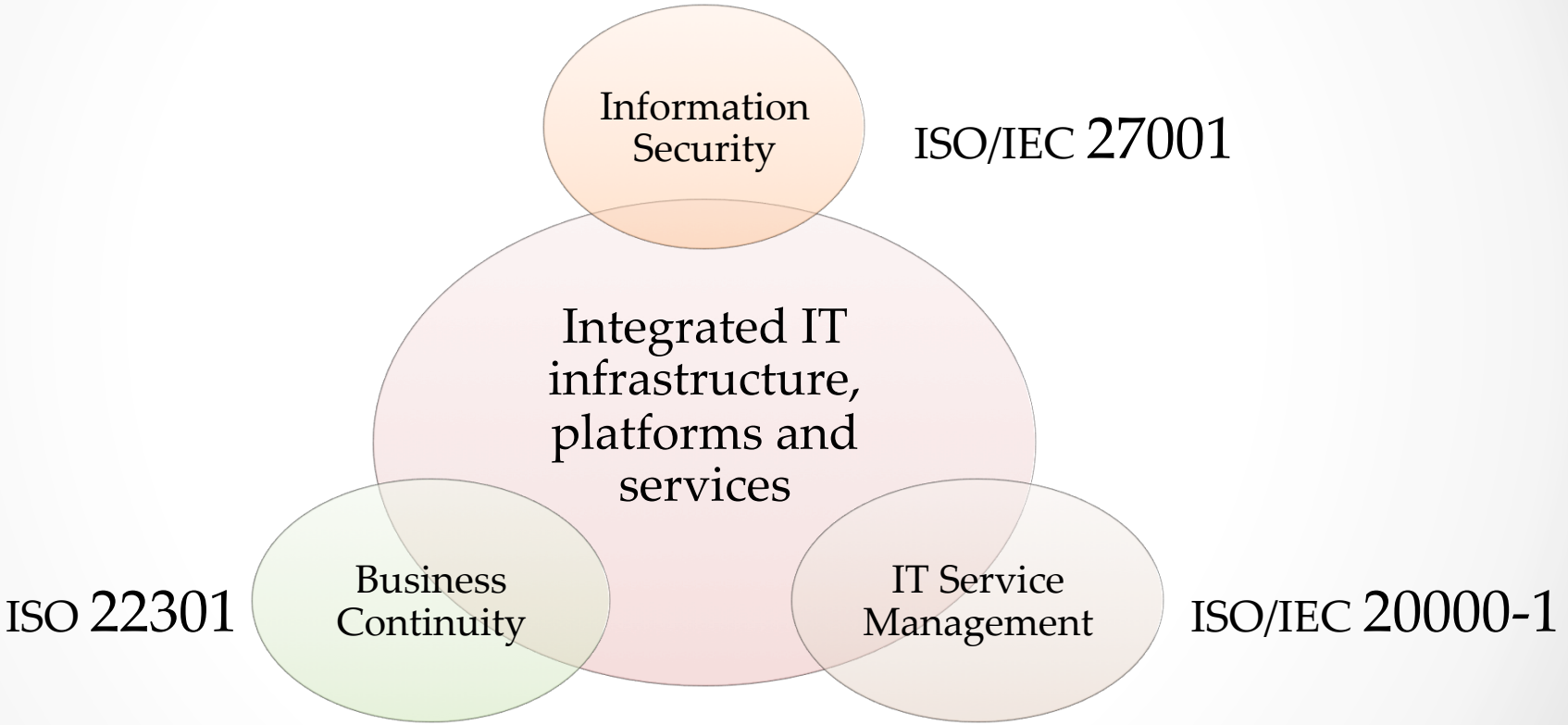
a) Requirements;
b) Methods and processes;
c) Security controls;
d) Sector and application specific use of ISMS;
e) Accreditation, certification, auditing of ISMS;
f) Governance;
g) Information security economics.

WG1 ISMS Standard (type A)

Standard	Title	Status	Abstract
ISO/IEC 27001	Information security management systems – Requirements	1st ed. 2005 Under revision (FDIS)	This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's business activities and the risks it faces.

