ISO/IEC JTC 1 N9318

2008-10-14

Replaces:

ISO/IEC JTC 1
Information Technology

Document Type:	other (defined)
Document Title:	JTC1 Study Group on IT Governance Report - Oct 2008
Document Source:	JTC1 Study Group on IT Governance 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:	18

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 Study Group on IT Governance N0038

DATE: 2008-10-09

ISO/IEC JTC 1

Study Group on IT Governance

Secretariat: SA (AU)

DOC TYPE:	**Report**
TITLE:	**JTC1 Study Group on IT Governance Report - Oct 2008**
SOURCE:	**JTC1 Study Group on IT Governance secretariat**
PROJECT:	
STATUS:	**JTC1 Study Group on IT Governance report for the 2009 JTC1 Plenary, Nara, Japan 2008**
ACTION ID:	**FYI / ACT**
DUE DATE:	
DISTRIBUTION:	**JTC1 Secretariat, Study Group on IT Governance**
MEDIUM:	
NO. OF PAGES:	**17**

Secretariat ISO/IEC JTC Study Group on ICT Governance:
Standards Australia, Level 10, 20 Bridge Street Sydney, NSW 2000
Telephone: +61 2 9237 6079; Facsimile: +61 2 9237 6020; e-mail: andrew.mckay@standards.org.au

ISO/IEC JTC1

Study Group on IT Governance

Interim Report

John Graham
Convener

Establishment

The Study Group on ICT Governance was established by Resolution 18 of JTC1 at its Plenary Meeting on the 8th to 13th October, 2007 in Australia. Terms of Reference dot points are referred to in the document headings as TOR 1 to TOR 7. References have been added below and are shown thus ***(TOR 1) .***

Resolution 18 – Establishment of Study Group on ICT Governance

JTC1 establishes a JTC1 Study Group on ICT Governance to investigate the need and feasibility of additional standardization and/or guidance in the area of ICT Governance.
The main objective of this Study Group is to understand the current activities and make recommendations to JTC1 based on the Terms of Reference below. The Terms of Reference of the Study Group are as follows:

Terms of Reference:

- Provide a definition of ICT Governance ***(TOR 1)***
- Assess the current state of affairs of ICT governance within JTC1 and its SCs and other relevant SDOs ***(TOR 2)***
- Consider the work undertaken by the SC7 SG on ICT Governance which has focused on aspects of the issue relating to SC7 scope ***(TOR 3****)*
- Review: ***(TOR 4****)*
  - related International standards ***(TOR 4.1)***;
  - elements of ICT governance in those standards ***(TOR 4.2)***;
  - national and regional governance activities ***(TOR 4.3)***;
  - existing organizations dealing with or involved in ICT Governance ***(TOR 4.4)***.
- Assess market requirements for the need and level of standardization in this area ***(TOR 5)***
- Identify a set of guiding principles for the development of ICT Governance standardization to meet market requirements ***(TOR 6)***
- Deliver a recommendation to JTC1 on actions to be taken- ***(TOR 7)***
- Meetings of the group may be physical or via electronic means

Membership in the Study Group will be open to:

- ISO/IEC JTC1 National Bodies and Liaisons, AROs and PAS submitters;
- ISO/IEC JTC1 SCs
- Members of ISO and IEC Central Office;
- ISO or IEC TCs, SCs WGs in liaison with JTC1 or its subgroups
- Invited experts with specific expertise in the field

JTC1 accepts the offer of the National Body of Australia to provide the Convener and Secretariat.

JTC1 instructs its Secretariat to issue a call for participants for the Study Group.

Acknowledgments

Dr Edward Lewis served as Convener of the Study Group from its inception until 29th May, 2008. He chaired both meetings of the Study Group and made major contributions to its work. The Study Group extends its thanks to Dr Lewis for his efforts.

Mr Andrew McKay has fulfilled the role of Secretariat for the Study Group and continues to do so. He has managed this role while battling a debilitating leg injury. The Study group thanks him for his efforts.

Participants

The Study Group Convener would like to thank the following people for their participation in the work of the Study Group:

Name	Nominating Organization	Nat. Body	Attended Meeting Sydney Feb. 19th-21st	Attended Meeting Berlin May 17th-18th
Edward Lewis (Convener to May 29)	SA	AU	In Person	In Person
Andrew McKay (Secretariat)	SA	AU	In Person	Apology
Max Shanahan	SA	AU	In Person	In Person
John Sheridan	SA	AU	In Person	Apology
Mark Toomey	SA	AU	In Person	In Person
John Graham (Convener from Aug 1)	SA	AU	In Person	In Person
Renati Barel (Acting Secretariat)	SA	AU		In Person
Alison Holt	NZS	NZ	In Person	In Person
Craig Pattison	NZS	NZ	In Person	Apology
Karen Higginbottom	ANSI	US	Apology	In Person
Melanie Cheong	SABS	ZA	Audio	In Person
Tess Du Plessis	SABS	ZA	Apology	In Person, 18th only
Alwyn Smit	SABS	ZA	Apology	
Pieter Neethling	SABS	ZA	Audio, 19th, 20th only	In Person, 18th only
Grantham Daniels	SABS	ZA		In Person
Charles Provencher	SCC / SC27	CA	In Person	In Person
Anatol W. Kark	SCC	CA		
Jake V. Th. Knoppers	SCC	CA		
Jean Bérubé	SCC	CA		In Person, 17th only
Jeffrey Posluns	SCC	CA		
Marc Taillefer	SCC	CA		
Pierre Sasseville	SCC	CA		
Serge Oligny	SCC	CA		
K.T. Hwang	KATS	KO	Apology	In Person, 17th only
Phil Brown	BSI	UK	In Person	
Peter Restell	BSI	UK	Apology	In Person
Valerie Barnole	AFNOR/SC6	FR	Audio, 19th, 20th only	In Person
Yoshiyuki Hirano		JP	In Person	In Person
Takashi Kan		JP	In Person	
Hans von Sommerfeld	SC27	DE		
Johann Amsenga	SC27	ZA		In Person, 18th only
Bernoit Poletti	SC27	LU		
Huang Zhenhai	SAC	China	Apology	
Lai Xiaolong	SAC	China	Apology	
Mika Johansson	FISMA	FI		In Person
Scott Jameson	JTC1 Chair	ISO		In Person
Angelika Plate	SC27	UK		In Person
Anders Carlstedt	SC27	SE		In Person
Asbjorn Hovsto	SC17	NO	Audio, 21st only	
François Coallier	SC7	ISO	In Person	In Person
Dennis Ravenelle	itSMF-I			In Person, 18th only
Wim van Gremberger	IND	Ind Expert	Apology	
Sushil Chatterji	IND	Ind Expert	Apology	In Person, 18th only
Bill Powell	IND	Ind Expert	Audio, 19th only	

Contents

Executive Summary

The Study Group on IT Governance has accepted the definition of the corporate governance of IT as defined in ISO/IEC 38500:2008, being the system by which the current and future use of IT is directed and controlled. It was noted by the Study Group that both JTC1 and SC7 used IT rather than ICT therefore it elected to use the term IT instead of ICT. It further elected to use “corporate governance of IT” in place of “IT governance”

The Study Group expects the definitions given to evolve, as will the current standard. It recommends that the responsibility for standardisation and harmonisation of corporate governance and management terminology be assigned to a suitably constituted body.

Current available documentation indicates that the only SC doing explicit work on the corporate governance of IT is SC7 however some scope issues are evident. Other SCs and TCs are doing highly relevant work within sub-domains of IT and specific market places. The work of SC27 and TC 68 is particularly relevant.

The work of the SC7 study Group was seen as highly relevant but did not address the issue of SC7 scope owing to the explicit statement in its establishing resolution.

The review identified a great deal of work relating to the corporate governance of IT but considerably less specifically addressing the corporate governance of IT as defined. A possible model for analysis has been outlined. A great deal of the review information has been drawn from the excellent SC7 Study Group report. The two most significant existing organisations identified were ISACA/ITGI and itSMF International.

The Study Group agreed that a full survey on market demands was not necessary however several significant documents pointed to corporate governance of IT being seen as both a major issue and, often, a misunderstood issue in the marketplace. The lack of involvement, and possibly recognition, by directors was seen as a particular concern. The work of the SC7 Study Group was drawn upon in the context of the need for standards and the King Report gave a telling statement on the need for international work. The point that standards would compliment existing conceptual frameworks rather than replace them was also emphasised.

A set of guiding principles has been recommended for the development of further standards in the field.

The Study Group recommends the formation of a working Group for the Corporate Governance of IT directly under JTC1. With this recommendation it foreshadows the possibility of eventual evolution to an SC, should it be deemed beneficial or required.

With the formation of this working Group, the Study Group requests a transition period to continue and facilitate ongoing work as well as resolve unresolved and consequential issues as not to impede progress or lose momentum while the Study Group moves to the status of a Working Group, following the JTC1 Plenary.

IT and ICT

It was noted by the Study Group that the general usage in both JTC1 and SC7 is IT (Information Technology) rather than ICT (Information and Communications Technology). The Scope of JTC1 is Information Technology rather than Information and Communication Technology. The abbreviation IT is therefore used throughout this report rather than ICT.

TOR 1 - Definition of IT Governance

The Concise Oxford English Dictionary is a reference for the English language under section 6.6.2. of ISO/IEC Directives, Part 2, 2004. All definitions attributed to the Oxford Dictionary are from the Eleventh Edition, Revised of this dictionary which is currently the most recent edition.

The Study Group agreed that, where applicable, the Oxford Dictionary definition of related terms should be used.

