SC27 WG4 Mission

Security controls and services

- Developing and maintaining International Standards, Technical Specifications and Technical Reports for information security in the area of *Security Controls and Services*, to assist organizations in the implementation of the ISO/IEC 27000-series of *Information Security Management Systems* (ISMS) International Standards and Technical Reports

- The scope of WG4 also includes evaluating and developing International Standards for addressing existing and emerging information security issues and needs and other security aspects that resulted from the proliferation and use of ICT and Internet related technology in organizations (such as multi-nationals corporations, SMEs, government departments, and non-profit organisations).

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party services	1st Ed. 2002	This Technical Report provides guidance for the use and management of Trusted Third Party (TTP) services, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. This Technical Report identifies different major categories of TTP services including time stamping, non-repudiation, key management, certificate management, and electronic notary public.
ISO/IEC 15816	Security information objects for access control	1st Ed. 2002	This International Standard provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1).
ISO/IEC 15945	Specification of TTP services to support the application of digital signatures	1st Ed. 2002	This International Standard defines the services required to support the application of digital signatures for non-repudiation of creation of a document. Since this implies integrity of the document and authenticity of the creator, the services described can also be combined to implement integrity and authenticity services.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 18028-3	IT network security – Part 3: Securing communications between networks using security gateways	1st Ed. 2005 (Being revised by ISO/IEC 27033-4)	This International Standard provides an overview of security gateways through a description of different architectures. It outlines the techniques for security gateways to analyse network traffic, and provides guidelines for the selection and configuration of security gateways.
ISO/IEC 18028-4	IT network security – Part 4: Securing remote access	1st Ed. 2005	This International Standard provides guidance for securely using remote access – a method to remotely connect a computer either to another computer or to a network using public networks – and its implication for IT security. In this it introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely.
ISO/IEC 18028-5	IT network security – Part 5: Securing communications across networks using virtual private networks	1st Ed. 2006 (Being revised by ISO/IEC 27033-5)	This International Standard provides detailed direction with respect to the security aspects of using Virtual Private Network (VPN) connections to inter-connect networks, and also to connect remote users to networks. It provides an overview of VPNs, presents VPN security objectives, and summarizes VPN security requirements. It gives guidance on the selection of secure VPNs, on the implementation of secure VPNs, and on the network monitoring of VPN security. It also provides information on typical technologies and protocols used by VPNs.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 18043	Selection, deployment and operations of intrusion detection systems	1st Ed. 2006 (Being revised by ISO/IEC 27039)	This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection System (IDS). In particular, it addresses the selection, deployment and operations of IDS. It also provides background information from which these guidelines are derived.
ISO/IEC 24762	Guidelines for information and communications technology disaster recovery services	1st Ed. 2008	This International Standard provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management, applicable to both "in-house" and "outsourced" ICT DR service providers of physical facilities and services. It covers the requirements that service providers should meet, recognizing that individual organizations may have additional requirements that are specific to them.
ISO/IEC 27031	Guidelines for ICT readiness for business continuity	1st Ed. 2011	This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.
ISO/IEC 27032	Guidelines for cybersecurity	1st Ed. 2012	This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 27033-1	Network Security – Part 1: Overview and concepts	1st Ed. 2009 (Revision of 18028-1) (Currently under revision)	This International Standard provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services and end-users, in addition to security of the information being transferred across the communication links.) Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts.
ISO/IEC 27033-2	Network Security – Part 2: Guidelines for the design and implementation of network security	1st Ed. 2012	This International Standards provides guidelines for organizations to plan, design, implement and document network security.
ISO/IEC 27033-3	Network Security – Part 3: Reference networking scenarios – Risks, design techniques and control issues	1st Ed. 2010	This International Standard describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. The information in this International Standard is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 27034-1	Application security – Part 1: Overview and concepts	1st Ed. 2011	ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications. This International Standard presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.
ISO/IEC 27035	Information security incident management	1st Ed. 2011 (Currently under revision)	This International Standard provides a structured and planned approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.
ISO/IEC 27037	Guidelines for the identification, collection, acquisition and preservation of digital evidence	1st Ed. 2012	ISO/IEC 27037 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.
ISO/IEC TR 29149	Best practice on the provision and use of time-stamping services	1st Ed. 2012	This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness and data integrity services, or non-repudiation services (in conjunction with other mechanisms). It covers time-stamp services, explaining how to generate, renew, and verify time-stamp tokens.