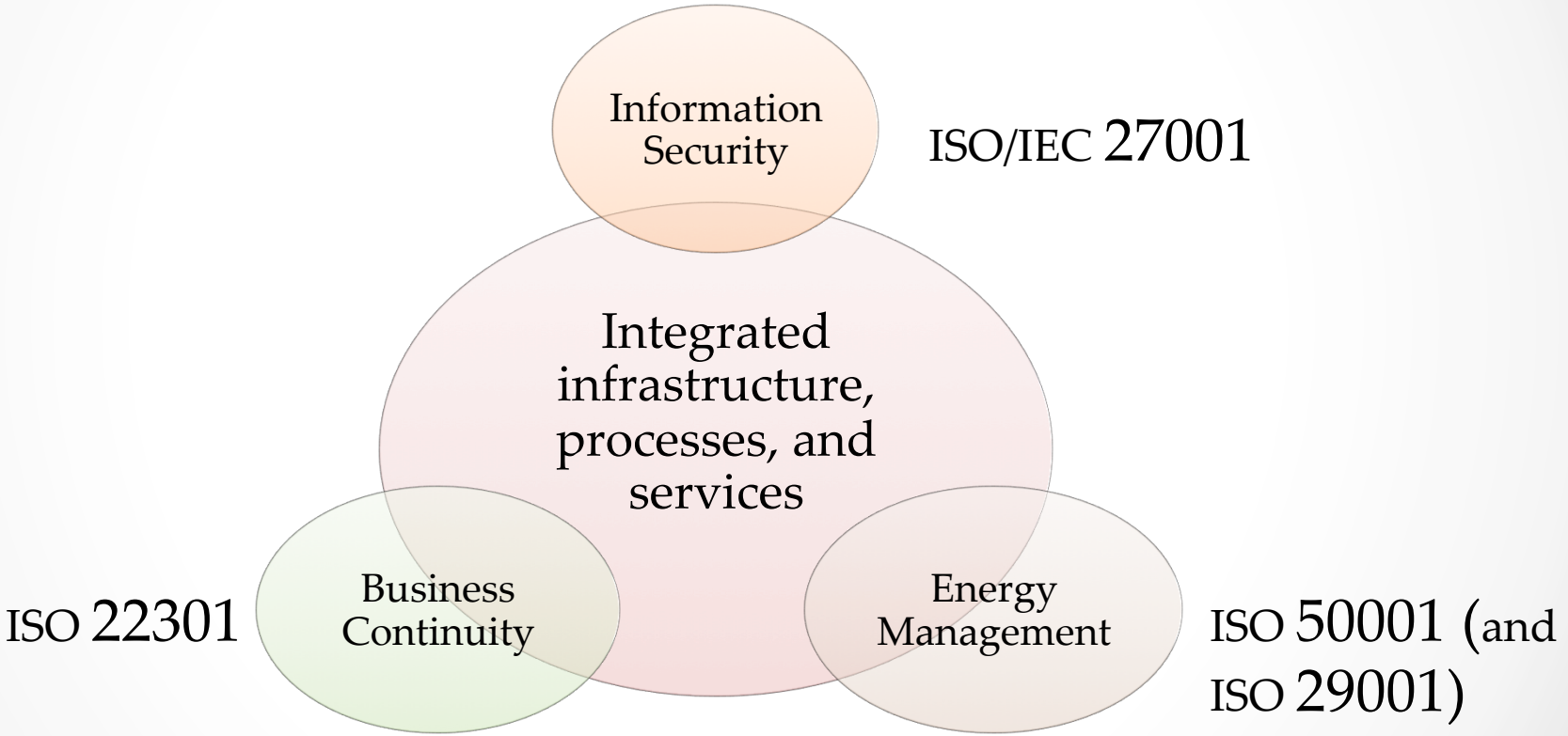
- Information security, risk based, continuous improvement enabled management system standard
- The biggest selling of all information security management standard (millions of copies sold)
- The current number of 27001 3rd party certifications is 14,000+ across 100 countries and covering every market sector
- Revised version – aligned to the Next Generation of Management System Standards (providing integrated application platform, service and infrastructure capability)

ISO/IEC 27001 - Example Integrated (Next Generation) Management System Environment



Some operational benefits: integrated – risk management and impact assessment, incident handling, asset management, trusted service management …

