AN INTRODUCTION TO STANDARDS RELATED TO INFORMATION SECURITY

Johann Amsenga

Eclipse RDC, a division of Armscor Business (Pty) Ltd
amsenga@acm.org
+27 12 671 6915
P.O. Box 7036, Pretoria, Republic of South Africa, 0001

ABSTRACT

"The good thing about standards is that there are so many of them." This humorous comment is often made when some well meaning team member wants to solve a problem by referring to a standard. This may be true, but what is also true is that information systems are becoming more "complex" (in the vaguest sense of the word), that systems and the information processed are more distributed and that the requirement for access is more demanding. Also, the requirement for access is not limited to, or from, a specific or single site, organisation or even country. This has a huge effect on interfacing requirements, information storage and presentation formats and, of course, security.

Adopting internationally recognised standards is a definite route to solve a lot of these problems. Standards are a mechanism for different stakeholders to refer to a common, trusted reference. Standards provide a common technological language, thus enabling a system stakeholder to provide definitions for terms used in a project, and to qualify vague expressions such as "complex".

The South African Bureau of Standards (SABS) is the recognised national institution for the promotion and maintenance of standards in South Africa. The SABS prepare and publish South African National Standards (identified by the letters SANS) reflecting national consensus on a wide range of subjects. A business unit of the SABS, Standards South Africa (StanSA), administers more than 450 technical committees and subcommittees to produce standards. The SABS is a member body of the

International Organisation for Standardisation (ISO) and participates actively in a number of their committees.

This tutorial provides a short introduction to International and South African National Standards related to Information Security. Some of the existing standards are highlighted and the development process is introduced. The tutorial focuses on ISO/IEC International Standards and the national adoption or development by StanSA.

KEY WORDS
Information Security, Security Requirements, System Life Cycle, International Standards, National Standards, SABS, StanSA, ISO/IEC, Development of Standards

AN INTRODUCTION TO STANDARDS RELATED TO INFORMATION SECURITY

1 INTRODUCTION

Information systems are becoming more complex – systems and the information processed are more distributed and the requirement for access is more demanding. Also, the requirement for access is not limited to, or from, a specific or single site, organisation or even country. This has a huge effect on interfacing requirements, information storage and presentation formats and, of course, security.

Adopting internationally and nationally recognised standards is a definite route to solve a lot of these problems. Standards are a mechanism for different stakeholders to refer to a common, trusted reference, and provide a common technological language.

The trusted reference and technological language provided by International Standards are especially important in the information security environment where many organisations view information security as new technology or an uncharted domain. These organisations often have to rely on so called security experts or, even worse, self proclaimed gurus. Security related standards can help these organisations to see through the "buzz" words and to better understand the role and place of security and the related technologies.

This paper provides an introduction to International and South African National Standards related to Information Security. Some of the existing standards are highlighted and the development process is introduced. The paper focuses on ISO/IEC International Standards and the national adoption or development by StanSA.

2 STANDARDS – PURPOSE AND ADVANTAGES

The South African Bureau of Standards (SABS) describes a standard as follows:

A Standard is a published document which lists specifications and procedures established to ensure that a material, product, method or service is fit for its purpose and perform in the manner it was intended for.

Standards define quality and establish safety criteria. Conformance to standards ensures quality and consistency.

The World Trade Organisation (WTO) defines a standard in its Agreement on Technical Barriers to Trade (TBT) as:

A document approved by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for products or related processes and production methods, with which compliance is not mandatory. It may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements as they apply to a product, process or production method.

Life is too short to reinvent the wheel. In the ever progressing world of information technology, it is good to know that a lot of the work has already been done. However, it is difficult to known which of the vast amount of resources can be trusted. International security related standards are developed by experts in the field, checked by the national standards bodies of many countries, and are internationally accepted and proven. National standards, on the other hand, also take the relevant country's environment into account. International standards adopted as a national standard, provides the best of both worlds.

3 INFORMATION SYSTEMS AND INFORMATION SECURITY

It is important to remember that security must be a stated requirement for any information system. Security must have the same importance as other requirements, such as functionality and usability. Also, security is a quality attribute. Security cannot be viewed in isolation. It is as much part of a system as any other component, and influences the concept, development, production, utilisation, support and retirement of a system just like any other requirement and limitation placed on the system. It is imperative that security be taken into account in all processes and stages of a system's life cycle, and that security must be managed.

From these observations, it is clear that information security cannot be addressed by applying information security standards alone. The information security standards must be used together with information system, management related and quality standards.

