ISO/IEC JTC 1 N 9044

2008-04-29

ISO/IEC JTC 1
Information Technology

Document Type: Other Document(Defined)

Document Title: Final Report of the SC7 Study Group on ICT Governance

Document Source: SWG on ICT Governance

Reference:

Document Status: This document is circulated to JTC 1 National Bodies for information

Action ID: Information

Due Date:

No. of Pages: 80

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 JTC1/SC7
Software and Systems Engineering
Secretariat: CANADA (SCC)

ISO/IEC JTC1/SC7 /N3973

2008-04-21

Document Type	SG Report
Title	Final Report of the SC7 Study Group on ICT Governance
Source	SWG on ICT Governance
Project	
Status	Final
Reference	Resolutions 924 and 1008, Supersede N3861
Action ID	FYI or ACT
Distribution	AG
No. of Pages	78
Note	To be discussed at the coming Berlin Plenary

Address reply to: ISO/IEC JTC1/SC7 Secretariat
École de technologie supérieure – Department of Software and IT Engineering
1100 Notre Dame Ouest, Montréal, Québec Canada H3C 1K3
secretariat@jtc1-sc7.org

www.jtc1-sc7.org

ISO/IEC JTC1/SC7

ICT Governance Study Group

Final Report

April 2008

Alison Holt & Ed Lewis

ICT Governance Study Group Chairs

PREFACE

Study Group Photo

(Thanks to Dennis, who took the photo – and so missed out in appearing in it.)

Study Group Participation

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

Alec Dorling

Alisdair McKenzie

Alwyn Smit

Andrew Dowse

Antoine Berthaut

Beatrix Barafort

Bernard O’Brien
Bill Powell
Brian Broadhurst
Brian Cusack
Christophe Feltus
Craig Pattison
Darcie Destito
Dave Sawdon
David Whapples
Dennis Ravenelle
Ed Lewis
Erik Guldentops
Frank van der Zwaag
Fred Hoberg
Frederic Georgel
Gargi Keeni
Garth Biggs
Gary Millar
Hella Shrader
Hiroshi Koizumi
Jenny Dugmore
John Graham
Jyrki Lahnalahti
K.T. Hwang
Kevin Holland
Marc Taillefer
Mark Toomey
Melanie Cheong
Mike Lowe
Paul Williams
Peter Restell
Rob Thomsett
Rupert Dodds

Steven Heal

Sushil Chatterji

Ton van Bergeijk

Wim van Grembergen

Yoshiyuki Hirano

With especial thanks to those of you who took ownership of one or more of our work items and submitted your completed material, and to the authors of the individual Annexures.

EXECUTIVE SUMMARY

The ICT Study Group, initiated at the SC7 2006 Plenary, has attracted a wide membership of ICT governance experts from 17 nations.

Study Group Work Programme

After a successful kick off meeting in Seoul at the end of October, 2006, the Study Group has made excellent progress through the Work Programme identified to complete the full report. The approach taken by the Study Group has been described in the body of this report.

Fast Track Result

The fast track ballot closed on 1st July, 2007. With 14 out of 19 in favour, and 5 negative votes out of 23 votes, the ballot result was "approved".

The next stage in the fast track process will be the resolution of the "no" votes, and the understanding and inclusion of the comments provided by the voting nations. The ad hoc ballot resolution committee met in Canberra at the beginning of August to begin this process. Australia, as requested in an SC7 resolution, has submitted a proposed distribution of comment report and a revised DIS. These have been published on the SC7 Web site.

The final ballot resolution meeting was held in Montreal at the end of October.

ISO/IEC DIS 29382 will be published as an international standard, ISO/IEC 38000 mid April 2008.

Next Steps

The Study Group will proceed as follows:

- Review ballot results of New Work Item (ISO/IEC JTC1/SC7 3895) for work to be undertaken in the area of ICT governance and related governance areas.
- Formal establishment of a Working Group once a New Work Item ballot has concluded successfully.
- Formal establishment of a Glossary of governance terms, to include definitions of Governance and Management, which are compatible with definitions in existing ISO Standards.
- Consideration of the conditions influencing governance in different national jurisdictions, with the aim of ensuring that new governance Standards have international currency.

TABLE OF CONTENTS

INTRODUCTION

Study Group Approach

At the initial face-to-face meeting in Seoul, Korea, October 2006, the Study Group started off by discussing the two Bangkok resolutions and agreeing a set of guiding principles or precepts for the work.

Precepts

The Study Group precepts were set as follows:

- There is a requirement for an international ICT governance standard, irrespective of the success of the submission of AS 8015 for fast track
- There is support for the content of the Australian standard, but it is felt that a more detailed standard is required
- There is a desire for a specification standard, but initially guidelines should be produced to drive adoption, to socialise concepts and to test acceptance. This will provide an opportunity to determine which "shoulds" are critical to the success of ICT governance
- The standard should be written at a high level to over-arch and to complement existing standards and frameworks – not to displace or replace them
- It would be desirable to set up formal liaisons to SC7 with ITGI, ISACA and a relationship with CISR – MIT Sloane School of Research

Scope

Having decided on a set of guiding principles, the group started work on defining the scope of the Study Group Report. This was carried out over a number of sessions. The group proceeded as follows:

- Reviewed documents that had been submitted for discussion
- Identified a set of initial precepts in response to the SC7 Resolution 924
- Developed a "blue sky view" of the elements of successful governance and a successful governance standard
- Came to an agreement on the content of the final Study Group Report

The Chair circulated the precepts and scope statements to the wider Study Group during the meeting in Seoul, to enable absent members to input into the direction of the group.

Programme of Work

Having determined the scope of the final report, the group then worked through the individual tasks required to complete it, assigned actions to group members and produced a timeline.

Based on resolution 924, and the agreed precepts, the Study Group work programme was set up to include:

a. The identification of a set of guiding principles for the development of an ICT Governance standard to meet market requirements

b. The identification of the ICT governance needs to be addressed in the standard

c. An assessment of where ICT governance sits within JTC1

d. A review of elements of ICT governance in existing SC7 standards

e. Analysis to determine the level of standard required to sit above existing frameworks and methodologies without replacing or displacing existing material. Identification of the sort of "standard" required - TR, code of practice or guidelines

f. Analysis of what would need to be added to AS 8015 to meet these needs

g. Analysis of whether a maturity framework could be included from the outset

h. Liaison Relationships: Contributions requested from existing bodies of knowledge

i. A review of national governance activities

j. Call to action dependent on AS 8015 fast tack result (which is now known)

WORK ITEMS

Overview

This section of the Report considers the items in the work programme that help to establish how Standards for governance should be produced. These items include establishing the definition of governance, to determine the scope of the Standard;

What is ICT Governance?