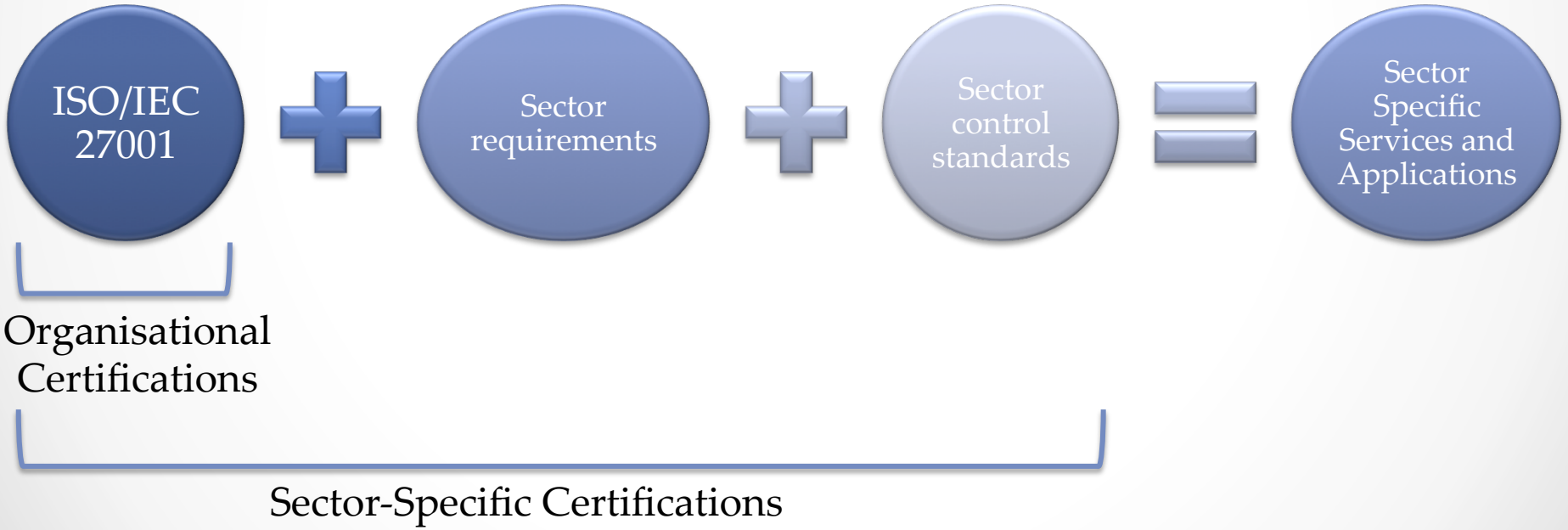
ISO/IEC 27001 - Example Integrated (Next Generation) Management System Environment



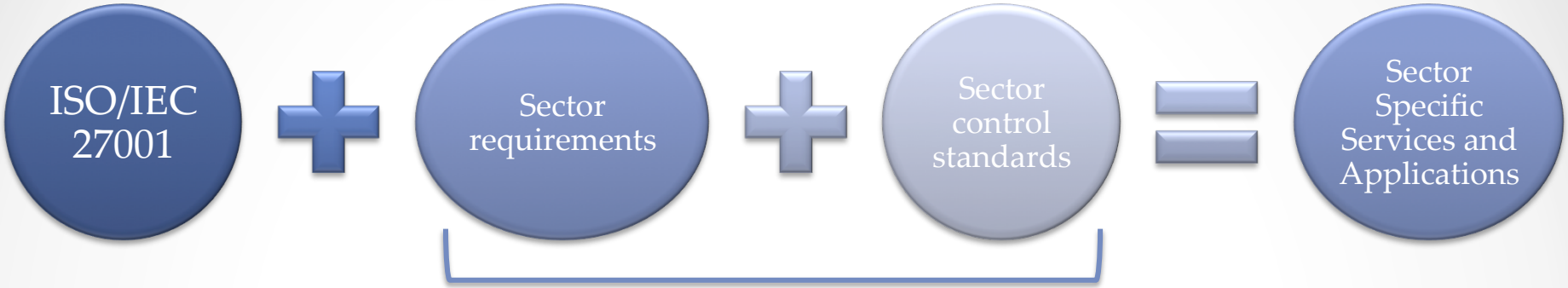
For example, for the Oil and Gas Industry possibly also integrated with ISO 29001 (oil and gas management system)

ISO/IEV 27009 Applying 27001 for Certification

Standard	Title	Status	Abstract
ISO/IEC 27009	Application of ISO/IEC 27001	WD	This standard considers the use of ISO/IEC 27001 for sector-specific applications.