It is for this reason that this paper introduces not only information security standards, but also system life cycle related standards, quality management and quality evaluation standards, and information security management standards.

4 INFORMATION SECURITY STANDARDS

Probably the most well known information security standard was the ISO/IEC 17799, which was adapted from the British standard BS 7799. This standard now forms part of the ISO/IEC 27000 family of standards that addresses Information Security Management Systems (ISMS), and has been renumbered to ISO/IEC 27002.

ISO, together with IEC, published a whole portfolio of standards related to generic methods, techniques and guidelines for information, IT and communication security. This includes the areas of security management, conformance assessments and security evaluation criteria. Work continues in the maintenance of these standards, as well as the development of new standards.

4.1 Information Security Management Systems

Information security is a fundamental component of governance and social responsibilities of organisations. Organisations are expected, and sometimes legally obliged, to implement and manage information security. Information security management systems are addressed by the ISO/IEC 27000 family of standards.

Examples of standards published or being developed in this category are:

- ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27003: Information technology – Security techniques – Information security management system implementation guidance
- ISO/IEC 27004: Information technology – Security techniques – Information security management measurements
- ISO/IEC 27005: Information technology – Security techniques – Information security risk management

- ISO/IEC 27006: Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

4.2 Cryptography and Security Mechanisms

A number of standards are produced by ISO/IEC that covers cryptographic and non-cryptographic techniques and mechanisms for use in security services. The techniques and mechanisms include:

- Confidentiality
- Entity authentication
- Non-repudiation
- Hash functions
- Digital signatures
- Key management

Examples of standards published or being developed in this category are:

- ISO/IEC 9797-1: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher
- ISO/IEC 9798-1: Information technology – Security techniques – Entity authentication – Part 1: General
- ISO/IEC 9979: Information technology – Security techniques – Procedures for the registration of cryptographic algorithms
- ISO/IEC 10118-1: Information technology – Security techniques – Hash-functions – Part 1: General
- ISO/IEC 11770-1: Information technology – Security techniques – Key management – Part 1: Framework
- ISO/IEC 15846-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General
- ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers

4.3 Security Evaluation Criteria

The standards for IT Security evaluation and certification of IT systems, components, and products are also very important. These standards include consideration of computer networks, distributed systems, associated application services, etc. Distinction is made on three aspects:

- Evaluation criteria
- Methodology for the application of the criteria
- Administrative procedures for evaluation, certification an accreditation schemes

Examples of standards published or being developed in this category are:

- ISO/IEC 15408-1: Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 15408-2: Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
- ISO/IEC 15408-3: Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements
- ISO/IEC 15443-1: Information technology – Security techniques – A framework for IT Security assurance – Part 1: Overview and framework
- ISO/IEC 15443-2: Information technology – Security techniques – A framework for IT Security assurance – Part 2: Assurance Methods
- ISO/IEC 15443-3: Information technology – Security techniques – A framework for IT Security assurance – Part 2: Analysis of Assurance Methods
- ISO/IEC 18045: Information technology – Security techniques – A framework for IT Security assurance – Methodology for IT Security Evaluation

4.4 Security Controls and Services

With the growing requirements for standards and guidelines addressing services and applications supporting the implementation of ISO/IEC 27001 control objectives and controls, a number of standards are being produced by ISO/IEC within the context of an overall internal control structure.

Examples of standards published or being developed in this category are:

- ISO/IEC 18043: Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
- ISO/IEC 18044: Information technology – Security techniques – Information security incident management

- ISO/IEC 24762: Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27033-1: Information technology – Security techniques – Network Security – Part 1: Guidelines for network security
- ISO/IEC 27034-1: Information technology – Security techniques – Guidelines for Application Security – Part 1: Overview and Concepts

4.5 Identity Management and Privacy Technologies

ISO/IEC develops and maintains standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

Examples of standards published or being developed in this category are:

- ISO/IEC 24760: Information technology – Security techniques – A framework for identity management
- ISO/IEC 29100: Information technology – Security techniques – A privacy framework
- ISO/IEC 29101: Information technology – Security techniques – A privacy reference architecture
- ISO/IEC 29115: Information technology – Security techniques – Entity authentication assurance

5 INFORMATION SYSTEM ENGINEERING STANDARDS

The introduction to ISO/IEC 15288 (Systems and Software Engineering – System life cycle processes) states the following.

The complexity of man-made systems has increased to an unprecedented level. This has led to new opportunities, but also to increased challenges for the organisations that create and utilise systems. These challenges exist throughout the life cycle of a system and at all levels of architectural detail. They arise from several sources:

- There are inherent differences among the hardware, software and human elements from which systems are constructed.
- Almost every present-day system contains, and/or is modelled and supported by computer-based technology.
- There is a lack of harmonization and integration of the involved disciplines, including science, engineering, management and finance.

