ISO/IEC JTC 1 N 9058

2008-05-13

ISO/IEC JTC 1
Information Technology

Document Type:	**Other Document(Defined)**
Document Title:	**Consideration of Scopes of Existing Standardisation Organisations**
Document Source:	**JTC1 Study Group on IT Governance Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for information**
Action ID:	**Information**
Due Date:	
No. of Pages:	**10**

ISO/IEC JTC 1 Study Group on IT Governance N0020

DATE: 2008-05-09

ISO/IEC JTC 1 Study Group on IT Governance Secretariat: SA (AU)

DOC TYPE:	Document for discussion
TITLE:	Consideration of Scopes of Existing Standardisation Organisations
SOURCE:	JTC1 Study Group on IT Governance secretariat
PROJECT:	
STATUS:	This document was produced by John Graham on the request of the JTC1 SGITG at meeting 001. This document was informally circulated to JTC 1 SGITG members on 6 May, and is now formally circulated to JTC 1 SGITG members and JTC 1 National Bodies and Subcommittees for use by the delegates to the second meeting of the JTC 1 SGITG, Berlin, 17-19 May 2008

.

ACTION ID:	FYI
DUE DATE:	
DISTRIBUTION:	JTC1 Study Group on IT Governance
MEDIUM:	
NO. OF PAGES:	9

Consideration of Scopes of Existing Standardisation Organisations

Initial Discussion

Prepared by John Graham (AU) for JTC1 Study Group on IT Governance
Berlin Meeting – May 17th to 18th 2008

An important part of the consideration of existing standards is the correlation of the coverage of those standards with the scopes of the bodies producing those standards. This is particularly important for entities within formal standard setting frameworks such as ISO and IEC.

This document is a preliminary document looking at JTC1 and four sub-committees (SC) of JTC1. The SCs are SC7, SC17, SC27 and SC37. The SCs are obviously not chosen at random, rather they are chosen for convenience and also on an arbitrary basis.

The actual scopes used for this document are based on a web search for material. They may or may not be current or correct, however they can be illustrative.

The basic thesis for this document is that the formally approved scope of a standard producing body is, or should be, more significant than the actual coverage of standards produced by that body. It is, if you like, a comparison between the “de jure” and “de facto” scope of a body.

This document is based on the document “A Framework for Organising and Categorising Standards related to Governance of Information Technology” by Mark Toomey. The version used is the version circulated to the Study Group in draft form as N0018 dated 2008-04-02. The document “IT and Governance Standards Information Request” also by Mark Toomey. This is document N0019 also dated 2008-04-02 and is also referred to.

Statements of Scope Used:

JTC 1: Standardization in the field of Information Technology.

Note: Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.

Source: ISO/IEC JTC 1 N8789 2007-09-24 JTC 1 Business Plan for the Period November 2006 – October 2007

JTC 1 SC 7:

Standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems.

Source: ISO/IEC JTC 1/SC 7 N3512 SC7 Chairman Presentation and AG Meeting Outputs, SC7 Opening Plenary, Bangkok, 2006-05-15

JTC 1 SC 17:

Standardization in the area of a) identification and related documents, b) cards, and c) devices associated with their use in inter-industry applications and international interchange

Source: ISO/IEC JTC 1/SC 17 WG1 N1416 Summary of SC17 Standards v.03

Consideration of Scopes of Existing Standardisation Organisations

Initial Discussion

Prepared by John Graham (AU) for JTC1 Study Group on IT Governance
Berlin Meeting – May 17th to 18th 2008

JTC 1 SC 27:

Standardization 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).

Excluded are:
-the embedding of mechanisms in applications.

Note that the SC 27 Scope and Area of Work includes the standardisation of cryptographic algorithms for integrity, authentication and non-repudiation services. Furthermore it includes the standardisation of cryptographic algorithms for confidentiality services for use in accordance with internationally accepted policies.

Source: Various. Primary Source: BSI Document IST_33-0401_06.pdf ISO/IEC JTC 1 SC 27 – IT Security Techniques

JTC 1 SC 37:

Standardization of genetic biometric technologies pertaining to human beings to support Inter-operability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.
Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.
Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protection techniques, biometric security testing, evaluations, and evaluations methodologies.