The definition of the immediately relevant terms is as follows.:

Govern - conduct the policy and affairs of a (state, organization, or people) – Oxford Dictionary

Governance – the action or method of governing – Oxford Dictionary

Hence the IT Governance could be reasonably defined as;

IT Governance – the action or method of governing IT

The preferred term is the Corporate Governance of IT which focuses on IT in the organisational context and is derived from:

Corporate Governance – The system by which organizations are directed and controlled.

This definition is adapted from the "Report of the Committee on the Financial Aspects of Corporate Governance", Sir Adrian Cadbury, London 1992 and the OECD Principles of Corporate Governance, OECD, 1999. It is used in ISO/IED 38500:2008. From this definition we have:

Corporate Governance of IT – The system by which the current and future use of IT is directed and controlled.

This is the core definition of ISO/IEC 38500:2008.

This report will use the Corporate Governance of IT as a replacement for IT Governance.

It is important to differentiate between management and governance. The definition of management from ISO/IEC 38500:2008 is:

Management – The system of controls and processes required to achieve the strategic objectives set by the organization's governing body. Management is subject to the policy guidance and monitoring set through corporate governance.

These definitions are initial definitions based on the first edition of the first standard on the Corporate Governance of IT, ISO/IEC 38500:2008. It is expected that they will evolve, as will the current standard.

The Study Group recommends that JTC1 assign responsibility for standardisation and harmonisation of the corporate governance and management terminology to a suitably constituted body, such as an Other Working Group under the Working Group on Corporate Governance of IT. The Study group recommends that the glossary compiled by Dr Edward Lewis (Australia) (JTC1-SGITG-N0015) be provided to any such body to help in harmonisation of terminology.

TOR 2 - Current State of Affairs of the Corporate Governance of IT within JTC1, its SCs and other relevant SDOs.

This information is compiled from the latest available business plans on the JTC1 LiveLink site. It is also supplemented by some SC submissions and covered in some detail in the review sections of this report. Some TC business plans have also been examined.

Two submissions relevant to TOR 2 were received from SC7(JTC1-SGIT-N0009, N0031) and two from SC27 relevant to TOR 2, (JTC1-SGIT-N0008, N0023). The SC27 submissions and the earlier SC7 submission were discussed by the Study Group at its meetings and noted. The second SC7 submission has been circulated to members.

The only SC that is currently doing specific work on the corporate governance of IT is SC7. They have published the first general international standard in this area (ISO/IEC 38500:2008) and have a number of NWIs and Study Groups in progress within SC7. There are however some scope issues with this SC given that JTC1 has declined on two occasions the opportunity to update the scope of SC7.

SC27 is doing a significant amount of work that is highly relevant to the corporate governance and management controls of IT. This work is in the domains of Information Security and Risk Management within the context of the corporate governance of IT and supports the requirements of the corporate governance of IT.

SC17 and 37 are doing work that is very relevant to the corporate governance of IT as it relates to ID cards and biometrics with attendant governance issues. SC31 has relevance where its work on impinges on personal identification. SC23 has particular relevance in the area of data storage media life and the attendant governance issues. SC6 also has relevance to the corporate governance of IT through its consideration of the acceptable use and treatment of information in transit.

Both ISO TC215 and TC68 have significant bearing on the corporate governance of IT within their respective market sectors of Medical Informatics and Financial Services. The relationship of TC68 is particularly strong and may well impose a general corporate governance context on the corporate governance of IT. TC215 is certainly exploring areas of the corporate governance of IT within its market place given its dealings with personal information including medical records.

TOR 3 - Consider the work undertaken by the SC7 SG on IT Governance which has Focused on Aspects of the Issue Relating to SC7 Scope

The SC7 Study Group Report is an excellent and detailed document which addressed the task:

"JTC1/SC7 instructs its Secretariat to establish a study group to investigate the possibility of additional standards or guidance in the area of ICT Governance.
As part of the scope of this study group, the direction of future activities will be determined. This scope is contained in the area of software and systems engineering."

This group was established by Resolution 924 of the 2006 Bangkok Plenary Meeting of SC7. The text quoted is from that resolution.

Due to the explicit statement in the establishing resolution the issue of SC7 scope was not addressed by the SC7 Study Group.

This report draws heavily on the SC7 Study Group Report.