There is therefore a need for a common framework to improve communication and cooperation among the parties that create, utilise and manage modern systems in order that they can work in an integrated, coherent fashion.

The standards produced by ISO/IEC in the domain of systems and software engineering, such as ISO/IEC 15288, concern those systems that are man-made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities.

Standards such as ISO/IEC 15288 provide a common process framework covering the life cycle of man-made systems. This life cycle spans the conception of ideas through to the retirement of a system. It provides the processes for acquiring and supplying systems. In addition, this framework provides for the assessment and improvement of the life cycle processes.

ISO/IEC 15288 also provides processes that support the definition, control and improvement of the life cycle processes used within an organisation or a project. Organisations and projects can use these life cycle processes when acquiring and supplying systems.

All these aspects are applicable to information security. Information security always forms part of a bigger system, and should thus be part of the consideration of the whole system, throughout the full life cycle, starting with the requirements imposed by security during the requirements analysis stages. Implementing information security results in the creation of a system in its own right, subject to all processes and standards of handling man-made systems. Information systems and information security cannot and should not be viewed as two mutually exclusive subjects.

As with information security, ISO, together with IEC, publishes a whole portfolio of standards related to processes, supporting tools and supporting technologies for the engineering of software products and systems. Work continues in the maintenance of these standards, as well as the development of new standards.

Since the scope of this work is so vast, examples of only a few of the areas addressed are given here.

5.1 Software Product Measurement and Evaluation

Standards and technical reports for software products evaluation and metrics for software products and processes. The software product quality requirements and evaluation (SQuaRE) series of standards are being developed in this area. Examples are:

- ISO/IEC 25000: Software Engineering -Software product Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE
- ISO/IEC 25001: Software engineering -Software product Quality Requirements and Evaluation (SQuaRE) - Planning and management
- ISO/IEC 25020: Software engineering -Software product Quality Requirements and Evaluation (SQuaRE) - Measurement reference model and guide

5.2 Life Cycle Management

Standards and technical reports on Life Cycle Management.

- ISO/IEC 12207: Systems and Software Engineering - Software Life Cycle Processes
- ISO/IEC 15026: Systems and Software Engineering - Systems and Software Assurance
- ISO/IEC 15288: Systems and software engineering - System life cycle processes
- ISO/IEC 15939: Systems and software engineering - Measurement process
- ISO/IEC 16085: Systems and software engineering -Life cycle processes -Risk management

6 OTHER STANDARDS

Due to the practical limitations of this paper, other applicable standardisation efforts of ISO and IEC are only listed.

6.1 Financial Services

Standards in the field of banking, securities and other financial services.

6.2 Quality Management and Quality Assurance

Standards for quality management, including generic quality management systems and supporting technologies. The well-known ISO 9000 series falls within this scope.

6.3 Telecommunications and Information Exchange Between Systems

Standards for telecommunications dealing with the exchange of information between open systems including system functions, procedures, parameters and equipment, as well as the conditions for their use.

6.4 Cards and Personal Identification

Standards in the area of identification and related documents, cards, and devices associated with their use in interindustry applications and international interchange.

6.5 Automatic Identification and Data Capture Techniques

Standards for data formats, data syntax, data structures, data encoding, and technologies for the process of automatic identification and data capture and of associated devices utilised in inter¬industry applications and international business interchanges.

6.6 Biometrics

Standards for generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems.

7 DEVELOPMENT OF INTERNATIONAL STANDARDS

A number of organisations develop international standards – ITU, IEEE, IEC, to name but a few. Increasingly, the SANS are being harmonised with international standards in order to facilitate trade.

The International Organisation for Standardisation (ISO) produces voluntary consensus standards through its decentralised global system of standardisation. This paper focuses on ISO because of the active involvement of the SABS in ISO and ISO/IEC committees.

ISO states the follow regarding the development of standards.

ISO is a network of the national standards institutes of 157 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organisation, its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members are in the private sector. Therefore, ISO is able to act as a bridging

organisation in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

Although ISO standards are voluntary, the fact that they are developed in response to market demand, and are based on consensus among the interested parties, ensures widespread applicability of the standards. Consensus, like technology, evolves and ISO takes account both of evolving technology and of evolving interests by requiring a review of its standards at least every five years to decide whether they should be maintained, updated or withdrawn. In this way, ISO standards retain their position as the state of the art, as agreed by an international cross-section of experts in the field.

