Document type: Business Plan
Title: SC 27 Business Plan and Dashboard, IT Security techniques for the PERIOD OVERED: October 2016 – September 2017
Status: This document is circulated for review and consideration at the November 2016 JTC 1 meeting in Norway.
Date of document: 2016-10-17
Source: SC 27 Secretariat
Expected action: ACT
Action due date: 2016-11-07
Email of secretary: lrajchel@ansi.org
Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1
ISO/IEC JTC 1/SC 27

Information technology — Security techniques

Secretariat: DIN, Germany

DOC TYPE: Business Plan


SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2016-10-12

PROJECT: 

STATUS: for submission to JTC 1

ACTION ID: FY1

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
H. Cuschieri, B. Garcia, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice — Chair
T. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG — Convenors
A. Fuchsberger, F. Kahn, SWG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 14
Business Plan for JTC 1/SC 27 ‘IT Security Techniques’

Period covered: October 2016 – September 2017
Submitted by: Walter Fumy, SC 27 Chairman

1 Management Summary

1.1 Chairman’s Remarks
This Business Plan has been prepared in accordance with Resolution 51 of the 28th SC 27 Plenary meeting in Tampa, FL, USA, 18th – 19th April 2016.

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, security processes, and 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 management systems;
- 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.
1.3 Project Report

1.3.1 Progress

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

- total number of projects: 230
- number of active projects: 70
- number of publications: 160

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, available at http://www.din.de/en/meta/jtc1sc27.

1.3.2 New Projects and Study Periods

The following new projects have been approved over the past 12 months either via a 3-month NP ballot, 60-day letter ballot, or by subdivision of existing projects. All of the new projects are supported by substantial NB interest:

- ISO/IEC NP 20547-4, Information technology – Big data reference architecture – Part 4: Security and privacy fabric (re-allocated from JTC 1/WG 9 to SC 27/WG 4 in close cooperation with WG 5);
- ISO/IEC NP 21878, Security guidelines for design and implementation of virtualized servers;
- ISO/IEC NP 27550, Privacy Engineering;
- ISO/IEC NP 27552, Enhancement to ISO/IEC 27001 for privacy management — Requirements;
- ISO/IEC NP 19989, Criteria and methodology for security evaluation of biometric systems — Part 1: Performance
  - Part 2: Presentation attack detection;
- ISO/IEC NP 14888-3: 2015/Amd.1, Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms – Amendment 1;
- ISO/IEC NP 18033-2: 2006/Amd.1, Encryption algorithms — Part 2: Asymmetric ciphers – Amendment 1;
- ISO/IEC NP 29115: 2013/Amd.1, Entity authentication assurance framework — Amendment 1;
- ISO/IEC NP 29192-6, Lightweight cryptography – Part 6: Message authentication codes (MACs).

In addition, SC 27 has resolved to revise the following projects:

- ISO/IEC 9798-5:2009, Entity authentication – Part 5: Mechanisms using zero knowledge techniques (revision of 3rd edition);
- ISO/IEC 18032:2005, Prime number generation (revision of 3rd edition);
- ISO/IEC 27002:2013, Code of practice for information security controls (revision of 2nd edition);

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

- Design Specification for the Revision of ISO/IEC 27002 (WG 1);
- Design Specification for the Revision of ISO/IEC 27005 (WG 1);
- Design Specification for the Revision of ISO/IEC 27014 (WG 1);
- Design Specification for the Guidelines on Cyber Insurance (WG 1);
- Design Specification for the Guidelines on Cyber Resilience (WG 1);
- Revision of ISO/IEC 11770-1 (WG 2);
- Revision of ISO/IEC 11770-2 (WG 2);
- Broadcast authentication protocols (WG 2);
- Revision of ISO/IEC 20009-2 and ISO/IEC 20008-2 (WG 2);
- Inclusion of the block cipher Kuznyechik in ISO/IEC 18033-3 (WG 2);
- Architecture of trusted connection to cloud services (WG 4);
- Application security validation (WG 4);
- Emerging virtualization security (WG 4);
- Guidelines for incident response operations (WG 4);
- Guidelines for Security in Internet of Things (IoT) (WG 4);
- ICT readiness for electronic discovery (WG 4);
- Virtualized roots of trust (WG 4);
- Guidelines for Privacy in Internet of Things (IoT) (WG 5);
- Editorial inconsistencies in ISO/IEC 29100, *Privacy framework* (WG 5);
- Entity authentication assurance framework (WG 5);
- Privacy in smart cities (WG 5).