Overview

The Seoul meeting of the Study Group raised the need for a clear definition or description of "ICT Governance". The members agreed that a clear and transparent definition is essential to the effective and efficient operation of both the Study Group and of the adoption of its products.

A country delegation had objected to the adoption of AS8015 partly on the grounds that "it was too early to have a definition of ICT Governance". The reply to that comment was that its one of the values of a Standard, it provides a definition. In doing so, it can help to reduce – if not remove – the confusion in the professional and the academic literature about the topic.

For example, the most common description of ICT Governance is based upon that given by Weill and Ross (see Annex A. Concepts of IT Governance). Their definition is limited to "decision rights and accountabilities". However, the description of how these rights are determined makes it obvious that the authors are referring to 'programme-level governance; that is, the governance to be exercised by senior managers and ICT specialists. It does not cover the governance to be exercised by the Board of Directors, as envisaged by AS8015 and the ITGI Board Briefing. They mention the Board of Directors only once, when quoting Wim Van Grembergen's definition. They refer to IT Boards or Management Boards only. This confusion in scope shows the need for a standard definition.

The following quotation contains the summary of the thoughts about the definition or description of ICT Governance raised in the discussions by the members of the Study Group during the Moscow meeting.

•*The objective of governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT.*

–*The system in which directors monitor, evaluate and direct IT management to ensure effectiveness, accountability and compliance of IT.*

•*The active distribution of decision-making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviors and results.*

–*who makes directing, controlling and executing decisions*

–*how the decisions will be made*

–*what information is required to make the decisions*

–*what decision-making mechanisms should be required*

–*how exceptions will be handled*

–*how the governance results should be reviewed and improved*

•*The governance framework that results from the ongoing and active distribution of decision rights.*

–*The decision making structures and governance processes for directing and controlling IT within the corporation*

–*The relationship among IT management, the corporation, and other stakeholders as well as the position of IT within the corporation*

•*The governance system for the continual improvement lifecycle of governance including the establishing, monitoring, evaluating and improving of IT governance*

Continually improve the alignment of IT governance with the desired strategic impact of IT

It can be seen that at that moment the Study Group had not finalized a definition. Accordingly, it asked for a paper canvassing various views about ICT Governance that were present in other reports or sources of thought. This paper is given in Annex A. Concepts of IT Governance.

This paper has provided a useful collation of some of the views about what is ICT Governance. It does not make any recommendation about definition. As part, or even most, of the paper draws upon the descriptions by Weill and Ross, so it is limited in its coverage of the scope of ICT Governance. The coverage of the ITGI *Board Briefing*, however, does extend the scope up to the level of interest for the Study Group at the moment. This issue of scope should be considered in resolving the definition of governance.

As well, the IBM Report quoted in the Annex, following the lead of the work that it, in turn draws upon, also adds the consideration of how to establish a governance system more than what the governance system should do. Accordingly, there should be a separation of descriptions and definitions for the function of governance and the formation of governance.

Conclusion

The Working Group should establish a Glossary of governance terms. The Glossary especially should include definitions that help to establish the difference between Governance and Management. The definitions must be compatible with those in existing ISO Standards.

Governance Needs to be Addressed in the Standard

Discussion

Annex B describes the need for and some indications of the value of, an international Standard in ICT Governance.

Conclusion for the Development of the Standard

The Study Group concludes that there is a need for an ICT Governance Standard to address the following organisational issues:

a. Establish the decision rights and accountability framework that "glues" the business components within IT (the various required management capabilities) together and drives the desired behaviour in IT.

b. Ensure that IT functions work together to achieve desired outcomes.

c. Achieve business objectives by ensuring that each element of the mission and strategy are assigned and managed.

d. Define and encourage desirable behaviour in the use of IT and in the execution of IT outsourcing arrangements.

e. Implement and integrate the desired business processes into the organization.

f. Provide stability and overcome the limitations of organizational structure.

g. Improve customer relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework.

h. Promote and achieve desired behaviour

i. Achieve higher value for the customer

Where (in ISO) does ICT Governance belong?

Discussion

Annex C describes the options for locating where a Working Group should be within the JTC1 sub-committee structure.

Conclusion

The Study Group concludes that from the options presented, the most favourable would be for a new IT Governance Working Group to be established in SC7 and to move out to a new Sub Committee within JTC1 as the group grows to a critical mass and establishes a portfolio of governance standards relating to the corporate governance of IT.

Since the interim version of this report was published in 2007, a JTC1 Study Group has been convened to work through this issue and to confirm the market requirements for a standard on the Corporate Governance of ICT.

Related Standards

Discussion

Annex D lists the ISO Standards that are related to governance. They could be considered as References within the set of Standards.

As well, the following resolution made by SC7 at the Plenary in Moscow on 29 May 07 should be noted.

JTC 1/SC 7 instruct its Secretariat to establish a Study Group on the Relationship of Life Cycle Processes and IT Service Management and Governance to investigate two items:

- *Various alternative technical approaches for representing the relationship between life cycle processes and the provision of IT services.*
- *The case for perceiving increased end-user value in a tighter relationship among the standards addressing IT service management, IT governance, and life cycle process definition and assessment.*

Contributions to the study group are invited from national bodies or liaison organizations. Via its membership, the group shall liaise with the following groups: WG 7, WG 10, WG 25 and the study group on IT governance.

The study group shall be chaired by Tony Coletta (Italy). Its membership shall consist of:

Teresa Doran and Anatol Kark (WG 7)

[One of] Alastair Walker or Alec Dorling (WG 10)

Jenny Dugmore and Melanie Cheong (WG 25)

Alison Holt (IT Governance Study Group)

The study group shall submit an interim report by 2007-09-15 for the interim meeting of SC 7 working groups and a final report by 2008-04-15 for the plenary meeting of SC 7. The group is authorized to conduct its work by correspondence, telephone conferencing, web conferencing and meetings.

Conclusion

The Study Group concludes that any work in the area of ICT governance should be carried out in consultation with the groups responsible for overlapping or related areas, to ensure harmonisation from the outset.

Type of Standard

Discussion

Annex E was prepared to consider the options for producing an ISO document if the Fast Track for AS8015 were not successful

Conclusion

Since this Annex was prepared and submitted, the fast track process has completed, and it looks likely that ISO/IEC DIS 29382 will proceed to become a full international standard. The Study Group proposes a series of technical reports to cover related governance issues and, in particular, to provide implementation guidance for organisations.

Further Activities

Discussion

The Study Group thinks that there is a need for several different types of publications that should be produced to support the Standard. It is not enough to produce just a written Standard.

Annex G contains brief descriptions of these types of publications; in print or on the Web. Appendix 1 expands upon the idea of a Technical Report on ICT Governance, showing a possible structure and sketching out its content. Appendix 2 contains a proposal for a Research Framework for ICT Governance that expands upon the "Background Books" described in Annex G.