Technical committees are established to serve specific industries or generic subjects, in order to develop International Standards or other ISO publications appropriate to the needs of that sector. Subcommittees are established and dissolved by the parent technical committee, subject to ratification by the technical management board. A subcommittee is set up to focus on specific parts of the overall standards requirement. Technical committees or subcommittees may establish working groups for specific tasks. All national bodies have the right to participate in the work of technical committees and subcommittees, either as a P-member, an O-member or a L-member.

P-members participate actively in the work, and have an obligation to vote on all questions formally submitted for voting within the technical committee or subcommittee, on enquiry drafts and final draft International Standards, and to participate in meetings. O-members follow the work as observers, and may receive committee documents and have the right to submit comments and to attend meetings. L-members (liaison members) has no power of vote, but has some options to attend meetings and receive documents.

A few of the relevant technical committees are listed below.

- ISO/IEC JTC 1 (Information Technology)
- ISO TC 68 (Financial services)
- ISO TC 176 (Quality management and quality assurance)

JTC 1 is a Joint Technical Committee of ISO and the International Electrotechnical Committee (IEC), and is responsible to develop standards and technical reports for information technology. A few of the relevant subcommittees of JTC 1 are listed below.

- ISO/IEC JTC 1 SC 6 (Telecommunications and Information Exchange Between Systems)
- ISO/IEC JTC 1 SC 7 (Systems and Software Engineering)
- ISO/IEC JTC 1 SC 17 (Cards and Personal Identification)
- ISO/IEC JTC 1 SC 25 (Interconnection of Information Technology Equipment)
- ISO/IEC JTC 1 SC 27 (Security Techniques)
- ISO/IEC JTC 1 SC 31 (Automatic identification and data capture techniques)
- ISO/IEC JTC 1 SC 37 (Biometrics)

7.1 Information Security Standards

SC 27 of JTC 1 is responsible for standardisation of generic methods and techniques for IT Security. This includes:

- identification of generic requirements (including requirements methodology) for IT system security services,
- development of security techniques and mechanisms (including registration procedures and relationships of security components),
- development of security guidelines (e.g. interpretative documents, risk analysis), and
- development of management support documentation and standards (e.g. terminology and security evaluation criteria).

SC 27 consists of the following working groups:

- WG 1 (Information security management systems)
- WG 2 (Cryptography and security mechanisms)
- WG 3 (Security evaluation criteria)
- WG 4 (Security controls and services)
- WG 5 (Identity management and privacy technologies)

7.2 Systems and Software Engineering Standards

SC 7 of JTC 1 is responsible for standardisation of processes, methods and supporting technologies for the engineering and management of software and systems throughout their life cycles.

SC 7 consists of the following working groups:

- WG 1a (ICT Governance)
- WG 2 (Systems and Software Documentation)
- WG 4 (Tools and Environment)
- WG 6 (Software Product Measurement and Evaluation)
- WG 7 (Life Cycle Management)
- WG 10 (Process Assessment)
- WG 19 (Open distributed processing and Modelling Languages)
- WG 20 (Software Engineering Body of Knowledge)
- WG 21 (Asset Management)
- WG 22 (Vocabulary)
- WG 23 (System Quality Management)
- WG 24 (SLC Profiles and Guidelines for VSE)
- WG 25 (IT Service Management)
- WG 26 (Software testing)
- WG 42 (Architecture)

8 DEVELOPMENT OF SOUTH AFRICAN STANDARDS

The South African Bureau of Standards (SABS) is the recognised national institution for the promotion and maintenance of standards in South Africa. The SABS prepare and publish South African National Standards (identified by the letters SANS).

As with ISO, standards are developed by committees. Committees can be technical committees (TCs), subcommittees (SCs) of technical committees, or working groups (WGs). A business unit of the SABS, Standards South Africa (StanSA), administers more than 450 technical committees and subcommittees to produce standards.

Technical committees are constituted to be representative of valid national interests in the standardisation of products or processes. Membership is preferably on the basis of organisation, association or forum representation as opposed to an individual basis. An organisation can join a technical committee or subcommittee as a P-member or an O-member.

A P-member participates actively in the work, and has an obligation to respond to documents circulated for comment, voting or both, and to participate in and vote at meetings. An O-member follows the work as an observer. Such a member will receive committee documents and may submit comments and participate in meetings, but may not vote.

The development of South African standards is funded by the state. StanSA acts as a facilitator in the development and maintenance of South African standards, and also as the publisher of standards.