### 1.4 Co-operation and Competition

SC 27 benefits from collaboration with an extremely large number of productive and valuable liaisons with many organizations

- within ISO/IEC JTC 1 including WG 7, WG 9, WG 10, WG11, SC 6, SC 7, SC 17, SC 22, SC 25, SC 31, SC 36, SC 37, SC 38 and SC 40;
- within ISO including TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, TC 272, TC 292, ISO/PC 302, ISO/CASCO, TMB/TCG MSS, TMB/SAG;
- within IEC including IEC/ACSEC, IEC/SC 45A, IEC/TG 57, IEC/TG 65; and
Currently SC 27 maintains 45 internal and 46 external liaisons. A complete list is available at www.din.de/meta/jtc1sc27/Members.

Selected aspects related to these liaisons are highlighted below.

1.4.1 SC 37 ‘Biometrics’

There is a close and advantageous synergy exists between biometrics and IT security. The potential contribution of SC 27 to biometrics standards is evident. Particularly, in 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 maintains close collaboration with SC 37 ‘Biometrics.’

1.4.2 TC 68/SC 2 ‘Financial Services — Security’

TC 68/SC 2 and SC 27 coordinate on IT security standards of mutual interest by sharing expertise and content, in order to avoid potential overlap in IT security standards development. In that respect, SC 27 contributed to the TC 68/SC 2 overview document on Financial Services Security Framework and regularly provides liaison statements on specific topics such as ISMS (information security management system) standards and cryptographic algorithms.

1.4.3 ITU-T Q3/SG17 and ITU-T FG Cloud Computing

ITU-T Q3/SG17 and SC 27 collaborate on several projects to progress common or twin text documents and to publish common standards. These projects include

- Draft Recommendation ITU-T X.1085 (bhsm) | ISO/IEC DIS/FDIS* 17922, Telebiometric authentication framework using biometric hardware security module;

* Subject to approval by ITU-T SG 17

1.4.4 The Common Criteria Development Board (CCDB)

The CCDB 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 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 CCDB to
review, comment and contribute to the project. Both the ISO/IEC 15408 and ISO/IEC 18045 are currently fully aligned with their CCDB counterparts. Recently the WG has been contributing to the CCDB exploratory work on future development of Common Criteria.

A number of SC 27/WG 3 projects complement the application of ISO/IEC 15408, such as ISO/IEC TR 20004, Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045, or ISO/IEC 17825, Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. This extended coverage increases the collaboration with the CCDB.

1.4.5 ISO/TC 292 Security and resilience

ISO TC 292 was created as the result of an initiative to restructure the security sector within ISO. Its broad scope covers Standardization in the field of security to enhance the safety and resilience of society. To avoid potential overlap and to ensure maximum effectiveness, SC 27 has established close cooperation with TC 292.

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 the financial and telecoms industry and governments. With the advancement of technology and advent of the Internet and the prospect of performing business on — line, information and IT security has been at the forefront of information and communications technology (ICT). As technological advancement continued across the board with greater connectivity and use of mobile devices security and privacy have emerged high on the management agenda, have been the subject of new legislation and the issues of security and privacy have made their way into many news headlines. For example, organizations deploying (remote) electronic services (e.g., e — business, e — government) need to ensure control over who has access to information and applications and what users are allowed to do once they have access. 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. Advancements in smart and mobile technology, social networking and greater use of personal technology (BYOD versus CYOD) have increased the concerns over security and privacy. Therefore the expertise and resources SC 27 has had to address many of these issues and challenges, in conjunction with other players in the business, technology and government space, in its delivery of world — class standards. The SC 27 outreach continues to grow as new security and privacy issues continue to grow. The following are some of the themes it has needed to address.

