ISO/IEC JTC 1 N9327

2008-10-14

Replaces:

ISO/IEC JTC 1
Information Technology

Document Type:	other (defined)
Document Title:	SC 27 Business Plan October 2008 – September 2009
Document Source:	SC 27 Secretariat
Document Status:	This document is circulated to National Bodies for review and consideration at the November 2008 JTC 1 Plenary meeting in Nara.
Action ID:	ACT
Due Date:	
No. of Pages:	13

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1/SC 27 N7311

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Business Plan

TITLE: SC 27 Business Plan October 2008 – September 2009

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2008-10-09

PROJECT:

STATUS: for submission to JTC 1

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
T. Humphreys, M.-C. Kang, K. Naemura, M. Ohlin, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 10

Secretariat ISO/IEC JTC 1/SC 27 - DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; e-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

Business Plan for JTC 1/SC 27 'Security Techniques'

Period covered: October 2008 - September 2009

Submitted by: Walter Fumy, SC 27 Chairman

1 Management Summary

1.1 Chairman's Remarks

Over the past years SC 27 has expanded and refocused its area of work, taking up new areas such as security of biometrics, identity management, and privacy. Consequently, the statement of scope for SC 27 needed to be adjusted and at its 19th Plenary meeting held May 2007 in St. Petersburg, SC 27 had approved a revised scope. However, the revised statement of scope for SC 27 was not endorsed by the October 2007 JTC 1 Plenary.

SC 27 has now approved the revised statement of scope contained in section 1.2 of this business plan, taking into account JTC 1's comments, and seeks endorsement by the November 2008 JTC 1 Plenary.

1.2 JTC 1/SC 27 Statement of Scope*

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

**) pending JTC 1 endorsement, see section 1.1.*

1.3 Project Report

1.3.1 Progress

The overall progress made over the past year was excellent as shown by the number of documents that have been published (see also section 2.2) and also by the target dates being kept in the majority of cases.

- total number of projects 90
- number of active projects 64
- number of publications: 75

SC 27 fully supports all its active projects. Details of the current status of all projects and their target dates can be found in SC 27 Standing Document SD 4, see also http://www.jtc1sc27.din.de/en .

1.3.2 New Projects and Study Periods

The following New Work Items for SC 27 have been approved over the past 12 months, all supported by substantial NB interest:

- NP 29128: *Verification of cryptographic protocols*.

  This standard will provide a technical base for the assessment of the security of cryptographic protocols. It will describe design evaluation criteria for these protocols, as well as methods to be applied in a verification process for such protocols.

- NP 29146: *A framework for access management*.

  This standard will provide a framework for the definition of access management and the secure management of the process of accessing information. This framework will be applicable to individuals as well as organizations of all types and sizes, and should be useful to organizations regardless of location or the nature of the activities they are involved in.

- NP 29147: *Responsible vulnerability disclosure*.

  This standard will provide a methodology for the disclosure and management of vulnerability alerts to be used by all interested parties. Those parties include the discoverer, vendor, and vulnerability information services. The standard will include methods to determine risk, format for disclosing vulnerability information, and methods for organizations to gather and process the disclosed information.

- NP 29149: *Best practice on the provision of time-stamping services*.

  This Technical Report will discuss additional considerations to be taken into account to provide the highest levels of trust to the users of time-stamping services.

- NP 29150: *Signcryption*.

  This standard will specify mechanisms for processing data with the combined objectives of data confidentiality, data integrity, data origin authentication, and data unforgeability. The mechanisms employ public key cryptographic techniques, and require both the originator and the recipient of the protected data to have their own public and private key pairs.

- NP 27010: *Information security management: Inter-sector communications.*

  This standard is to provide guidance for information security interworking and communications between industries in the same sectors, in different industry sectors and with governments, either in times of crisis and to protect critical infrastructure or for mutual recognition under normal business circumstances to meet legal, regulatory and contractual obligations.

- NP 27012: *Information security management guidelines for e-government services*.

  This standard will provide guidance to the Public Administration on how to adapt 27002 controls and processes to its specific tasks and legally bounding procedures, i.e. guidelines on how to meet baseline information security management requirements and implement appropriate controls and processes to meet confidentiality, integrity, availability and any other relevant security properties.