TOR 4 - Review

TOR 4.1 and 4.2 - Related International Standards; Elements of Governance in those Standards

Mark Toomey (Australia)

A key factor in developing a strategy for ongoing management and development of standards for governance and management of information technology is to understand the extent to which existing standards and current work in progress addresses these two dimensions.
To establish a rigorous understanding of the orientation of standards, a five layer model was developed, proposed and accepted by the study group. The model is set out in ISO/IEC JTC1 Study Group on IT Governance N0021. From this model, an information request (ISO/IEC JTC1 Study Group on IT Governance N0032) was prepared, and issued on 25 August 2008 to the JTC1 Secretariat for on-forwarding to all JTC1 Sub Committees and Working Group Conveners with a due date of 2008-09-07. Study Group members were at the same time asked to assist in expediting responses, by "providing the document to any contacts within the JTC1 communities above that would be interested in completing the request".
As at 2008-09-19, three submissions have been received, from:

- SC7 (JTC1-SGITG-N0033);
- SC27 (JTC1-SGITG-N0034); and
- Institute of Directors, South Africa (JTC1-SGITG-N0035)

ISACA and the IT Governance Institute provided information on three products – The Board Briefing, the CobiT framework, and the new ValIT framework. This information was received too late for full integration into the report. The information confirms that one of the major frameworks (CobiT) frequently cited as being an "IT Governance" framework is in fact a management framework (which by virtue of providing management guidance contributes to governance of IT), that board responsibility for IT is an important issue, and that there is a need for further guidance on corporate governance of IT'

Twenty-three standards (including standards families and technical reports) are described in the responses, plus the King II report from South Africa. It is noted that the SC27 response, a single document that covers ISO/IEC27001 was prepared against an earlier draft version of the information request, and uses a different, less useful format for classifying the standards.

Of the standards reported by SC7, only one – ISO/IEC 38500 – was assessed as being "exclusively relevant" to Corporate Governance of Information Technology. One – ISO/IEC 16805 – was assessed as having substantial elements relative to the category, while thirteen other standards were considered to have significant elements relating to corporate governance of IT. This was an unexpected result – it had been anticipated that there would be no other standards in the SC7 portfolio that addressed Corporate Governance of IT.
Further consideration of the response from SC7 shows that all fourteen standards assessed as having substantial or significant relevance to corporate governance were also classified as being exclusively relevant to management control of IT. In the sense that corporate governance includes oversight of management, and requires assurance that management systems are both appropriate and effective, it might be considered that these standards are relevant to corporate governance. However, close inspection shows that the standards provide no specific guidance to the governing body itself and therefore qualify for inclusion in the Corporate Governance layer only by virtue of their relevance to the Management Control layer. As a result, it would seem more appropriate to consider these standards as having no more than peripheral relevance to Corporate Governance, while being predominantly relevant to Management Control.

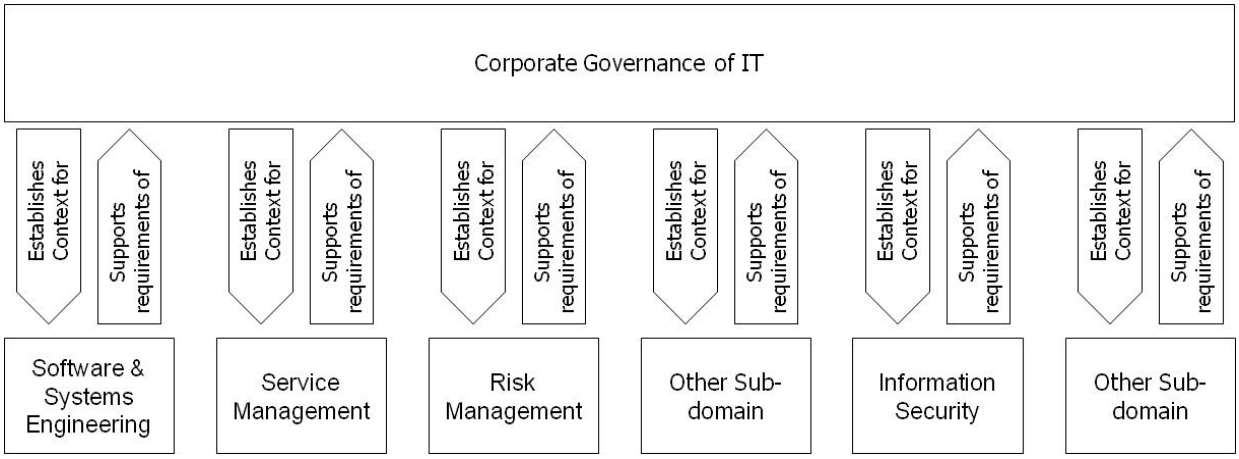
The same assessment applies to the one standard reported by SC27 – ISO/IEC 27001. While clearly addressing management control, its relevance to corporate governance appears to be primarily as a basis for the governing body's assessment of management's efforts, and the effectiveness of the organization's security arrangements. It does not provide any specific instruction to the governing body.