Assurance, Confidence and Management of Information and IT Security and Privacy

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 IT products and systems. In addition, user have the need for management of risk across the organisation, in this case SC7s best — selling management standard ISO/IEC 27001 (Information security management system (ISMS) requirements) satisfies this requirement and also provides for the third party accredited certification of an organization’s ISMS. ISO/IEC 27001 is of course part of the bigger family of management system standards — ISO 9001 (Quality management), ISO 14001 (Environment management), ISO 22000 (Food safety management), ISO 50001 (Energy management) and ISO 22301 (Business continuity management).
Governance of Information Security and Cyberspace Protection

A rapidly emerging and critical area of standardization to address corporate needs around the world is that of corporate governance whether in the form of information security governance (ISG), operation governance or IT governance. SC 27 has already developed one standard in this area ISO/IEC 27014 Governance of information security which define a framework, establish objectives, principles, and processes, and show how it can be used to evaluate, direct, and monitor the governance of information security within an ISMS environment. Protecting corporate information assets from cyber risks cannot be solved by IT security solutions and technologies alone, standards such as ISO/IEC 27001, ISO/IEC 27014 and the emerging cyber resilience and insurance standards are crucial. 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.

Privacy

Users ask more and more about protection of the privacy of their information and data. There is a close relationship between information and IT security and privacy. The issues being addressed are sometimes complex, and sensitive. This can especially be seen in the area of Identity Management, e.g. relating to the issue, who controls and is entitled to use which very personal data about whom. SC 27 addresses the technological challenges resulting from this issue in its 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”.

Sector Specifics

Standardized security techniques are becoming mandatory requirements across most sectors for e — and m — commerce, health — care, telecoms, energy sector, automotive and many other application areas in both the commercial and government sectors. SC 27 is a centre of expertise for the standardization of security techniques for addressing the security and privacy requirements and market needs across many market sectors.

The short term future sees many market opportunities for SC 27 to expand the deployment of its standards and its expertise as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security, privacy, and IT security has been at the forefront of the related standardization for more than twenty — five years. It has the right mix of skills and resources to deliver security standards to market requirements as demonstrated 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.

Cyber Incident Preparedness, Response, Recovery and Investigation

Apart from the need for guidelines and standards enabling or contributing to the implementation and assurance of security, SC 27 has addressed the need for guidelines and standards addressing cyber incident management, specific activities in handling potential digital evidence, and common investigation processes across various investigation scenarios.

Advanced and Evolving Technologies

Standards for Cloud security and privacy have been an important part of SC27’s recent activities. Furthermore, emerging technologies such as the “Internet of things” and “Big Data” are gaining more and more attention. SC 27 has started looking into the security and privacy aspects of these emerging technologies with a view of standardization. In addition, technologies such as RFID pose new challenges with respect to security and privacy, and in view of specific constraints, require dedicated solutions, such as lightweight cryptographic techniques, authentication.
More and more, organizations are recognizing the importance of addressing security and privacy within their systems and process, software engineering processes, as well as within the supply chain operations.

2.2 Achievements

2.2.1 Publications
Since October 2015, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:


In addition, a number of Technical Corrigenda have been published over the past 12 months.

2.2.2 Documents awaiting Publication
The following International Standards or Technical Reports developed by SC 27 have been finalized and are awaiting publication:
• ISO/IEC 18031:2011/Amd.1 (4th Q 2016), Random bit generation — Amendment 1;
• ISO/IEC 18367 (1st edition) (4th Q 2016), Cryptographic algorithms and security mechanisms conformance testing;
• ITU-T X.1051 | ISO/IEC 27011 (2nd edition) (4th Q 2016 or 1st Q 2017), Information security control guidelines based on ISO/IEC 27002 for telecommunications organizations;

2.3 Resource
The last SC 27 Plenary meeting took place April 18 - 19 2016 in Tampa, FL, USA and was attended by 80 delegates from 31 of the current 53 P-members.

The five SC 27 Working Groups held meetings April 11 - 15, 2016 in Tampa, FL, USA and October 2016 in Jaipur, India. In both the Tampa and Jaipur meetings around 280 delegates attended spread across the five SC 27 Working Groups.