- NP 27009: *Guidance for auditors on ISMS controls*.

  This standard will provide guidance to audits on the implementation of ISMS controls. This importance of this guideline is aimed at helping auditors with advice to provide a better understanding of these controls from an auditing perspective.

- NP 27035: *Information security incident management*.

  This standard will provide guidance on information security incident management for information security managers, and information system, service and network managers.

Furthermore, in the period covered by this business plan SC 27 has resolved to initiate the following New Work Items ballots:

- *Information security management guidelines for financial and insurance services.*
- *Information security governance framework.*
- *Guidance for the integrated implementation of 20000-1 with 27001 (collaborative with SC7).*

- *Guidelines for security of outsourcing.*
- *Guidelines for identification, collection, and/or acquisition and preservation of digital evidence.*
- *Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures.*
- *Privacy Capability Maturity Model.*
- *Secure System Engineering Principles and Techniques.*
- *Lightweight cryptography*

In addition, SC 27 has established Study Periods on the following topics:

- *Object identifiers and ASN.1 syntax.*
- *Sector-specific ISMS standards for the World Lottery Association.*
- *Information security for Critical Infrastructure – Sector-specific guidance.*
- *Information security governance.*
- *Technical ISM audits.*
- *Secret sharing mechanisms.*
- *Security of outsourcing.*
- *Categorization and classification of information security incident.*
- *Evidence acquisition procedure for digital forensics.*
- *Tamperproof Protection Requirements and Evaluation.*

1.3 Co-operation and Competition

SC 27 enjoys a large number of very fruitful and valuable liaisons with many organizations within ISO/IEC JTC 1 including SC 6, SC 7, SC 17, SC 36, and SC 37, within ISO including TC 68, TC 215, ISO/CASCO and to several external organizations including CCDB, ETSI, CEN/NISSG, ITU-T, FIRST and ISSEA. Selected aspects related to theses liaisons are highlighted below.

1.3.1 SC 37 'Biometrics'

Strong synergy exists between biometrics and IT security. The potential contribution of SC 27 to biometrics standards is evident. In particular, the areas of template protection techniques, algorithm security, and security evaluation are fields where SC 27 has the necessary experience to complement the mandate of SC 37. Therefore, SC 27 has established close collaboration with SC 37 'Biometrics'.

1.3.2 TC 68 'Financial Services'

TC 68 and SC 27 collaborate on IT security standards of mutual interest. To encourage such cooperation, to share expertise and content, and to avoid overlap in standards development and manage New Work Item proposals that are relevant to both committees, a joint *'Coordination Committee on Security Work'* has been established. The latest meeting of this committee took place September 11, 2008 in Berlin where a number of cooperation topics have been agreed.

1.3.3 ITU-T Q10/SG17

ITU-T Q10/SG17 and SC 27/WG 1 collaborate on several projects in order to progress common or twin text documents and to publish common standards. These projects include

- ISO/IEC 15816: *Security information objects for access control* (= ITU-T X.841)
- ISO/IEC 14516: *Guidelines on the use and management of Trusted Third Party services* (= ITU-T X.842)
- ISO/IEC 15945: *Specification of TTP services to support the application of digital signatures* (= ITU-T X.843)
- ISO/IEC 18028: *IT network security**
- ISO/IEC 27001: *ISMS requirements*
- ISO/IEC 27002: *Code of practice for information security management*
- ISO/IEC 27011: *Information security management guidelines for telecommunications* (= ITU-T X.1051)
- ISO/IEC 29115: *Entity Authentication Assurance* (= ITU-T x.eea)

*) This work is also done in collaboration with JTC 1/SC 6.

