WG3 Mission

Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

a) security evaluation criteria;

b) methodology for application of the criteria;

c) security functional and assurance specification of IT systems, components and products;

d) testing methodology for determination of security functional and assurance conformance;

e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 11889	Trusted Platform Module	1st Ed	ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general.
ISO/IEC 15408	Evaluation criteria for IT security	3rd Ed	ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
ISO/IEC TR 15443	A framework for IT security assurance	2nd Ed.	ISO/IEC TR 15443 guides the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel.
ISO/IEC TR 15446	Guide for the production of Protection Profiles and Security Targets	2nd Ed.	ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408.
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	4th WD	This International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4.
ISO/IEC 18045	Methodology for IT security evaluation	2nd Ed.	ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 18367	Cryptographic algorithms and security mechanisms conformance testing	2nd WD	The purpose of this standard is to address conformance testing methods of cryptographic algorithms and security mechanisms implemented in a cryptographic module.
ISO/IEC 19790	Security requirements for cryptographic modules	2nd Ed	ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems
ISO/IEC TR 19791	Security assessment of operational systems	Under review	ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems.
ISO/IEC 19792	Security evaluation of biometrics	1st Ed	ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system.
ISO/IEC TR 20004	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	1st WD Under review	ISO/IEC TR 20004:2012 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.
ISO/IEC 21827	Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)	2nd Ed	ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 24759	Test requirements for cryptographic modules	DIS Under review	ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006.
ISO/IEC 29128	Verification of cryptographic protocols	1st Ed	ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols.
ISO/IEC 29147	Vulnerability Disclosure	DIS	This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services.
ISO/IEC TR 30104	Physical security attacks, mitigation techniques and security requirements	PDTS	This Technical Report addresses how security assurance can be stated for products where the risk of the security environment requires the support of physical protection mechanisms.
ISO/IEC 30111	Vulnerability handling processes	DIS In publication	This International Standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services.
ISO/IEC 30127	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis	WD	This Technical Report provides guidelines for the planning, development and execution of penetration testing under ISO/IEC 15408 and ISO/IEC 18045 Vulnerability Assessment for software targets of evaluation.

WG3 Standards

Study Periods	New Work Items
Standards for Privacy Seal Programs	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications
Security evaluation of anti spoofing techniques for biometrics	
Predictive Assurance	
High Assurance	