Looking at the SC7 and SC27 responses in a different way suggests that there are several distinct sub-domains into which the standards can be classified. The result of a preliminary assessment in this regard follows (before making decisions based on this model, it would be appropriate for the model to be formally developed and ratified):

Standard Number	Standard name	Management of Information Technology Sub-domains				
		Software & Systems Engineering	Service Management	Risk Management	Not determined	Information Security
ISO/IEC 15288	Systems Life Cycle Processes	Y				
ISO/IEC 20000	IT Services Management		Y			
ISO/IEC 12207	Software Life Cycle Processes	Y				
ISO/IEC 90003	Guidelines for the application of ISO 9001:2000 to computer software	Y				
ISO/IEC TR90005	Guidelines for the application of ISO 9001 to system life cycle processes	Y				
ISO/IEC NWIP 90006	Guidelines for the application of ISO 9001 to IT service management		Y			
ISO/IEC 15504	Process Assessment				Y	
ISO/IEC CD TR 24748	Guide for life cycle management	Y				
ISO/IEC 19770	Software asset management	Y				
ISO/IEC 16085	Life cycle processes -- Risk management			Y		
ISO/IEC 16326	Life cycle processes - Project management	Y				
ISO/IEC 26702	Application and management of the systems engineering process	Y				
ISO/IEC 14764	Software Life Cycle Processes – Maintenance	Y				
ISO/IEC TR 29110	Lifecycle Profiles for Very Small Enterprises (VSE)	Y				
ISO/IEC NP 29115	IT Performance Benchmarking Framework		Y?			
ISO/IEC CD 29118	Tools and Methods of requirements engineering and management for product lines	Y				
ISO/IEC TR 9294	Software Life Cycle Processes	Y				
ISO/IEC 15929	Systems and software engineering – Measurement process	Y				
ISO/IEC 15026	Systems and Software Assurance	Y				
ISO/IEC 25000	Software product Quality Requirements and Evaluation (SquaRE)	Y				
ISO/IEC 23026	Recommended Practice for the Internet – Web Site Engineering, Web Site Management, and Web Site Life Cycle	Y				
ISO/IEC 27001	ISMS Requirements					Y

While no attempt has been made to develop a comprehensive model, it appears clear that there are several sub-domains within the overall topic of Management of Information Technology.

The apparent relationship of standards in the Corporate Governance and Management Control layers would thus appear to be:



Further analysis is recommended to ascertain what sub-domains might exist in the above model, and to review the existing and under-development standards to determine their allocation across domains.

For completeness of this report, it is noted that the assessment of the King II report provides confirmation that corporate governance of information technology is a domain of corporate governance, and that corporate governance of IT can be and is described independently of management activities.

TOR 4.3 - National and Regional governance Activities

This work was extremely well covered in the SC7 Study Group Report. The following summary is directly from Appendix I of that report and was compiled by Brian Cusack (NZ), Mikhail Potoski (Russia) and Chistophe Feltus (Luxembourg). It has only been updated as required.

Jurisdiction	Overview
Australia	**Having an ICT Governance Standard (AS8015) that has now been accepted as an international standard (ISO/IEC 38500) is a big step towards improving business performance. The Standard is growing in stature and adoption. Experience shows that it is critical that the people at Board & CEO level are responsible for the implementation of an ICT Standard.**
Japan	**The Financial Instruments and Exchange Law (what we call J-SOX act) was enacted in May 2006 and became effective on 1st April 2008 in Japan.** **The government has published the New Legislative Framework for Investor Protection to support ''Financial Instruments and Exchange Law'' in February 2007. The introduction of the new framework will make any corporate apply IT governance strictly.**
Korea	**Strong Government support has accelerated IT adoption and now ICT Governance acceptance and growth. The Ministry of Information & Communications is driving an ICT Governance public sector framework development. In general there are big changes and high expectations for ICT Governance adoption.**
Luxembourg	**There is no national ICT Governance Standard and the culture of governance exists differently according to the sector of activity. The financial sector has implemented partial or totally IT standards such as CobiT or ITIL. The industrial sector has a lower maturity level. Point a**

Jurisdiction	Overview
	view regulator, the CSSF (National supervisory body of the financial institutions) is the main actor for the financial institutions.
New Zealand	**The NZ Government takes the implementation of International Standards seriously and aligns the OECD rankings and International trade with the attainment of Standards adoption. ICT Governance research is being undertaken in two Universities and there are several case studies in both the public and private sectors of successful Governance implementation benefiting performances.**
Russia	**There is strong industry interest towards ICT governance guidelines and methods. In current practice CobiT is widely used for this purpose, although MIT CISR IT governance model is also being considered by some organizations.**
Singapore	**Currently there are 42 national ICT standards that have been developed, adopted and maintained by the 9 technical committees of the national IT standards committee (ITSC). There is a discernible focus in the area of ICT Governance in the last year and a readiness for a new ICT Standard.**
South Africa	**There is a high awareness of ICT Governance issues and the King II Report on corporate governance has highlighted the necessity of good governance. There is much national legislation related to but not focusing on governance, as well as adoption of related ISO standards. There is readiness for ICT governance guidance (TR type 3 for state of art in specific field), however with the amount of international material available and differences in national legislation, this may be difficult.**
UK	**There are a raft of current regulations that relate to ICT Governance and additional legalisation arising from Corporate Governance (based on the UK combined Code). There are currently 37 BS ISO/IEC standards in use. The new ICT Governance standard has been much publicised in the press and is awaited.**
US	**There is no standard proposed by the US that directly addresses Governance. The CIO role is undergoing change and the IT view of Governance is mixed. Sarbanes Oxley and the general legal climate has led to a lurking fear of personal liability.**

TOR 4.4 - Existing Organizations Dealing With or Involved In the Governance of IT

This area was also well covered in the SC7 Study Group Report. There are two significant organizations dealing with the Governance of IT outside the ISO/IEC community. Both of these organizations are international in scope and membership. They are ISACA/ITGI and itSMF International.