1.3.4 The International Common Criteria Project (ICCP)

The ICCP and SC 27/WG 3 have had a long-standing technical liaison on projects related to IT Security Evaluation Criteria. Thus, Working Group 3 has been working in close co-operation with the Common Criteria Development Board (CCDB) on the development of the Common Criteria, which has been simultaneously published as ISO/IEC 15408. The co-operation has been extended to also involve the work on 18045 “Evaluation methodology for IT security”. This close cooperation allows NBs not represented in the ICCP to review, comment and contribute to the project. An update of 15408, to bring it in line with the recently updated version 3.1 within the ICCP, is now close to completion. The related standard on Evaluation Methodology, 18045, has already been aligned. Recently the WG has been contributing to the ICCP exploratory work on future development of Common Criteria.

2 Period Review

2.1 Market Requirements

Up until the 1970s, the use of security techniques to protect information and communications was largely restricted to some specific areas of application - such as banking - and to governments. With the advent of the Internet and the prospect of performing business on-line, IT security has been in the forefront of information and communications technology (ICT) have emerged high on the management agenda, have been the subject of new legislation and has made its way into many news headlines. E.g., organizations deploying electronic services (e.g., e-business, e-government) need to ensure control over who gets into applications and what users are allowed once they are in. User identification, authentication and authorization management technologies address these issues. Electronic signatures provide data integrity and non-repudiation and thus help to accelerate the growth in secure electronic business and subsequently to eliminate paper-based transactions.

At the same time, users need confidence in the effectiveness of the implemented security; an area where security evaluation and resulting assurance play an important part – here we have the Common Criteria (ISO/IEC 15408) for the security evaluation of products and systems and ISO/IEC 27001 for the third party certification of an organization’s information

security management system (ISMS) – similar to the model for ISO 9001 (Quality), ISO 14001 (Environment) and ISO 22000 (Food safety management).

In addition, users ask more and more about protection of their privacy and the related data. The relation between IT security and privacy is close, complex, and delicate. This can especially be seen in the area of Identity Management, e.g. pointing to the issue, who owns which very personal data about whom. SC 27 addresses this issue in its new Working Group 5 “Identity Management and Privacy Technologies”, e.g. by ISO/IEC 24760 “A Framework for Identity Management” and ISO/IEC 29100 “Privacy Framework”.

Standardized security techniques are becoming mandatory requirements for e-commerce, health-care, telecoms, automotive and many other application areas in both the commercial and government sectors. SC 27 addresses those market needs and provides a center of expertise for the standardization of security techniques.

The near future sees many market opportunities for SC 27 to expand the deployment of its standards as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security and IT security has always been at the forefront of security standardization. It has the right blend of skills and resources to deliver security standards to market requirements as borne out by its past track record. As applications of security technologies have broadened during the last years, so have both the membership of SC 27 and its programme of work.

A rapidly emerging and critical area of standardization to address corporate needs around the world is that of governance whether in the form of IT governance or information security governance (ISG). SC 27 is embarking on a programme of work into ISG in collaboration with other groups in JTC 1 dealing with other governance issues such as IT governance. Protecting corporate information assets cannot be solved by IT security solutions and technologies alone. Hence resolving strategic issues concerning the protection of corporate information assets and to support the organization’s corporate governance relies on effective information security governance.

The scope of information security governance is to:

- Help meet corporate governance requirements related to information security
- Align information security objectives with business objectives
- Ensure a risk-based approach is adopted for information security management
- Implement effective management controls for information security management
- Evaluate, direct, and monitor an information security management system
- Safeguard information of all types, including electronic, paper, and spoken
- Ensure good conduct of people in using information

2.2 Achievements

2.2.1 Publications

Since October 2007, the following International Standards and Technical Reports have been published:

- ISO/IEC 11770-2: *Key management – Part 2: Mechanisms using symmetric techniques (2nd edition)*.

  Publication date: 2008-06-15

  ISO/IEC 11770-2 defines key establishment mechanisms using symmetric cryptographic techniques. It addresses three environments for the establishment of keys: Point-to-Point,

Key Distribution Centre (KDC), and Key Translation Centre (KTC). It describes the required content of messages which carry keying material or are necessary to set up the conditions under which the keying material can be established.

- ISO/IEC 11770-3: *Key management – Part 3: Mechanisms using asymmetric techniques (2nd edition).*

  Publication date: 2008-07-15

  ISO/IEC 11770-3 defines key management mechanisms based on asymmetric cryptographic techniques to establish a shared secret key for a symmetric cryptographic technique between two entities by key agreement or by key transport, or to make an entity's public key available to other entities by key transport.