Two options are available when considering a new national standard:

- Adopt without change an international or regional standard. This has the advantage that the resulting adopted standard is produced cheaply, quickly and easily. It might not, however, represent fully the needs and requirements of the South African market.
- Develop a South African standard containing at least some different requirements. This has the advantage that a more focused standard can be achieved that addresses local needs well. The development of such a standard is costly and time consuming, and the result of the process may well be a re-invention of the wheel.

Nearly all the information security related SANS standards are adopted from ISO/IEC International Standards or ISO/IEC Technical Reports.

The underlying principles of the preparation of national standards and other normative documents published by StanSA are described in SANS 1-1:2003 Standards for Standards, Part 1: The development of national standards and other normative documents.

A few of the relevant technical committees are listed below. The stated responsibilities have been taken from the scope of each committee as provided on its website.

- StanSA TC 71 (Information Technology) is responsible for standardisation and dissemination of information in the field of information technology and electronic data interchange.
- StanSA TC 74 (Communication Technology) is responsible for standardisation in the field of communication technology of consumer and professional electronics.
- StanSA TC 168 (Banking Sector), which is responsible for standardisation in the field of the banking, securities and other financial services.
- StanSA TC 176 (Quality Assurance and Quality Management Matters) is responsible for standardisation in the field of quality assurance and

quality management including generic quality management systems (QMS) and supporting technologies.

- StanSA TC 178 (Risk Management) is responsible for standardisation in the field of organisation wide risk management in accordance with good corporate governance and other risk management best practices.
- • StanSA TC 179 (Security Management) is responsible for standardisation of systematic approaches to security management in various fields.
- StanSA TC 5120.14 (Security) is responsible for standardisation in the field of security in terms of entrance control and the storage of valuables and the minimisation risk.

It may seem strange that the committees for Security Management and Security are also listed. However, it must be remembered that physical security also plays a role in information security.

8.1 Information Security Standards

SC 71F (Information Security) is a subcommittee of TC 71. This committee is responsible for Standardisation in the field of information security, including guides and codes of practice intended to assist organisations to develop security standards and effective security management practices, as well as specifications to support certification of companies as a means to promote confidence by other organisations and consumers.

The activities of StanSA SC 71F and its working groups correspond to those of ISO/IEC JTC 1 SC 27.

8.2 ICT Systems and Software Engineering Standards

SC 71C (ICT Systems and Software Engineering) is a subcommittee of TC 71, and is responsible for Standardisation in the field of systems and software engineering, excluding hardware. This may be expanded as standardisation of processes, supporting tools and supporting technologies for the engineering of software products and systems, and the development of a unified set of systems and software engineering standards widely accepted by the intended class of users.

The activities of StanSA SC 71C and its working groups correspond to those of ISO/IEC JTC 1 SC 7, although because of resource limitations, not all SC 7 working groups are always addressed.

9 HOW TO BECOME INVOLVED

StanSA participate in technical committees and subcommittees of ISO and the International Electrotechnical Commission (IEC). The views of local stakeholders are gathered through local technical committees and subcommittees, and conveyed to the appropriate international committees of ISO and IEC. This is an extremely important function, as it ensures that, wherever possible, local considerations are incorporated into international standards during their formation.

Because StanSA is committed, wherever possible, to adopting international standards for local use, it is vital that international standards accommodate the needs of local stakeholders. Also, through this participation, South Africa can influence the contents of international standards.

It is important that South African organisations participate in standards committee work, to ensure that their views are known.

Organisations wishing to be part of this exciting opportunity, should contact the SABS, or the author.

10 CONCLUSION

This paper only touched the tip of the iceberg where international security standards are concerned. For more information on ISO and SANS standards, a visit to the respective web sites are recommended. Also, ISO is only one of a number of international organisations developing standards or recommendations related to information security, for example the IEEE and ITU-T.

11 REFERENCES

SABS, Web page of the South African Bureau of Standards, http://www.sabs.co.za, Visited June

2007 ISO, Web page of the International Organisation for Standardisation, http://www.iso.org, Visited June 2007

ISO, My ISO Job - Guidance for delegates and experts, 2005 ISO, Joining In – Participating in International Standardization, 2007 Standards South Africa, SANS 1-1, Standards for standards - Part 1: The Development of National

Standards and other Normative documents, Edition 1, 2003 ISO, ISO/IEC Directives Part 1, Procedures for the Technical Work, Edition 5, 2004 ISO/IEC JTC1, ISO/IEC JTC 1/SC27 N5757, Directives, Edition 5, Version 3.0, 2007