Annex H of the SC7 Study Group Report by Max Shanahan (ISACA), Dennis Ravenelle (itSMF I), Craig Pattison (itSMF I) gives some comments as to the relevance of these organisations.

ISACA is described in the Annex as follows:

"ISACA/ITGI has a documented body of knowledge and management practices in Control objectives for IT (COBIT 4.1 an integrated framework that addresses the full lifecycle for IT), and business governance of IT (ValIT defines key processes and management practices). COBIT is a mature framework which is widely accepted within business, assurance and IT communities as a statement of best practices requirement across the full system lifecycle. It also provides performance indicators and maturity measures to assist business and IT in monitoring performance and assessing capability at the process level. ITGI has an active research base to assist the continued its development of this model. Val IT is a collection of best practices for managing the portfolio of IT-enabled business investments in an organisation."

Craig Pattison (itSMF I) makes the following points about itSMF International in his draft letter quoted in the same Annex:

“

1. itSMF International represents the leading association of practitioners in the domain of IT Service Management worldwide and by extension many of the most knowledgeable and experienced industry leaders who are challenged to define and resolve ICT Governance questions in the real world on a daily basis.
2. The relationships established between the practitioner community of the itSMF and the leading vendors of ITSM solutions and proprietary frameworks of solution providers aimed at ICT Governance support and definition, allows us to draw on a vast amount of information, research and developed work-product to the study group for consideration and possible inclusion in its standards development effort.
3. itSMF International, through its communication and distribution channels; that includes a network of over 45 national chapters around the world provides a valuable medium for disseminating information, performing research, and marketing the work of the ICT Governance Study Group.”

TOR 5 - Assessment of Market Requirements for the Need and Level of Standardization in this Area

The Study Group does not have available to it direct empirical data on the need and level of standardisation in this area.

The approach used must therefore be indirect. The area considered must be wider than that indicated by the definition of corporate governance of IT given in this report. This allows for evolution of the definition and further consideration of the difference between governance and management.

The first component of any consideration must be to establish whether the corporate governance of IT is seen as an issue in the marketplace.

The ISACA Top Business/Technology Issues, 2008 identifies seven business issues as being the top seven business issues relating to IT in 2008. These issues are:

“

1. Regulatory compliance-…..
2. Enterprise-based IT management and IT governance-….
3. Information security management-….
4. Disaster recovery/business continuity-….
5. IT value management-….
6. Challenges of managing IT risks-….
7. Compliance with financial reporting standards-….”

(ISACA Top Business/Technology Issues Survey Results, 2008 p5-6 [summarised])

This was a global survey. All of these issues are related to the corporate governance of IT to a greater or lesser extent.

The IT Governance Global Status Report 2008 and 2006 documents produced by Pricewaterhouse Coopers for the IT Governance Institute give further insight into the perceptions of these issues in the marketplace.

The Global Status Report is perhaps limited by its concentration of responses from the IT function in large corporations. The proportion of responses from general management has dropped from 27% in 2003 to 3% in 2008. It is also interesting to note that from 2006 to 2008 the proportion of large organisations (> 500 staff) in the survey went from 56% to 75%. The survey appears not to include directors (as defined in ISO/IEC 38500:2008) which is a significant omission given that they are the governors in an organization.

The 2008 Status Report contains some interesting data on the implementation of IT governance (as defined by ITGI). In the original 2003 Report 42% were not considering implementation, 15% were in the process of implementation and 25% had already implemented, in the 2008 Report 20% were not considering implementation, 34% were in the process of implementation and 18% had already implemented. The increase in the number in the process of implementation and the decrease in the number already implemented is significant in possibly indicating a growing awareness of what is involved.

There is certainly evidence that the corporate governance of IT is seen as a current issue although the evidence does concentrate on a subset of all organisations.