The next set of Working Group meetings are scheduled for October 23 - 27, 2016 in Abu Dhabi, United Arab Emirates. The next SC 27 Plenary will take place April 24 - 25, 2017 in Hamilton, New Zealand and will be preceded by meetings of the five SC 27 Working Groups, April 18 - 22, 2017 at the same location.

Overall, the resources and expertise prove to be sufficient to meet the many challenges SC 27 is facing. For selected projects, SC 27 resources are complemented by resources from appropriate SC 27 liaison organizations.

The current 6-month meeting cycle of SC 27 has shown to be an efficient use of resources for the development of standards. This 6-month cycle tradition allows holding meetings at about the same time every year and helps to minimize the delegates’ travel budgets.

In the style of management system type continual improvement regarding the efficiency and quality of work and deliverables within SC 27 and its WGs; achieving the right balance between WG autonomy and coordination at SC 27 level; and to make optimal use of the relevant ISO processes and tools available; SC 27 has two Special Working Groups, one on Management (SWG-M) and one on Transversal Items (SWG-T).

3 Focus Next Work Period

3.1 Deliverables
Deliverables expected from the next work period (October 2016 — September 2017) include
• ISO/IEC 10116 (4th edition), Modes of operation for an n-bit block cipher;
• ISO/IEC 10118-3 (1st edition), Hash-functions — Part 3: Dedicated hash-functions;
• ISO/IEC TR 15446 (3rd edition), Guide for production of Protection Profiles and Security Targets (PP/ST);
• ISO/IEC 15946-5 (2nd edition), Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation;
• ISO/IEC TS 19249 (1st edition), Catalogue of architectural and design principles for secure products, systems, and applications;
• ISO/IEC 19592-2 (1st edition), Secret sharing — Part 2: Fundamental mechanisms;
• ISO/IEC TS 19608 (1st edition), Guidance for developing security and privacy functional requirements based on ISO/IEC 15408;
• ISO/IEC 27003 (2nd edition), Information security management system implementation — Guidance;
• ISO/IEC 27004 (2nd edition), Information security management — Monitoring, measurement, analysis and evaluation;
• ISO/IEC 27007 (2nd edition), Guidelines for information security management systems auditing;
• ISO/IEC TS 27008 (2nd edition), Guidelines for the assessment of information security controls;
• ISO/IEC 27019 (2nd edition), Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry;
• ISO/IEC 27021 (2nd edition), Competence requirements for information security management systems professionals;
• ISO/IEC 27034-7 (1st edition), Application security — Part 7: Application security assurance prediction model;
• ISO/IEC 29003 (1st edition), Identity proofing;

3.2 Strategies
SC 27’s core area of work is the standardization of generic methods and techniques for information and IT security and privacy. Among its ‘users’ are other standardization groups that adopt these where appropriate, in whole or in part, and provide detailed, sector-specific guidance for selected options. An important means to ensure the timely development of market-oriented standards, methods and techniques for information and IT security and privacy is the cooperation with such users, such as SC 7, SC 17, SC 25, SC 36, SC 37, SC 38, SC 40, JTC 1/WG 7, JTC 1/WG 10, TC 68/SC 2, TC 292, and ITU-T, and all the other organisations under clause 1.4 that SC cooperates with.

3.2.1 Challenges
The time needed to develop market driven standards is not always consistent with the market requirements and timeframe for these standards. Ways and means to continually improve the timely development and delivery of standards while guaranteeing the adequate quality and suitability are reviewed on a regular basis.

For some specific standards, such as cryptographic algorithms, cryptographic parameter generation, etc., internal SC 27 resources are not sufficient to conduct appropriate security evaluation and to ensure the desired technical quality. In these cases, SC 27 needs to ensure to establish the necessary cooperation with external initiatives in this area.

3.2.2 Opportunities
Standardized security techniques are becoming mandatory requirements for e- and m-commerce, e-government, telecoms, health-care, energy sector and many other application and service areas. The use of security techniques and in particular of identification, authentication and 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 information security governance, the telecom sector, healthcare sector or for the financial sector.