The main suggestion for future activities is the preparation of supporting Standards. The first other Standard, concerning the governance of IT projects, is being considered in Australia by the Standards Australia IT-030 Committee. Drafts are under view at the moment.

The possible Accreditation Scheme relates to the Maturity Model given in Annex H. Following the precedence set by ISO 20000, the Standard could be supported by an Part 3, providing a basis for assessing the extent of governance in an organization. A possible personal accreditation scheme was mentioned but not taken up in much detail.

The EDIFICE is under construction at www.itee.adfa.edu.au/~ejl/Portal .

Two of the proposed research books proposed in Appendix 2 to Annex G are underway. A publisher has been approached (by Brian Cusack) for the book about national jurisdictions. The workshop for the "Canberra Book", covering the theory and application of IT Governance was held in Canberra on 12 Aug 07. There are currently 20 collaborators in the production of this book, using Google Docs.

It is possible that the Canberra Book, or part of it, become the Technical Report outlined in Appendix 1.

The 'family of documents' described in Annex G is certainly needed. Members of the Study Group have been approached 'back home' for advice or consultancies about IT governance. These documents, often in the form of short, targeted leaflets would help to give this guidance. These documents should be simple to produce and simpler to read.

Conclusion

The Study Group concludes that a Study Group should be set up within the new Working Group to consider the following initiatives:

- Additional Standards, for the other levels of governance or particular roles
- Development of complementary books
- Development of a governance accreditation and certification scheme
- Development of a communications medium such as a web based portal (such as EDIFICE at www.itee.adfa.edu.au/~ejl/Portal), as a means for introducing collaborators in the Standards process to the theories and techniques of IT Governance
- Design and publication of brochures, handbooks, check lists and guidelines
- Development of a glossary of terms
- Development of tools to support the adoption of governance

Conclusion about Research Framework

The Study Group concludes that the major objectives of a research framework are twofold, namely:

- Systematic classification of past and present research on IT governance
- Identification and proposed focus on future research efforts

Conclusion about a Technical Report

The Study Group concludes that the technical report format would be a useful template for the socialisation of related governance topics such as project governance and operational governance, prior to the development of a full international standard..

Need for a Maturity Model

Discussion

Annex G contains a proposal for the development of a maturity Model in ICT Governance.

Conclusion

The Study Group concludes that there is a need for a maturity framework associated with the standard to enable organisations to measure their performance, understand their strengths and identify areas where governance should be improved.

Liaisons

Discussion

Annex H describes the benefits of ISACA becoming a Liaison A organization.

Conclusion

The Study Group concludes that the input from the Liaison A organisations, itSMF and ISACA, has proved extremely useful in providing a representative view across a wide cross section of stakeholders about the market requirement, and the possible adoption and adaptation of IT governance.

National Activity concerning Governance

Discussion

Annex I lists the legislation and other actions that are pertinent to ICT governance in the various national jurisdictions.

Conclusion

The Study Group notes the conditions influencing governance in the different national jurisdictions, and proposes that the new governance Working Group consider these conditions so that Standards and supporting documents are applicable for all nations.

Call to Action

Proposed New Work Item

At the request of the Study Group, Melanie Cheong has prepared a draft New Work Item (NWI). It is given in Annex J.

The details of the NWI will depend upon the results of the comment disposition and resolution at the Montreal meeting in October.

APPENDIX 1 - ORIGINAL STUDY GROUP RESOLUTION

Study Group Initiation – May 2006

The work of the Study Group was established by resolution 924 at the SC7 2006 Bangkok Plenary, as follows:

> "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.

The Study Group shall take into consideration:

- ISO/IEC 16085
- ISO/IEC 20000

And:

- ISO 9000
- ISO 27000
- ISO 14000

And:

- AS 8015 (N3463)
- AS/NZ 4360
- COBIT

There are several organisations that are working in this area that should be investigated for possible liaisons:

- ISACA and ITGI
- TC 207
- itSMFI
- Other interested SCs within JTC1

The study group will make recommendations on changes to existing standards/guidance and/or the creation of new standards or TR. Its membership will consist of:

- Alwyn Smit, South Africa
- Alec Dorling, UK
- Ian Hirst, Australia

- Alison Holt, New Zealand
- David Keech, UK
- Jenny Dugmore, UK
- Melanie Cheong, South Africa
- Beatrix Barafort, Luxembourg
- Jyrki Lahnalahti, Finland
- Marc Tailefer, Canada
- Fred Hoberg, South Africa
- Ed Lewis, Australia
- Craig Pattison, itSMFI
- Darcie Destito, US
- Gargi Keeni, India
- Hiroshi Koizumi, Japan

Additional members can be added until 2006-09-15. Nominations must be sent to the SC7 secretariat.

The study group will be chaired by Alison Holt (New Zealand) and co-chaired by Ed Lewis (Australia) and will submit a report by 2004-04-15. The study group will meet concurrently with WG 25"

Study Group Start Up

A number of governance experts joined the Study Group before the closing date of 15th September, 2006. The first face-to-face meeting was held at the SC7 interim plenary meeting in Seoul in October.

Fast Track of AS 8015:2005

The fast track of AS 8015:2005 was initiated by Resolution 917 at the SC7 2006 Bangkok Plenary, as follows:

> "JTC1/SC7 invites the Australian National Body to submit its national standard AS 8015:2005, (N3463) Corporate Governance of Information and Communication Technology for processing under the fast-track procedures of ISO/IEC JTC1. Comments from the fast track, if any, will be reviewed by the SC7/Study Group on ICT Governance."

AS 8015 was submitted for fast track by Standards Australia in October 2006, and passed the JTC1 30-day review for Fast Track Ballot in January 2007.

ANNEXURES

ANNEX A. CONCEPTS OF IT GOVERNANCE

Sushil Chatterji

Bill Powell

Context

Information Technology Governance, IT Governance or ICT Governance, is a subset of Corporate Governance that is focused on the governance of the use of information technology by the corporation. The rising interest in IT Governance is partly due to compliance initiatives [e.g. Sarbanes-Oxley (USA) and Basel II (Europe)], as well as the acknowledgement that IT decision making can make a significant negative or positive impact on a business.

The objective of ICT Governance is to determine and cause the desired behavior and results to achieve the desired strategic impact of IT. ICT Governance involves the active distribution of decision-making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviors and results.

The governance framework that results from the ongoing and active distribution of decision rights would provide for the continual improvement lifecycle of governance as it applies to ICT, including establishing, monitoring, evaluating and improving of ICT Governance.

Existing Definitions

OECD Corporate Governance Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. (*OECD Code on Corporate Governance*)

World Bank Definition of Corporate Governance Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, the Board of Directors, the controlling shareholders and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.