Source: ISO/IEC JTC 1 SC 37 N348 2003-10-24 SC 37 Business Plan for the Period December 2002 through September 2003

Framework for Comparison and Analysis

In order to provide consistency with the study of actual standards produced, this discussion uses the framework as presented in N0018. The following is paraphrased from that document for brevity and clarity. Individual references to the document have not been cited.

This framework by Mark Toomey is based on a number of domains of corporate governance of which the particular domain considered is Information Technology.

Within that domain the 5 layers or categories are specified as:

Corporate Governance of Information Technology: “the system by which the current and future use of IT is directed and controlled” (Corporate Governance Layer)

Management Control of Information Technology: “ the system of controls and processes required to achieve the strategic objectives set by the organisation’s governing body” (Management Control Layer)

“The Systems & Applications Layer contains standards that relate to a specific use of IT to provide a capability to an organisation.”

“The Technical Delivery Layer contains standards that relate to the design and construction of Systems and Applications.”

“The Components and Interfaces Layer contains standards that relate to the basic building blocks of Information Technology.”

The framework allows for the identification of Sub-Domains as required.

The graphical rendition of the framework is fully covered in N0018.

For this discussion the Layers will be abstracted to five points on an ordinal scale. Sub-Domains will be used as appropriate to complement the Layers as allowed in N0018.

The measurement of coverage in each of the Layers is obviously constrained by the Sub-Domain. Sub-Domains are very prominent in the sample of scopes used. In many cases the Sub-Domain is seemingly accurately reflected in the name of the SC. There is a potential issue in the more accurate definition of those Sub-Domains and the related issues of Layers that, at least in part, transcend Sub-Domains. There is also the issue of intersection of Sub-Domains that must be considered carefully

The estimate of a scope’s coverage of a Layer, within the confines of any identified Sub-Domain, will be essentially on the 5 point scale suggested by Mark Toomey in the immediate predecessor document to N0018 (private communication). For each Layer the Extent of coverage will be measured on a 5 point scale (0= nil, 5 = complete). The intervening values suggested are: 1 = peripheral, 2 = slight, 3 = significant, 4 = substantial. I believe the term ‘complete’ is more appropriate than ‘substantial’ for the 5th point although I do get the impression from a perusal of the data that ‘complete’ may also imply ‘exclusive’ which is not necessarily desirable. The concept of percentage of scope seems to be inappropriate although it appears to be appropriate for actual standards documents.

The estimates, a term I think must be used instead of measurements due to their subjectivity, should be treated as values on a 6 point ordinal scale and any analysis based on this.

Each Sub-Domain classification and estimate should be accompanied by a brief description/justification.

Consideration of Scopes of Existing Standardisation Organisations

Initial Discussion

Prepared by John Graham (AU) for JTC1 Study Group on IT Governance
Berlin Meeting – May 17th to 18th 2008

Illustrative Application of Framework

Applying the framework to JTC 1 and the four SCs given above illustrates how the analysis would function. In this case the analysis is superficial owing to the limited time available. It is designed to facilitate discussion of the framework rather than the actual analyses.

1. JTC 1 Overview Scope

Scope Statement: Standardization in the field of Information Technology.

Sub-Domain: None (All inclusive)

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	5	No exclusions
Management Control Layer	5	No exclusions
Systems & Applications Layer	5	No exclusions
Technical Delivery Layer	5	No exclusions
Components and Interfaces Layer	5	No exclusions

]

2. JTC 1 Note to Scope

Scope Statement: Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.

Sub-Domain: None (All inclusive)

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	0	Not included
Management Control Layer	3	Some argument for inclusion in development
Systems & Applications Layer	3	Can be included as a synthesis of the individual elements
Technical Delivery Layer	5	Fully covered
Components and Interfaces Layer	5	Fully covered

3. SC 7

Scope Statement: Standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems.