- ISO/IEC 14888-1: *Digital signatures with appendix - Part 1: General (2nd edition)*.

  Publication date: 2008-04-15

  ISO/IEC 14888-1 provides general principles and requirements for digital signatures with appendix. It also gives definitions and symbols which are used in all parts of ISO/IEC 14888.

- ISO/IEC 14888-2: *Digital signatures with appendix - Part 2: Integer factorization based mechanisms (2nd edition).*

  Publication date: 2008-04-15

  ISO/IEC 14888-2 specifies digital signatures with appendix whose security is based on the difficulty of factoring the modulus in use. For each signature scheme, it specifies the relationships and constraints between all the data elements required for signing and verifying, a signature mechanism, and a verification mechanism.

- ISO/IEC 15408-2: *Evaluation criteria for IT Security – Part 2: Security functional components (3rd edition).*

  Publication date: 2008-08-15

  ISO/IEC 15408-2 contains a catalogue of functional requirement building blocks from which the security functionality of products and systems can be expressed. It also contains a paradigm for expressing and categorizing security functionality.

- ISO/IEC 15408-3: *Evaluation criteria for IT Security – Part 3: Security assurance components (3rd edition).*

  Publication date: 2008-08-15

  ISO/IEC 15408-3 contains a catalogue of assurance building blocks that can be applied to provide confidence in the security of products and systems. The standard also provides seven, hierarchical predefined packages of assurance requirements, named Evaluation Assurance Levels.

- ISO/IEC 15946-1: *Cryptographic techniques based on elliptic curves – Part 1: General (2nd edition).*

  Publication date: 2008-04-15

  ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. Part 1 of this standard describes the mathematical background and general techniques necessary for implementing any of the mechanisms defined in other parts of ISO/IEC 15946.

- ISO/IEC 18014-1: Time-stamping services -- Part 1: Framework

  Publication date: 2008-09-01

Part 1 of ISO/IEC 18014 serves as the introductory part for time-stamping. In this it identifies the objective of a time-stamping authority, describes a general model on which time-stamping services are based, defines time-stamping services and the basic protocols of time-stamping, specifies the basic protocols between the involved entities and describes linking protocols for a time-stamping authority.

- ISO/IEC 18045: *Methodology for IT security evaluation (2nd edition).*

  Publication date: 2008-08-15

  ISO/IEC 18045 provides detailed techniques to be applied when assessing products and systems against IS 15408. The application of this standard is important to support mutual recognition of evaluation results.

- ISO/IEC 24759: *Test requirements for cryptographic modules.*

  Publication date: 2008-07-01

  ISO/IEC 24759 describes the methods that will be used by laboratories to test whether a cryptographic module conforms to ISO/IEC 19790. It includes detailed procedures, inspections, and tests that the tester must follow, and the expected results that must be achieved for the cryptographic module to satisfy the requirements of ISO/IEC 19790.

- ISO/IEC 24762: *Guidelines for information and communications technology disaster recovery services*.

  Publication date: 2008-02-01

  This standard specifies guidelines for disaster recovery services focusing on the desired disaster recovery facilities and services capability. ISO/IEC 24762 deals with the provision of fallback and recovery support to an organization's information and communication system, including test, implementation and execution aspects of disaster recovery.

- ISO/IEC 27005: *Information security risk management*.

  Publication date: 2008-06-15

  ISO/IEC 27005 provides guidelines for information security risk management. The 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.

- ISO/IEC TR 15443-3: *A framework for IT security assurance – Part 3: Analysis of assurance methods*.

  Publication date: 2007-12-15

  Part 3 of TR 15443 analyses the various assurance methods with respect to their assurance properties. This analysis is to aid assurance authorities in assessing the relative value of each assurance approach and determining the assurance approach(s) that will provide the assurance results most appropriate to their needs - all within the specific context of their operating environment.