MIT Sloan Center for Information Systems Research IT Governance is specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT. *(MIT CISR Working Paper No. 326; April 2002).*

AS 8015 – Australian National Standards Corporate Governance of ICT is the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization. *(Corporate Governance of Information and Communication Technology; January 2005).*

ITGI (IT Governance Institute) IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives. *(Board Briefing, 2nd edition; 2003).*

University of Tasmania The survey of the literature by academics from the University of Tasmania (*Webb, Phyl, Pollard, Carol, and Ridley, Gail (2006), Attempting to Define IT Governance: Wisdom or Folly?, Proceedings of the 39th Hawaii International Conference on Systems Sciences*) brings out the 'elements' that are common to a range of suggested definitions. The elements are: strategic alignment, delivery of business values, performance management, risk management, policies and procedures, and control and accountability. Their resultant definition is

> IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management.

It should be noted that there is some overlap between some of these elements (risk management includes performance management, as 'risk analysis') and that alignment should involve sub-elements such as strategic plans and Enterprise Architecture.

Description, Scope and Attributes

Governance includes the active distribution of decision rights and accountabilities. The active distribution of decision-making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviours and results. The desired behaviour and results are determined by the board's view of the strategic impact of IT.

- who makes directing, controlling and executing decisions
- how the decisions will be made
- what information is required to make the decisions
- what decision-making mechanisms should be required
- how exceptions will be handled
- how the governance results should be reviewed and improved

IBM has observed that various approaches to decision rights may be appropriate based on an organization's risk posture and other current business requirements. Different approaches may be required within one organization for different decision types. Different approaches may be required different organizations due to different business objectives. Different approaches may be required at different times due to changing business conditions. Common approaches to decision rights may include establishing decision rights within various decision making structures. *(Ref: IBM Technical Report for ISO Study Group on IT Governance; May 2007)*

It is important to note that the desired behavior and results are determined by the boards' view of the desired strategic impact of IT. Organizations can't just focus on IT as one class of resource – they need to clarify classes of competencies and assets within IT and the unique value each class, For instance in a manufacturing business the desired strategic may be to enable very low cost but reliable production as well as innovative and leading edge design capabilities. Within IT, there are some aspects that are more strategically valuable to those corporate objectives, with other aspects that can be treated as a commodity. This determination of the desired strategic impact of IT should ensure alignment of the corporations need and demand for each IT capability and the delivery approach for that capability.

Governance Framework

The governance framework results from the ongoing and active distribution of decision rights and accountabilities. This framework is a point in time snapshot of decision rights and accountabilities. The framework is complete if each activity required to achieve the desired strategic impact of IT has clearly assigned decision rights and accountabilities, this includes:

The decision making structures and governance processes for directing and controlling IT within the corporation

The relationship among IT management, the corporation, and other stakeholders as well as the position of IT within the corporation

Note:

MIT CISR also has proposed an IT Governance Framework, which simply stated is the harmonization of business objectives, IT governance style and business performance goals. (Ref: MIT CISR Working paper No. 326; April 2002)

IBM describes the IT Governance and Management System Framework as laying the foundation for the IT endeavour within a business, taking into account factors such as vision, values, goals, and overall business objectives. In addition, it establishes the guiding principles (a management philosophy) based on these factors. (Ref: IBM Technical Report for ISO Study Group on IT Governance)

Lifecycle Management of IT Governance

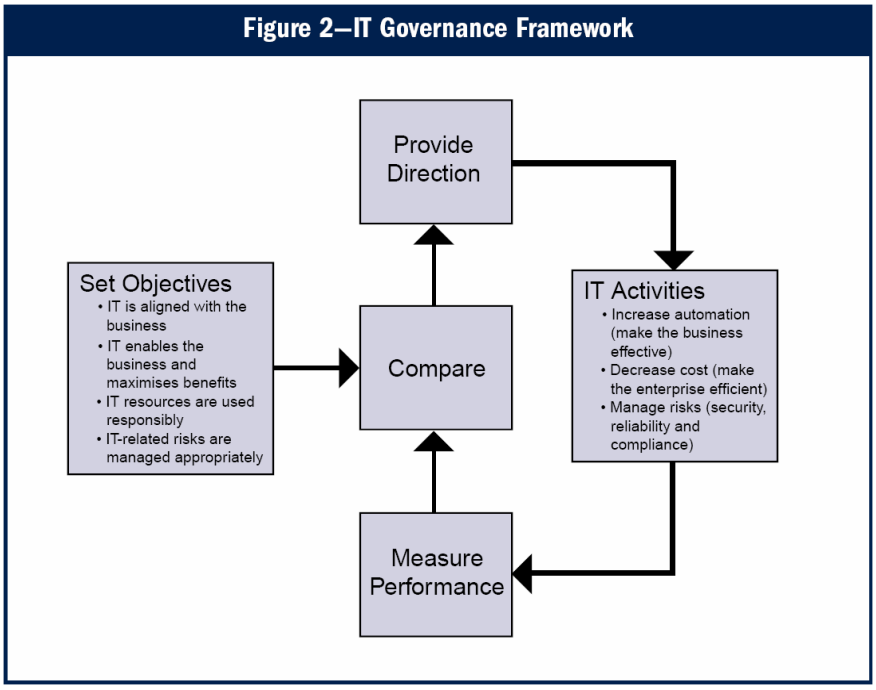
This is the system for the continual improvement lifecycle of governance including the establishing, monitoring, evaluating and improving of IT governance. It is a lifecycle system in which directors ensure the effectiveness, accountability and compliance of

IT management processes and systems. Continually improve the alignment of IT governance with the board's view of the desired strategic impact of IT

The governance process starts with setting objectives with a clear articulation of the desired strategic impact of the various resources and competencies within IT. After that, an initial set of decision rights and accountabilities is established creating the initial governance framework. From then on, a continuous lifecycle is established for measuring performance, comparing to objectives, redirecting decision rights, accountabilities and activities where necessary. Changes of objectives are determined where appropriate. While objectives are primarily the responsibility of the board and performance measures that of management, it is evident they should be developed in concert so that the objectives are achievable and the measures represent the objectives correctly. *(Ref: ITGI Board Briefing, 2nd edition; 2003)*

In response to the direction received, the IT function needs to determine how to meet the objectives and adjust the management system.

Figure 2—IT Governance Framework



The ITGI, in its Board Briefing document, mentions that IT governance is also a continuous life cycle, which can be entered at any point. Usually one starts with the strategy and its alignment throughout the enterprise. Then implementation occurs, delivering the value the strategy promised and addressing the risks that need mitigation. At regular intervals (some recommend continuously) the strategy needs to be monitored and the results measured, reported and acted upon. Generally, on an annual basis, the strategy is re-evaluated and realigned, if needed. It is common that many of these activities may be occurring at the same time to achieve the continual steering that may be required.