Sub-Domain: Software (products and systems)

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	**0**	Not included
Management Control Layer	**0**	Not included
Systems & Applications Layer	**2**	It is arguable that specific systems and applications are outside this scope
Technical Delivery Layer	**5**	Fully covered under processes and supporting tools
Components and Interfaces Layer	**5**	Fully covered under supporting technologies

4. SC 17

Scope Statement: Standardization in the area of a) identification and related documents, b) cards, and c) devices associated with their use in inter-industry applications and international interchange

Sub-Domain: Cards and identity documents

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	**0**	Not included
Management Control Layer	**0**	Not included
Systems & Applications Layer	**4**	Covered particularly in c) but also in a) and b).
Technical Delivery Layer	**5**	Fully covered
Components and Interfaces Layer	**5**	Fully covered

5. SC 27

Scope Statement: Standardization 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).

Excluded are:
-the embedding of mechanisms in applications.

Note that the SC 27 Scope and Area of Work includes the standardisation of cryptographic algorithms for integrity, authentication and non-repudiation services. Furthermore it includes the standardisation of cryptographic algorithms for confidentiality services for use in accordance with internationally accepted policies.

Sub-Domain: IT Security

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	3	Risk analysis and interpretative documents
Management Control Layer	4	Management support documentation and standards
Systems & Applications Layer	5	Security techniques and mechanisms.
Technical Delivery Layer	5	Cryptographic algorithms
Components and Interfaces Layer	5	Cryptographic algorithms

6. SC 37

Scope Statement: Standardization of genetic biometric technologies pertaining to human beings to support
Inter-operability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.
Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.
Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protection techniques, biometric security testing, evaluations, and evaluations methodologies.

Sub-Domain: Biometrics

Coverage of Layers

Layer	Coverage	Rationale
Corporate Governance Layer	**1**	Cross jurisdictional and societal aspects?
Management Control Layer	**0**	Nothing evident
Systems & Applications Layer	**0**	Excluded
Technical Delivery Layer	**5**	Core of specification
Components and Interfaces Layer	**5**	Core of specification

Next Steps

The most obvious issues are the resources available to this project, the organisational scope of it, the accessibility of confirmed and correct statements of scope, the potential subjectivity of the analysis and, hence, the possibility of extracting meaningful conclusions taking into account the other issues.

The project to date has had two phases. The first was interaction with Mark Toomey to refine elements of the framework for categorisation of standards and the data required to categorise those standards. This has resulted in N0018 and N0019. These documents are Mark’s, my role has been to assist in refining and editing them. The second phase is this document. No external resources have been utilised or available to us. To complete this project for both standards and organisations as suggested at the February meeting is going to require substantial resources. In particular secretarial, web facilities and plain old fashioned leg work. Both Mark and I have ‘day’ jobs.

The organisational scope of the project needs to be carefully considered. There is no question that all SCs in JTC 1 need to be covered. There are certainly a number of ISO and IEC Technical Committees that need consideration and a few external organisations. I suggest that these can be identified by liaisons. It is arguable that the analysis of scopes is essentially irrelevant outside the confines of ISO and IEC as there is no consideration of locating this work outside ISO and IEC. The scope of the project and the associated standards project must be moderated by the availability of resources.

Consideration of Scopes of Existing Standardisation Organisations

Initial Discussion

Prepared by John Graham (AU) for JTC1 Study Group on IT Governance Berlin Meeting – May 17th to 18th 2008

The lack of availability of confirmed, correct and current statements of scope has emerged as an issue. Even though these are in the public domain they are not easy to obtain. This is an issue that needs to be addressed by the secretariat of the Study Group. I certainly have some reservations about the data used in this document.

The major issue is the potential subjectivity of the analysis and the consequent possibility of extracting meaningful conclusions. The only approach I can see is to seek a large number of responses categorising scopes according to a clear set of guidelines. The exercise of bringing together a clear set of scopes will, in itself, be useful. Asking a significant number of persons to categorise these scopes will hopefully remove much of the subjectivity. The most promising approach in the time available is to use a web based survey based on the software the secretariat is hopefully licensing. The project plan for this whole exercise needs to be very tight and well check-pointed.

I suggest that meaningful conclusions can be drawn on scopes if the response is sufficient in depth and quality. This applies equally to the enquiries on the categorisation of standards. If both responses are sufficient in depth and quality then meaningful conclusions can be drawn.

The conclusions sought relate to the overall coverage of both scopes and standards and the potential needs for extra bodies at appropriate levels.

John Graham
20th April, 2008