Growing awareness, concerns and opportunities with regard to privacy in society offer another area of opportunity for SC 27.

3.2.3 Marketing Initiatives and Joint Standardization Events

SC 27 has established the position of a Communications Officer, whose role is to promote the work of SC 27 through different channels: press releases and articles, conferences and workshops, interactive ISO chat forums and other media channels, as well as though Wikipedia pages. This effort is aimed at promoting the broad and detailed scope of standards that SC 27 develops and publishes. The growth in SC 27 outreach has benefited many users in the business and government community. The press releases are targeted at users, auditors, implementers and management in all sectors of industry and commerce, and for government users. A small selection of the recent ISO articles promoting the use of SC 27 work include:

- Security toolbox protects organizations from cyber-attacks (Dec 2015);
- Common terminology for information security management just revised (Feb 2016);
- Are we safe in the Internet of Things? (Sept 2016).

The distribution channels include international user groups and associations interested in security standards, security journals, ISO publications and newsletters, 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). SC 27 management and experts working contribute to papers, presentations and talks in many conferences, seminars and workshops at events around the world.

The SC 27 publication standing document SD11 provides a very accessible overview of the work of SC 27. SD11 is freely available to everyone and is downloadable via the SC 27 Web site http://www.din.de/meta/jtc1sc27.

On the occasion of its 20th birthday, the “SC 27 Platinum Book – Twenty Years of ISO/IEC JTC 1/SC 27 Information Security Standardization” has been produced. Included in this book are many articles written by experts working in SC 27 as well as by current and past officers of SC 27. The book further contains statements by SC 27 liaison organizations as well as by some National Bodies. An electronic version is available from the SC 27 Web Site. In Spring 2015 SC27 celebrated its 25th birthday with a further ‘birthday book’, which was launched at its Plenary and WG meetings in Kuching, Sarawak, Malaysia.

At most of its WG meetings SC 27 engages with local industry to hold knowledge transfer workshops. At the SC 27 meeting in Hong Kong (April 2014), SC 27 collaborated with the department of the Hong Kong responsible for IT Services to run a very successful workshop on SC 27 standards and the implementation of these standards by businesses in Hong Kong. Workshops were held at the last two WG meetings in Mexico City and Kuching, Sarawak, and a further workshop is planned for the next SC 27 meetings in Jaipur, India (October 2015).

Over the years officers of SC 27 have been invited to take part and give presentations at many seminars and conferences including the joint Chinese/US symposium on Cyber — Security in October 2011 and the Cyber Security conferences in Bangkok in March 2013 and July 2014, and in the Cyber Security Technology Summit in Wuhan, Hubei Province, China 19-20th Sept 2016. In September 2014 the Chair of SC 27 and the Convenor of WG 1 took part in the ITU-T SG17 workshop on security standardization for developing countries, also the Chair of SC 27 and the Convenor of WG 1 took part in the World Internet Conference Dec 2015 in Wuzhen, China.

Tutorial and press material on SC 27, its projects, and its standardization roadmaps are available from http://www.din.de/meta/jtc1sc27.
3.3 Work Programme Priorities

3.3.1 Working Group 1
Priority tasks for Working Group 1 include keeping the WG 1 Roadmap up-to-date, and to ensure effective and timely progression of:

Projects under revision:
- ISO/IEC 27002:2013, Code of practice for information security controls (revision of 2\textsuperscript{nd} ed.);
- ISO/IEC 27003:2010, Information security management system – guidance (revision of 1\textsuperscript{st} ed.);
- ISO/IEC 27004:2009, Information security management Monitoring, measurement, analysis and evaluation (revision of 1\textsuperscript{st} edition);
- ISO/IEC 27007:2011, Guidelines for information security management systems auditing (revision of 1\textsuperscript{st} ed.);
- ISO/IEC TR 27008:2011, Guidelines for auditors on ISMS controls (revision of 1\textsuperscript{st} edition);
- ITU-T X.1054 | ISO/IEC 27014:2013, Governance of information security;
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (revision of 1\textsuperscript{st} edition).