This life cycle does not take place in a vacuum. Each enterprise operates in an environment that is influenced by:

- Stakeholder values
- The mission, vision and values of the enterprise
- The community and company ethics and culture
- Applicable laws, regulations and policies
- Industry practices

  (Ref: ITGI Board Briefing, 2nd edition; 2003)

IBM has also expressed that IT Governance as a lifecycle process – it must be planned, designed, implemented, reviewed and improved as a lifecycle. This lifecycle could be described in terms of the Plan, Do, Check, Act lifecycle common in international standards. Common lifecycle activities might include:

- Defining and establishing Governance
- Identifying and handling exceptions
- Learning from exceptions
- Reviewing governance results
- Redefining desired behaviors and improving governance
- Improving the management system that provides the information required for decision making including governance tools, (Models, Dashboards, Standards)

  (Ref: IBM Technical Report for ISO Study Group on IT Governance)

In its latest definition (October 2006) Gartner has defined IT Governance as a series of lifecycle processes. Accordingly, it has outlined a number of these processes for the design, implementation and execution of IT Governance. They describe this lifecycle as:

- *Strategize:* Develop a strategy for governance that will ensure participation on a sustained basis by key participants. Getting the right strategy to do this is critical. Because IT governance's purpose is to ensure that the business meets its goals, it is driven by business strategy. This is to enable an IT governance strategy to be developed that is driven by, and has the goal of, "ensuring the effective and efficient use of IT in enabling an organization to achieve its goals."
- *Plan:* Create a comprehensive plan for the implementation of that strategy. This should not only address the design of the IT governance process steps and support logistics, but also the culture change-management aspects of ensuring that all participants are educated and motivated to make IT governance a success.

- *Implement:* Implement the plan in such a way that the importance of IT governance to the business and to the success key participants is clear and that process responsibilities and accountabilities are understood. CIOs' feedback stating that their major problem with IT governance is a lack of business engagement often reflects the fact that business managers don't understand how IT governance will be executed as a process and what their role and responsibilities in it will be
- *Manage:* Manage and support the ongoing IT governance processes. As with most cross-organizational management processes, IT governance requires a "champion" to promote its value and maintain interest. This could be the CIO or another corporate senior manager, such as the CFO or CEO. Success also requires staff support to handle administrative and logistics issues and to ensure, for instance, that process-step deliverables are appropriately generated and distributed.
- *Monitor:* Monitor the results and effectiveness of IT governance and feedback results to the IT governance strategy and planning cycle to maintain performance. IT governance works best when it is integrated with existing decision-making processes and reflects their style and management culture. Because organizations change constantly, IT governance will require "tweaking" or adjustment to continue to reflect organizational reality.

  (Ref: Gartner Research note G00139986; 16 Oct. 06).

Principles

The Australian National Standard AS 8016 defines six principles for good corporate governance of ICT. The principles are applicable to most organizations. The application of these principles will vary with the size and business operations of organizations.

Principle 1: Establish clearly understood responsibilities for ICT.

Ensure that individuals and groups within the organization understand and accept their responsibilities for ICT.

Principle 2: Plan ICT to best support the organization.

Ensure that ICT plans fit the current and ongoing needs of the organization and that the ICT plans support the corporate plans.

Principle 3: Acquire ICT validly.

Ensure that ICT acquisitions are made for approved reasons in the approved way; on the basis of appropriate and ongoing analysis. Ensure that there is appropriate balance between costs, risks, long term and short term benefits.

Principle 4: Ensure that ICT performs well, whenever required.

Ensure that ICT is fit for its purpose in supporting the organization, is kept responsive to changing business requirements, and provides support to the business at all times when required by the business.

Principle 5: Ensure ICT conforms with formal rules.

Ensure that ICT conforms with all external regulations and complies with all internal policies and practices.

Principle 6: Ensure ICT use respects human factors.

Ensure that ICT meets the current and evolving needs of all the 'people in the process'.

(Ref: AS 8015 - Corporate Governance of Information and Communication Technology; January 2005)

Roles and Responsibilities

The ITGI publication Board Briefing on IT Governance provides a detailed description of the roles and responsibilities of various functions in an organisation with respect to its defined 5 focus areas of IT Governance (value delivery, strategic alignment, risk management, resource management, and performance measurement): Board of Directors, IT Strategy Committee, CEO, Business Executives, CIO, IT Steering Committee, Technology Council, IT Architecture Review Board *(Ref: Appendix E, ITGI Board Briefing, 2nd edition; 2003).*

The ITGI publication also details the function of, as well as roles and responsibilities for the IT Governance Strategy which it advocates, and draws a comparative distinction with the IT Steering Committee *(Ref: Appendix F, ITGI Board Briefing, 2nd edition; 2003).*

Gartner has described broadly in its IT Governance Relationship Model how IT Governance relates to other business and IT management responsibilities, (from the bottom level up).

- The basics of business management are to develop business strategies to achieve business goals and manage the planning and execution required to deliver them. Monitoring and measuring provide feedback to operational and senior business management and to the board (or organizational equivalent) as input to their responsibilities for organizational success.
- Next, IT strategy can inform and be informed by business strategic and operational planning, as the business develops its strategies and refines its plans. IT planning informs and is informed by business planning and directs the IT component of execution.
- There is a senior management responsibility for oversight of operational management activities and a responsibility to inform the board so that it can fulfill its responsibilities to the shareholders or other forms of ownership of the organization.
- IT governance, as practiced today, attempts to interconnect with all the other roles to be informed of organizational goals and plans, provide direction and support to IT-related strategy, planning and execution, and inform senior

business management and the board to support them in discharging their responsibilities.

(Ref: Gartner Research note G00139986; 16 Oct. 06).

Determinants

MIT CISR has studied 24 large multi-unit business firms in U.S. and Europe, showing that firms govern IT very differently depending on a number of factors including: the predominant role for IT, which performance metrics were important, and the degree of deliberate design (rather than no design) of IT governance. Regarding the primary role of IT in the organisation helping to determine IT Governance, firms in the study varied in how they viewed the primary role of IT. In some firms the role of IT is to reduce cost and duplication. In other firms the primary role of IT is to enable future business strategies. These two types of firms varied significantly on the percent of their resources invested in IT, the amount of senior management attention given to IT and the types of performance benefits expected from IT. Firms where IT was viewed as enabling future business strategies invest up to three times more in IT as a percentage of revenues than firms where the major role of IT major role was to cut costs. Concluding from this, the study suggests that firms with different views for the role of IT require different governance approaches. *(Ref: MIT CISR Working paper No. 326; April 2002).*

When considering this aspect of governance, it is important to note that if the desired strategic impact of IT is limited to monolithic value statements like "cut costs", IT will be unable to focus resources in the best interest of the corporation. The corporation must be more specific in its articulation of the desired strategic impact of IT, otherwise IT will under serve some needs and over serve others.