2.2.2 Documents awaiting Publication

The following International Standards and Technical Reports developed by SC 27 have been finalized and are awaiting publication:

- ISO/IEC 21827: *Systems Security Engineering - Capability Maturity Model (SSE-CMM) (2nd edition).*
- ISO/IEC 27011 (= ITU-T X.1051): *Information security management guidelines for telecommunications organizations*.

2.3 Resources

The last SC 27 Plenary meeting took place April 21-22, 2008 in Kyoto, Japan and was attended by 65 delegates from 25 of the current 39 P-members.

The five SC 27 Working Groups held meetings October 6-10, 2008 in Limassol, Cyprus, and April 14–18, 2008 in Kyoto, Japan. In average, these WG meetings were attended by about 200 delegates in total.

The next Working Group meetings are scheduled for May 4–8, 2009 in Beijing, China and for November 2-6 in Redmond, USA. The next SC 27 Plenary meeting is planned to take place May 11–12, 2009 in Beijing, China.

Overall, the resources and expertise prove to be sufficient to meet the many challenges, SC 27 is facing. In particular, the two newly established Working Groups have attracted additional experts from all regions worldwide. With the new multi-part project ISO/IEC 11889 on Trusted Platform Modules (JTC 1 PAS process) SC 27 is further expanding its range of expertise into security engineering.

3 Focus Next Work Period

3.1 Deliverables

Deliverables expected from the next work period (October 2008 - September 2009) include

- ISO/IEC 9797-1: *Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher (2nd edition)*.
- ISO/IEC 9798-2: *Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithm (3rd edition)*.
- ISO/IEC 11889-1: *Trusted Platform Module - Part 1: Overview (Publicly available Specification).*
- ISO/IEC 11889-2: *Trusted Platform Module - Part 2: Design principles (Publicly available Specification).*
- ISO/IEC 11889-3: *Trusted Platform Module - Part 3: Structures (Publicly available Specification).*
- ISO/IEC 11889-4: *Trusted Platform Module - Part 4: Commands (Publicly available Specification).*
- ISO/IEC 13888-1: *Non-repudiation - Part 1: General (2nd edition)*.
- ISO/IEC 15408-1: *Evaluation criteria for IT Security – Part 1: Introduction and general model (3rd edition).*
- ISO/IEC 15446: Guide for the production of Protection Profiles and Security Targets (2nd edition).
- ISO/IEC 19772: *Authenticated encryption.*
- ISO/IEC 19792: *Security evaluation of biometrics*.
- ISO/IEC 24761: *Authentication context for biometrics.*

3.2 Strategies

SC 27's Area of Work is the standardization of generic methods and techniques for IT security. Among its 'users' are other standardization groups that adopt these where

appropriate, in whole or in part, and provide a selection of required options. An important means to ensure the timely development of market-oriented methods and techniques for IT security is the cooperation with such users, such as SC 7, SC 37 and TC 68.

3.2.1 Risks

The time to develop market driven standards is not always consistent with the market needs and timeframe for these standards. Ways and means to continually improve the timely development and delivery of standards are reviewed on a regular basis.

3.2.2 Opportunities

Standardized security techniques are becoming mandatory requirements for e-commerce, health-care, and many other application areas. The use of security techniques and in particular of electronic signatures constitutes a core element in e-business, e-government and other on-line activities. Over the last years, SC 27's work programme has included the basic techniques required for these activities. The existing portfolio of SC 27 work items and standards can be used to define a security framework, e.g., for governance, e-government, the telecom sector, healthcare sector or for the financial/insurance sector.

3.2.3 Marketing Initiatives and Joint Standardization Events

SC 27 has established the position of a PR officer and produces and distributes a number of press releases each year. These aim at promoting the standards that SC 27 develops and publishes. The press releases are targeted at users, implementers and management in industry and commerce. The distribution channels include international user groups and associations interested in security standards, security journals, publications and news letters, the SC 27 Web site as well standards development bodies (within ISO/IEC, ITU-T, CEN, ETSI and other bodies such as IETF and IEEE).

In the past year again many conference and workshop presentations focused on SC 27 activities, including

- RSA conference Japan, Tokyo, April 2008
- International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy, August 2008
- Industry Seminar, Cyprus, October 2008.