One of the major issues involved is the information sources used by the surveys. It is all gathered from senior executives rather than those who are, or should be, governing the organisation. The directors (as defined in ISO/IEC 38500:2008) are those who should be governing. Corporate governance of organisations is the responsibility of the directors of that organisation. The corporate governance of IT is a component of corporate governance and is equally the directors responsibility. What little information there is available suggests that directors are not accepting this responsibility. A very interesting article by Huff, S.L., Maher, P.M. and Munro, M.C. in MIS Quarterly Executive (Vol 5. No. 2/ June 2006) entitled "Information Technology and the Board of Directors: Is There an IT Attention Deficit?" states in its Executive Summary: "We found an 'IT attention deficit' in these boards. The CIOs were nearly unanimous that boards should pay attention to: the IT vision, the IT strategic plan, IT competitive advantage, IT effectiveness, IT risk, and very large application development decisions and projects. All 17 boards were unanimous only on paying attention to IT risk. One half of the boards of the financial services firms had discussed the other topics. But none of the boards of the primary resource firms (….) had discussed the other topics." The available literature suggests that this result is not unique to Canada where this work was done. There seems to be a significant lack of attention from directors to the corporate governance of IT.

The issue of potential demand for standards is less definite.

In Annex B. of the SC7 Study Group Report Bill Powell (US) lists a set of possible requirements for a standard in the area of governance of IT. These are:

- Provide clarity on appropriate roles, relationships, decision making responsibilities and accountability between directors and IT managers
- Provide clarity regarding the distinction and relationship of governance to the management system
- Provide clarity regarding the distinction and relationship of governance to the management system and management processes
- Document a core description, definition and principles of IT governance to enable the industry to move on to innovation and development regarding governance - beyond definitions.
- Enable new thought leadership from the industry. The ubiquitous critical dependencies on IT drive the need for new thought leadership regarding governance. There has been significant activity regarding governance in the industry, mostly over the problem, the general description, definition and general principles. There is close agreement, but there is still significant activity related to definition. It would benefit the industry to have a basic agreed to definition to enable the industry activity to focus on greater value contributions to this vitally important topic.
- A standard for governance could also help clarify the role and position of IT within the business. This could help promote a healthy shift from a focus on technology orientation to a business orientation within IT.
- A standard must be applicable to organizations of different size. The standard must be scalable and therefore very likely would need to be principles based.
- There is probably a future requirement for derivative material to provide additional guidance for applying governance principles to various circumstances including: Varying organization sizes, business sectors, and organization types."

While these requirements were drafted before the finalisation of ISO/IEC 38500:2008 and envisage a single standard they have an ongoing relevance for future work. These requirements are based on perceptions of market needs, if not demands, and reflect a distillation of thoughts from the SC7 Study Group by one who is intimately involved in servicing demand. The demand from directors is even less defined although, in the light of the discussion above, the need is very well defined. ISO/IEC 38500:2008 is the first standard to address directors as an audience and give them non-prescriptive advice in the form of guiding principles. There is undoubtedly further need in this area.

The question of the need for international standardisation, given a need for standardisation, is encapsulated in a quotation from the 2002 report of the King Committee on Corporate Governance (Institute of Directors in Southern Africa) which states in Para 21, page 13 of the Executive Summary:

“In the information age everyone, willingly or not, is a member of the global market place:”

The implication of this is that any work must be international to be reasonably able to serve organisations in an increasingly borderless world.

It is also important to note that standards for the corporate governance of IT are not intended as a replacement for existing frameworks but rather to complement those frameworks by giving guidance to the directors of organisations.

TOR 6 - Guiding Principles for the Development of Governance of IT Standardization to Meet Market Requirements

All standards within the domain of the Corporate Governance of IT:

- should be anchored in accepted fundamental concepts of Corporate Governance such as those of the OECD;
- should be equally applicable to large and small organisations, both public and private, profit and not for profit;
- should be “principles based” wherever appropriate and sensible;
- should be as short and simple as appropriate;
- must use a common vocabulary with clear definitions;
- must conform to a common framework (e.g. Evaluate, Direct, Monitor) for both individual documents and sets of documents;
- must be both internally and externally consistent, external consistency should be with other relevant products;
- should be able to be applied on a consistent basis without prescribing a particular organisation or process;
- must clearly show objectives and minimise exceptions.

TOR 7 - Recommendation to JTC1 on Actions to be Taken

Resolution 7 of the May meeting of the Study Group in Berlin states:

The Study Group resolves to recommend the formation of a working group for the Governance of IT directly under JTC1.

In prior discussion the Study Group foreshadowed the possibility of eventual evolution to an SC, should it be deemed beneficial or required

The initial scope of this working group would be to produce standards and other documents relating to the corporate governance of IT which has been defined as the system by which the current and future use of IT is directed and controlled.

While the Corporate Governance of IT Working Group is being formed , the Study Group requests a transition period so that the following unresolved and consequential issues may be dealt with:

It needs to be resolved whether the new working group is created by transferring WG1a from SC7 to JTC1 or whether a new entity is created and all members of WG1a are invited to join. In this latter case the secretariat and convener need to be resolved. It is assumed that the membership of the working group will be opened to all nominees of JTC1 member NBs and liaisons.

The schedule of meetings needs to be defined and issues of potential co-location resolved.

The working group will need to establish liaison relationships with all relevant bodies mentioned in this document. This includes but is not limited to SC27, SC7, TC68, TC215, ISACA/ITGI, itSMF-I and, possibly, SC6, SC17, SC23, SC31 and SC37.