Critical Success Factors

The ITGI, in its Board Briefing Document, describes critical success factors as "conditions, capabilities, competencies, and behaviours not always under one's own control to obtain".

Examples of these CSFs for IT Governance include:

- Sensitivity to the fact that IT is integral to the enterprise and not something to be relegated to a technical function; IT strategy as an integral part of enterprise strategy; and IT Governance as an integral part of enterprise governance.
- Awareness of IT's criticality to the enterprise and ensuing formal acceptance of responsibility by management who engage specialists to assist them
- Management that is goal-focused and has the appropriate information on markets, customers and internal processes
- A business culture that establishes accountability, encourages cross-divisional co-operation and teamwork, promotes continuous process improvement and handles failure well

- Definition of IT governance activities with a clear purpose, and their documentation and implementation, based on enterprise needs; no ambiguous accountabilities
- Ability to work well with partners and suppliers in support of the extended enterprise
- Focus on the enterprise goals, strategic initiatives, the use of technology to enhance the enterprise and on the availability of sufficient resources and capabilities to keep up with the business demands
- Informal channels of communications with management and external auditors to create a culture of openness
- A code of conduct established in co-operation between management and board, which is reviewed for compliance and formally signed off by senior management
- Implementation of a strategic management system that provides visibility to the IT governance issues of IS strategic alignment, value delivery, risk management, resource management and service performance

(Ref: Appendix C, ITGI Board Briefing, 2nd edition; 2003).

IBM has defined that two critical success factors for effective IT Governance are: clarity and transparency. A lack of clarity or transparency in IT Governance and decision-making is an early indicator of potential failure of governance to achieve its desired behaviours and outcomes.

(Ref: IBM Technical Report for ISO Study Group on IT Governance)

Other critical success factors include:

- Common straightforward internal messaging and communication
- Demonstrative, valuable linkage to business requirements
- Pragmatic adoption of an over-arching governance framework

Governance Processes and Management Processes

The governance framework that is established through the active distribution of decision rights and accountabilities should include governance processes. Governance processes are not the management processes described in bodies of knowledge like ITIL, ISO IEC 20000, COBIT Control Objectives, eTOM or other management model frameworks.

For example, IBM has outlined common IT Governance processes as follows:

- Exception and Appeals Processes
- Compliance processes
- Vitality processes

- Communication processes
- Managing the governance framework of decision rights and accountability

  (Ref: IBM Technical Report for ISO Study Group on IT Governance)

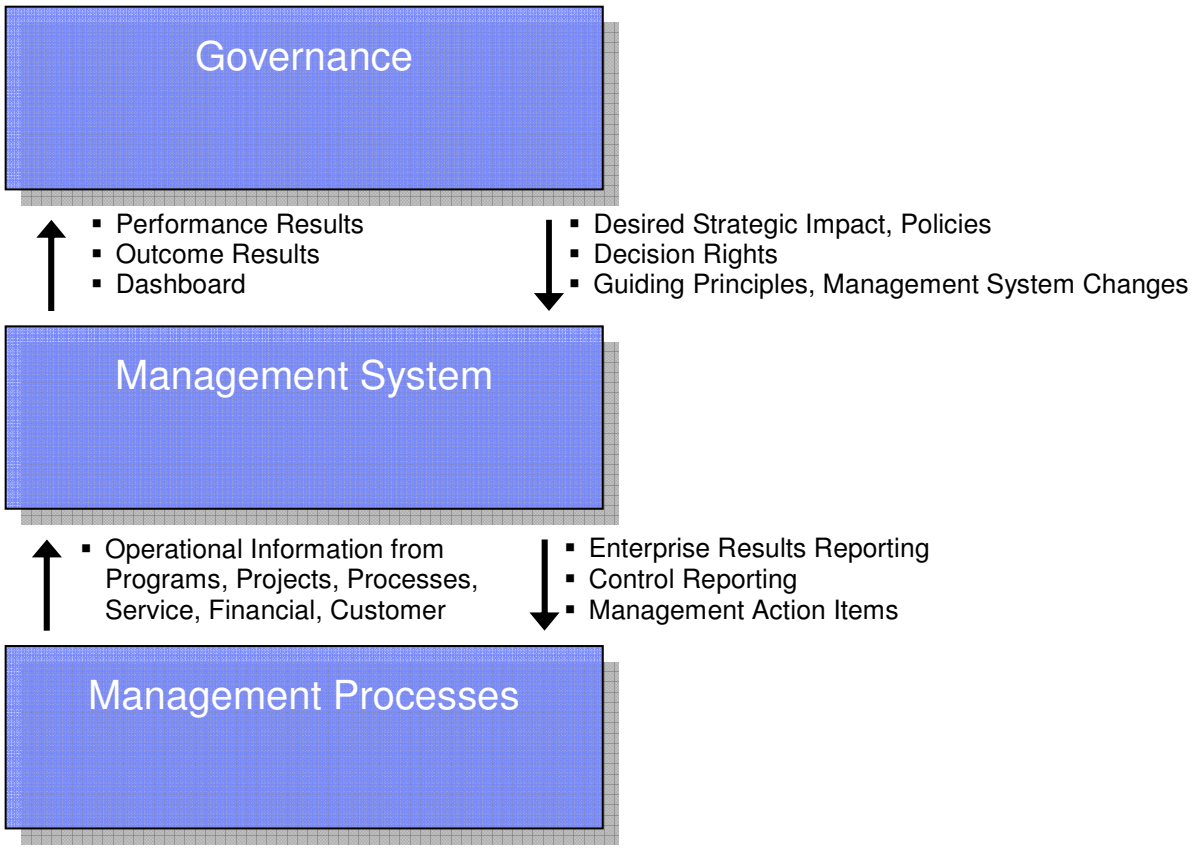
IT governance entails a number of activities for the board and for executive management, such as becoming informed of the role and impact of IT on the enterprise, assigning responsibilities, defining constraints within which to operate, and obtaining assurance.

The activities that are required, as part of governance should be defined as governance processes. These processes should describe how management will be governed.

The IBM Governance Reference Model makes a clear distinction between IT Governance itself and the underlying management system and processes that support it. In the IBM model, the domain of management focuses on the efficient and effective use and supply of a firm's resources and capabilities. Governance faces the dual demand of

j. achieving current business operations and performance objectives and

k. transforming and positioning firm resources for meeting future business challenges. This dual role is what separates governance from management.