ISO/IEC 27009 Use of 27001 for Sector-Specific Applications (Examples)



- *Telecoms (ISO/IEC 27011)*
- *Finance (ISO/IEC 27015 & ISO 13569)*
- *Healthcare (ISO 27799)*
- *Cyber-security (ISO/IEC 27031 +)*
- *Cloud (ISO/IEC 27017 & 17018)*
- *Industrial Control Systems*

- *Network Security Services (ISO/IEC 27033)*
- *ICT Readiness for Business Continuity (ISO/IEC 27031) and Incident Handling Services (ISO/IEC 27034)*
- *Disaster Recovery Services (ISO/IEC 24762)*
- *Supplier Relationships (ISO/IEC 27036)*
- *PII (ISO/IEC 29100 +)*
- *Trusted Services (service management, time-stamping, PKI – ISO/IEC 20000-1, ISO/IEC 29149, ISO/IEC 14516, ISO/IEC 15945, T-Scheme etc)*

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27000	Overview and vocabulary	2nd ed. 2012 Under revision	This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.
ISO/IEC 27002	Code of practice for information security controls	1st ed. 2005 DIS stage	This International Standard offers a collection of commonly accepted information security control objectives and controls and includes guidelines for implementing these controls.
ISO/IEC 27003	Information security management system implementation guidance	1st ed. 2010 Under revision	This will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review and improve the ISMS.

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27004	Information security management measurements	1st ed. 2009 Under revision	This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems.
ISO/IEC 27005	Information security risk management	2nd ed. 2011 Revision is planned	This standard ISO/IEC 27005 provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

WG1 ISMS Certification and Auditing Standards

Standard	Title	Status	Abstract
ISO/IEC 27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	2nd ed. Pub. 2011 2nd WD 2013	The scope of this standard is to specify general requirements a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/ registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration. This International Standard follows the structure of ISO/IEC 17021 with the inclusion of additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification.
ISO/IEC 27007	Guidelines for information security management systems auditing	1st ed. Pub. 2011	This International Standard provides guidance on conducting information security management system (ISMS) audits, as well as guidance on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. It is applicable to internal or external audits of an ISMS.

WG1 ISMS Certification and Auditing Standards

Standard	Title	Status	Abstract
ISO/IEC 27008	Guidelines for auditors on ISMS controls	1st ed. Pub. 2012	This Technical Report provides guidance for assessing the implementation of ISMS controls selected through a risk-based approach for information security management.
NWIP	Requirements for the Certification of Information Security Management Professionals	NWIP Ballot	

WG1 ISMS Sector Standards (type B)

Standard	Title	Status	Abstract
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications	1st ed. Pub. 2012	This International Standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to inter-organisational and inter-sector communications.
ITU-T X. 1051 | ISO/ IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/ IEC 27002	1st ed. 2008 Revision to start Oct 2013	This Recommendation | International Standard: a) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications organizations based on ISO/IEC 27002; b) provides an implementation baseline of Information Security Management within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities and services.

WG1 ISMS Sector Standards (type B)

Standard	Title	Status	Abstract
ISO/IEC 27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	1st ed. Pub. 2012	This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations which are intending to either: a. Implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa; b. Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or c. Align existing ISO/IEC 27001 and ISO/IEC 20000-1 management system (MS) implementations.

WG1 ISMS Sector Standards (type B)

Standard	Title	Status	Abstract
ISO/IEC 27014	Governance of information security	1st ed. Pub. 2013	This International Standard provides guidance on the development and use of governance of information security (GIS) through which organisations direct and control the information security management system (ISMS) process as specified in ISO/IEC 27001.
ISO/IEC 27015	Information security management guidelines for financial services	1st ed. Pub. 2012	This International Standard provides requirements, guidelines and general principles for initiating, implementing, maintaining, and improving the information security management within finance and insurance sectors based upon ISO/IEC 27001 and ISO/IEC 27002.

WG1 ISMS Sector Standards (type B)

Standard	Title	Status	Abstract
ISO/IEC 27016	Information security management - Organisational economics	DTR 2013	This technical report provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources.
ISO/IEC 27017	Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	5th WD 2013	The scope of this Technical Specification/ International Standard is to define guidelines supporting the implementation of Information Security Management for the use of cloud service. The adoption of this Technical Specification/ International Standard allows cloud consumers and providers to meet baseline information security management with the selection of appropriate controls and implementation guidance based on risk assessment for the use of cloud service.