The scope of the new entity needs refining. This includes further consideration of the system of corporate governance of IT and its relationship with management systems and determining which elements of these should be included in the scope. The scope must also provide for specific exclusions where work is being done by SCs and TCs relating to sub-domain (of IT) specific elements of the corporate governance of IT.

Redefinition of scope may imply creation of an SC with multiple working groups or a WG having multiple Other Working Groups and possibly AD Hoc Working Groups.
Other issues arising as a result of consideration of this report by JTC1.

Listing of Documents Registered with the Study Group

The following set of documents contains a large number of documents. Some of these are very large. The set of documents is provided as a separate ZIP file for the ref. of JTC 1 in J1N9356.

Approx. Date	Document Number	Title/Description
13/12/2007	JTC1-SGITG-N0001	Notice of meeting
21/01/2008	JTC1-SGITG-N0002	Draft agenda
28/02/2008	JTC1-SGITG-N0003	JTC1 Resolution 18 – 2007
28/02/2008	JTC1-SGITG-N0004	Interim Report of the SC7 Study Group on ICT Governance
28/02/2008	JTC1-SGITG-N0005	Draft Glossary of Terms in IT Governance v1.0
28/02/2008	JTC1-SGITG-N0006	Draft Glossary of Terms in IT Governance v2.0
23/04/2008	JTC1-SGITG-N0007	Draft Glossary of Terms in IT Governance v2.1
28/02/2008	JTC1-SGITG-N0008	Statement from ISO IEC JTC1 SC27 WG1 Convener
28/02/2008	JTC1-SGITG-N0009	SC7 Chairman Contribution to the JTC1 SG on ICT Governance
26/03/2008	JTC1-SGITG-N0010	AFNOR contribution to the agenda of SG ICT Gov meeting 8926
27/03/2008	JTC1-SGITG-N0011	Final agenda
27/03/2008	JTC1-SGITG-N0012	AFNOR's 2nd contribution to the agenda of SG ICT Gov meeting 8926
23/04/2008	JTC1-SGITG-N0013	Draft minutes
23/04/2008	JTC1-SGITG-N0013	rev1 Draft minutes JTC1 SGITG meeting Sydney Feb 2008
23/04/2008	JTC1-SGITG-N0014	Notice of meeting Berlin 17-18 May 2008
23/04/2008	JTC1-SGITG-N0015	Draft Glossary of Terms in IT Governance v3.0
23/04/2008	JTC1-SGITG-N0015	rev1 Draft Glossary of Terms in IT Governance v3.0
23/04/2008	JTC1-SGITG-N0016	N-Doc Register - N0001-N0016
19/04/2008	JTC1-SGITG-N0018	Standards Framework
19/04/2008	JTC1-SGITG-N0019	IT and Governance Standards Information Request
12/05/2008	JTC1-SGITG-N0020	Consideration of Scopes of Existing Standardisation Organisations
12/05/2008	JTC1-SGITG-N0021	Standards Framework v5 final draft
12/05/2008	JTC1-SGITG-N0022	IT and Governance Standards Information Request Rev 3
13/05/2008	JTC1-SGITG-N0023	SC27 WG 1 Liaison Statement
14/05/2008	JTC1-SGITG-N0024	SC27 response to JTC1 SGITG N0019 - IT and Governance Standards Information Request for discussion at meeting 002 in Berlin May 17-18
16/05/2008	JTC1-SGITG-N0025	Draft agenda meeting 002
5/06/2008	JTC1-SGITG-N0026	Draft minutes JTC1 SGITG meeting 002 Berlin May 2008
11/06/2008	JTC1-SGITG-N0027	Integration of EDM and PDCA Cycles - Mark Toomey
11/06/2008	JTC1-SGITG-N0028	PDCA and EDM - Angelika Plate
11/06/2008	JTC1-SGITG-N0029	AnnL PDCA - Ed Lewis
4/08/2008	JTC1 SGITG N0030	- Appointment of new convener of JTC1 SGITG
15/08/2008	JTC1-SGITG-N0031	SC7 Statement IT Governance
25/08/2008	JTC1-SGITG-N0032	IT and Governance Standards Information Request
19/09/2008	JTC1-SGITG-N0033	ISOIEC JTC1SC7 Chairman preliminary response to JTC1 N9255 IT and Governance Standards Information Request.
19/09/2008	JTC1-SGITG-N0034	SC27 response to JTC1 SGITG N0019 - IT and Governance Standards Information Request.
19/09/2008	JTC1-SGITG-N0035	SA IoD response to IT and Governance Standards Information Request.
29/09/2008	JTC1-SGITG-N0036	JTC1 SGITG ZA members response to JTC1 SGITG draft report
29/09/2008	JTC1-SGITG-N0037	ISACA-ITGI response to IT and Governance Standards Information Request.

END OF REPORT