Governance framework (General & Fractal)

- Principles and Management Model
- Structures, decision paths, escalation paths - WHO makes WHAT decisions, WHEN, constrained by WHAT policies, rules, and regulations, and based on WHAT data and metrics
- Roles and RACI's within structures
- Processes – decision making, governance evaluation, exception handling
- Measurements and tool requirements
- Establishing "Governance of…"

Management System

- Management Framework
- Performance and outcome measurements
- Monitor, analyze, report,
- Operate controls

Governance relies upon an effective management system to acquire and provide information required for good decision-making, but it is critical to understand that the management system is not governance.

The management system defines, establishes, operates, and improves upon a management framework for conducting IT activities. The management framework will outline, as an example, the management model, guiding principles, methods, organization design, information framework, process structure, policies, and practices to guide the IT organization towards its stated goals. Once the management framework is defined and implemented, a continuous evaluation process should be executed to enable better decision making by executives focusing on whether the business model is succeeding or should be modified to better achieve the objectives.

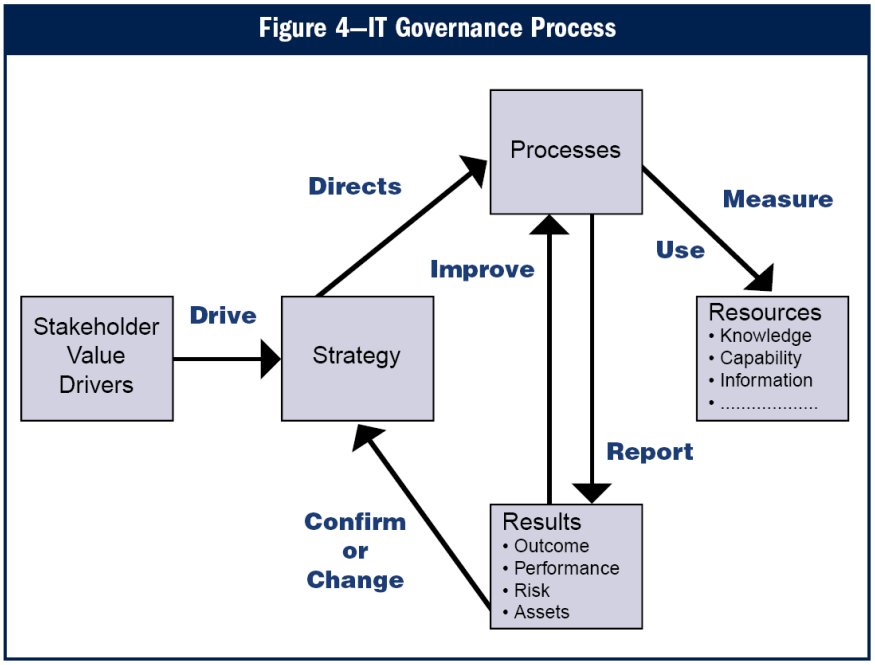
Governance considers and sets the decision rights and accountabilities required to determine the direction the management framework must achieve. Governance is a decision rights and accountability framework for directing, controlling and executing IT endeavours in order to determine and achieve desired behaviours and results.

(Ref: IBM Technical Report for ISO Study Group on IT Governance)

The ITGI has expressed IT Governance also as a process in which "the IT strategy drives the IT management processes", which obtain resources necessary to execute their responsibilities like measuring performance, managing risk and managing the management system itself.

The IT management processes report against these responsibilities on process performance and outcome, risks mitigated and accepted, and resources consumed. Management system reports should confirm either that the strategy is properly executed or provide indications that strategic redirection is required.

The ITGI view of the IT Governance process is depicted in the diagram below:



(Ref: ITGI Board Briefing, 2nd edition; 2003).

Governance Focus Areas/Domains

There are different models depicting the various domains within IT that may all be useful in different contexts. Each provides a different type of "lense" with which to view IT at a high level.

There are different ways to view the "parts" of IT that need to be governed.

- Governance of each IT Competency in IT
- Governance of each business component within IT
- Governance of each process in IT
- Governance of each service provided IT
- Governance of each desired strategic impact offered to the business by IT
- Governance of 5 domains of value

In its Board Briefing, the ITGI has defined and elaborated in detail five primary focus areas of IT Governance. These are:

- *Strategic alignment*, with focus on aligning with the business and collaborative solutions.
- *Value delivery*, concentrating on optimizing expenses and proving the value of IT.
- *Risk management*, addressing the safeguarding of IT assets, disaster recovery and continuity of operations.

- *Resource management,* optimizing knowledge and IT infrastructure.
- *Performance measurement,* tracking project delivery and monitoring IT services.

  (Ref: ITGI Board Briefing, 2nd edition; 2003).

According to the MIT CISR, Effective IT governance requires careful analysis about who makes decisions and how decisions are made in at least four critical domains of IT: principles, infrastructure, architecture, and investment and prioritization. The four domains are highly inter-related but a firm often has different governance archetypes for the different domains.

- *IT principles* are high-level statements about how IT is used in the firm. IT principles capture the essence of a firm's future direction and how IT will be used.
- *IT infrastructure strategies* describe the approach to building the IT foundation for the firm.
- *IT architecture* provides an integrated set of technical choices to guide the organization in satisfying business needs.
- *IT investment and prioritization* covers the whole decision-making process of IT investment.

  (Ref: MIT CISR Working paper No. 326; April 2002).

Outcomes and Benefits

MIT CISR researchers Peter Weill and Jeanne Ross conducted an IT Value study of 256 enterprises over the period of 2001-2003 on the governance patterns of large, complex enterprises leading on specific performance objectives. The study showed that good IT Governance pays off as firms with better than average IT Governance have at least 20% higher return on assets than other firms with the same strategic objectives. Weill and Ross make the argument that IT business value directly result from effective IT Governance.

In an earlier work, Peter Weill and co-author Marianne Broadbent reported on their research on why some firms achieve more business value from IT investments. They summarize their findings into five common characteristics of an IT management culture in these firms:

l. More top management commitment to IT.

m. Less political turbulence.

n. More satisfied users of systems.

o. More integrated business and IT planning.

p. More experience with IT.