In addition, several articles have been published, four alone in ISO Focus (volume 4, no. 5 May 2007) bringing to the public attention achievements of successful standardization work in the area of Information Security Management Systems (ISMS) as well as new approaches being underway within the newly established Working Group 4 "Security Controls" and WG 5 "Identity Management and Privacy Technologies". Seven other articles have been published in ISO Management Systems, including an article jointly written with SC7/WG25 on the integration of the ISO/IEC 27001 information security management system requirements and ISO/IEC 20000-1 service management standards.

Both WG 4 and WG 5 have on their agenda projects to be developed in close cooperation with their liaison organizations especially with ITU-T SG17 and ITU-T D but also with such liaison members as Liberty Alliance, FIDIS, OASIS, The Open Group, ETSI/TISPAN, W3C.

SD11 provides a very accessible overview of the work of SC27. This includes a number of the SC27 articles that have been published by ISO in the publications ISO Focus, ISO Journal and ISO Management System. SD11 is freely available to everyone and is downloadable via the SC27 Web Site (http://www.jtc1sc27.din.de/sce/sd11).

The following international workshops have taken place:

- Joint ITU-T SG17/Q.6 & SC 27/WG 4 Workshop on Cybersecurity Standards in Geneva on 26th October 2007. Further details can be found at http://www.jtc1sc27.din.de/sue/ws_cybersec.
- Joint ITU-T SG17/Q.6 /SC 27/WG 5 / FIDIS Workshop on Identity Management Standards in Lucerne on 30th September 2007. More details can be obtained from the workshop's web site at http://www.jtc1sc27.din.de/sue/ws_idm.

Tutorial and press material on SC 27, its projects, and its standardization roadmaps is available from http://www.jtc1sc27.din.de/

3.3 Work Programme Priorities

Priority tasks for Working Group 1 include to ensure that work on projects 27004: *Information security measurements* and 27003) *Information security management system risk management* are completed as planned, and keeping the WG1 Roadmap up-to-date. In addition, WG 1's role in the cooperation with ITU-T is of strategic importance in particular on the topics of Network Security, information security governance, risk management profiles and the ISO 27000 ISMS standards.

For Working Group 2, priorities for the next work period include the successful completion of the WG 2 projects mentioned in section 3.1. In addition, WG 2's roles in the cooperation with TC 68 *Banking and Related Financial Services* are of strategic importance.

Priority for Working Group 3 is to ensure that work on projects 19792 *Security Evaluation of Biometrics* and Part 1 of 15408 *Information Technology Security Evaluation Criteria* is completed as planned. WG 3's cooperation with the Common Criteria Development Board (CCDB) remains important. Related to this work is the nearly completed update of ISO/IEC TR 15446 *Guide for the production of Protection Profiles and Security Targets*. The co-operation with SC 37 (Biometrics) is currently focusing on project 19792 *Security evaluation of biometrics* addressing the basis for trust in the security of applied biometrics. A new area for WG 3 is its project 29147 on *Responsible Vulnerability Disclosure* which attempts to provide a standard governing the relationship between researchers and vendors in the context of dissemination of security vulnerability information related to IT products. This project has attracted new experts to the WG.

Priorities for Working Group 4 are to consolidate progress on the transfer of projects from WG1 on supporting ISMS services and mechanisms. For example, the maintenance and updating of the multipart standard on *Network Security* (project 1.27.28), and the *TTP services* standards as well as the successful completion of the *Disaster recovery services* standard. In addition, WG 4 has initiated work on new projects such as cybersecurity, application security, ICT readiness for business continuity, security of outsourcing, and guidance for the identification, collection and/or acquisition, and preservation of digital evidence..

Priorities for Working Group 5 are to develop foundational frameworks and architectures for identity management and privacy (projects 24760 *A framework for identity management*, 29100 *Privacy framework, and 29101 Privacy Architecture*) and to consolidate progress on biometrics projects transferred from Working Group 2 (project 24761 *Biometric authentication contex*t and 24745 *Biometric template protection*), that are also requested by SC 37. At the same time Working Group 5 is developing a standards development roadmap, that is being used to identify, promote, and prioritize future work on supporting technologies, models, and methodologies