Projects under development:
- ISO/IEC 27021, Requirements for information security management professionals;
- Guidelines for cyber insurance;
- Guidelines for cyber resilience.

3.3.2 Working Group 2
Working Group 2 priorities for the next work period include the successful completion of the WG 2 projects mentioned in section 3.1, as well as the timely development of specifications for the recently established projects

- ISO/IEC 18032 (2nd edition), Prime number generation;
- ISO/IEC 29192-6 (1st edition), Lightweight cryptography — Part 6: Message authentication codes (MACs);

In addition, WG 2’s roles in the cooperation with TC 68 Banking and Related Financial Services are of strategic importance.

3.3.3 Working Group 3
The many years of successful application of ISO/IEC 15408 and ISO/IEC 18045 have expanded the need for assurance in a wide range of products, and wider assurance scenarios. This has led to initiatives to cover more and complementing security assurance evaluation methods, and Working Group 3 is embracing in a review of the core ISO/IEC 15408 and ISO/IEC 18045 that will address these new market needs, and which should be efficient in doing so for the future 10-20 years.

All new IT security challenges, like cloud computing, or cyber security at large, demand secure technology, products, systems and services, and their security evaluation and testing is increasingly important, a demand that the WG 3 needs to address and provide responses to. The maintenance of the current WG 3 project catalogue is being challenged with new study periods and work item proposals that aim to address these new areas of IT security evaluation and testing.
3.3.4 Working Group 4

Work is continuing in the areas of:

- Virtualisation;
- Internet of things;
- Cybersecurity;
- Application security;
- Cloud computing;
- Public key infrastructure;
- Incident management.

A priority is the publication of:

- ISO/IEC 27034-5, Application security — Part 5: Protocols and application security controls data structure;

3.3.5 Working Group 5

After completion of foundational frameworks (especially ISO/IEC 24760 A framework for identity management and ISO/IEC 29100 Privacy framework) priorities for Working Group 5 are to develop standards according to its standards development roadmap, that is being used to identify, promote, and prioritize future work on supporting technologies, models, and methodologies. This is also influenced by the upcoming of more innovative privacy and identity management legislation around the world that relies more on standards. Example projects are Privacy impact assessment (ISO/IEC 29134), Identity proofing (ISO/IEC 29003), and Code of practice for personally identifiable information protection (ISO/IEC 29151). More recent examples are Privacy enhancing data de-identification techniques (ISO/IEC 20889), Guidelines for online privacy notices and consent (ISO/IEC 29184), Privacy engineering (ISO/IEC 27550), and Enhancement to ISO/IEC 27001 for privacy management — Requirements (ISO/IEC 27552).
JTC 1/SC 27 DASHBOARD 2016
Performance Indicators

Systematic Reviews

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Closed</th>
<th>Closed On time</th>
<th>% on time</th>
<th>Number Published</th>
<th>Avg time to Publish</th>
<th># within timeframe</th>
<th>% within timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>9</td>
<td>9</td>
<td>100%</td>
<td>22</td>
<td>37.64</td>
<td>14</td>
<td>63,63%</td>
</tr>
<tr>
<td>2016</td>
<td>4</td>
<td>4</td>
<td>100%</td>
<td>21</td>
<td>53.76</td>
<td>3</td>
<td>57,14%</td>
</tr>
</tbody>
</table>

New Work Items
- Security guidelines for design and implementation of virtualized servers
- Privacy Engineering
- Criteria and methodology for security evaluation of biometric systems
- Anonymous entity authentication
- Enhancement to ISO/IEC 27001 for privacy management
- Lightweight cryptography – Part 6: Message authentication codes
- Anonymous entity authentication – Part 3: Mechanisms based on blind signatures

Work Group Studies
- Cyber insurance guidelines
- Cyber resilience guidelines
- Broadcast authentication protocols
- Guidelines for Privacy in Internet of Things
- Guidelines for Security in Internet of Things
- ICT readiness for electronic discovery
- Information security guidance for PKI service providers
- Design specification for the revision of 27002, 27005 and 27014