(Ref: Weill, P. & Broadbent, M., Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology, Harvard Business School Press 1998;

MIT CISR Research Briefing Vol. III No. 3A; October 2003; Weill, P. & Ross, J., IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press 2004)

In its technical report, IBM outlines 9 common outcomes for IT Governance:

a. Establish the decision rights and accountability framework that "glues" the business components within IT (the various required management capabilities) together and drives the desired behavior in IT.

b. Ensure that IT functions work together to achieve desired outcomes.

c. Achieve business objectives by ensuring that each element of the mission and strategy are assigned and managed.

d. Define and encourage desirable behavior in the use of IT and in the execution of IT outsourcing arrangements.

e. Implement and integrate the desired business processes into the organization.

f. Provide stability and overcome the limitations of organizational structure.

g. Improve customer relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework.

h. Promote and achieve desired behavior

i. Achieve higher value for the customer

ANNEX B. ICT GOVERNANCE NEEDS TO BE ADDRESSED IN THE STANDARD

Bill Powell

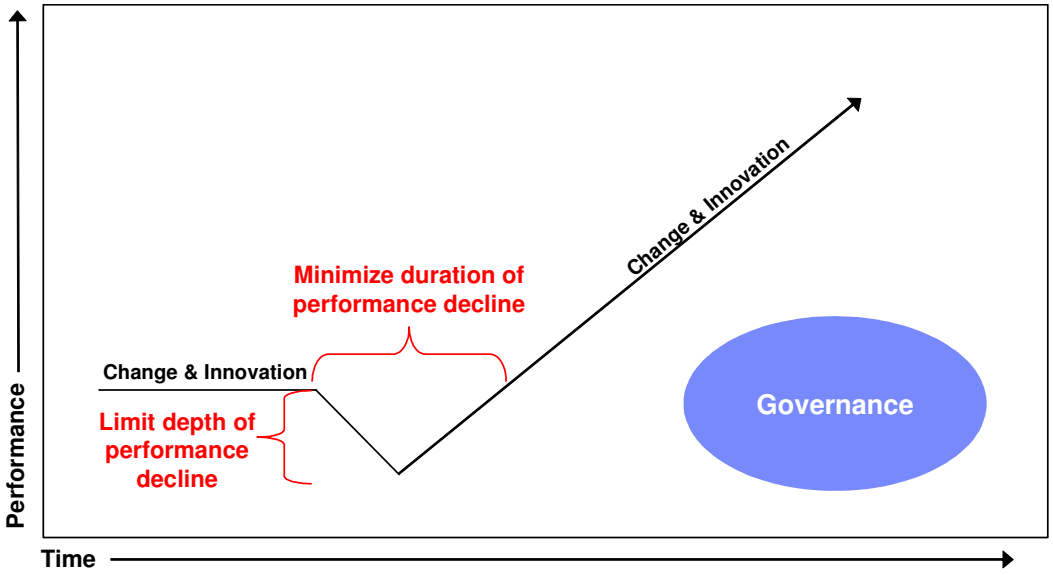
Requirements for a Standard

While there is a value to improved understanding of governance and improved governance itself, it does not follow that an international standard is the right means to deliver that value to the market. The role of the standards body should be to capture the minimum agreed to attributes of governance as accepted universally to enable the market to continue to develop and innovate approaches to governance. Potential value could be achieved if the standard clarified some of the basic attributes of governance.

- 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.

General Benefits of Effective IT Governance

"*The directors of such [public] companies, however, being the managers rather of other*



people's money than of their own, it cannot well be expected that they should watch over it with the same anxious vigilance with which the partners in a private copartnery frequently watch over their own. … Negligence and profusion, therefore, must always prevail, more or less, in the management of the affairs of such a company."
The Wealth of Nations, 1776

If there is a difference with the past, it seems to be in the scale of the financial and economic consequences that have stemmed from the more recent episodes of misconduct.

Governance has always been an integral part of IT management. In additional to regulatory compliance, effective businesses have realized that focusing on technology, organizational structure and even process design itself does not deliver business results. Governance is required to implement the processes into the organization. Achieving business results has always been dependant on effective governance linked to effective and efficient execution.

"*Communicating and supporting IT governance is the single most important IT role of senior leaders.*" IT Governance, Harvard Business School Press

"*Top-tier companies generate returns on their IT investments up to 40% greater than their competitors.*" Weill & Broadbent 1998

"*Investors will pay as much as 28% more for shares of well-governed companies.*"
McKinsey 2002

"*Above-average IT governance had more than 20% higher profits than firms with poor governance.*"
Weill & Ross 2004

Top-performing governance enables IT to realize intended value where others fail, by implementing effective governance to operationalize the strategic intent and to institutionalize good practices.

The unique value of governance is in limiting the depth and duration of performance decline during periods of change and innovation. While management alone may be able to move the organization to a new level of performance or value through effective risk, strategy, planning, development, operational and other management processes, without clear and effective governance, the depth and duration of performance decline may itself damage the organization

---

Beneficiaries of Effective IT Governance

Who benefits from effective IT Governance and a well-conceived governance standard? - All organizations that want specific guidance on governance and approaches to better decision-making - not just corporations and industry groups – will benefit from agreed to standards related to IT governance.

Any organization where the direction and control of IT has a material impact on the business performance and outcomes – for instance – public or private companies, government entities, and not-for-profit organizations, regulatory and compliance organizations.

The beneficiaries of effective IT governance and a well conceived standard for IT Governance include:

- The Business
- Stockholders
- The Board of Directors
- The Chief Financial Officer (CFO)
- The Chief Information Officer (CIO)
- Managing Directors
- Educators
- Management
- Employees
- Customers
- External IT Service Providers and Partners

Benefits to Beneficiaries Effective Governance

The Business - Improved creation and management of business value through effective governance of the IT business component. IT can enable innovation and differentiation

but only if resources are not completely consumed by reactive execution and management.

Stockholders - Stockholders receive benefit by having a transparent decision and accountability framework for achieving business objectives. Transparency in decision making reduces confusion and improves management effectiveness. Improved margins can also result from eliminating redundancy, overlap and lack of clarity.

Potential Investors - Provide clarity for one of the primary leading indicators of future value and corporate potential. Potential investors (financial investment or any other type of investment, like brand equity, partnerships, associations or other relationship types) may develop private approaches to assessing or understanding the quality of governance as way of judging the potential future value of the relationship or investment.

The Board of Directors - The board of directors benefits by understanding the basic attributes of the core elements that should be place to direct and control the strategic impact of the potential value of IT.

The Chief Financial Officer (CFO) - Clarity and transparency over decision-making enables the discovery of bad decisions, ineffective decision makers, analysis of the root causes of ineffective decision-making, and improved clarity for the requirements for the management system that enables effective decision-making by providing information and communicating policies that guide delegated decision-making.

The Chief Information Officer (CIO) - Improved clarity over the job role of the CIO. If the CIO focuses on managing IT, IT will not be governed. Execution of management processes will consume all of the time and increase the risks associated with poor demand side as well as supply side governance. The CIO needs the business to help establish effective IT governance so IT can be directed and controlled.

Managing Directors - Clarity and transparency in decision-making rights and accountability can improve job satisfaction, reduce nepotism by highlighting it, improve longevity and keep directors focused on business value rather than frustration with politics. Improved ability to have the desired direction acted upon by having clearly understood accountability chains

Educators - More complete and valuable curriculum enabling the development of more valuable degreed professionals

Management - Management receives benefit from having clearly assigned roles and responsibilities for executing the strategy and a defined and improvable approach to encouraging desirable behavior. Overlapping or unclear governance results in internal friction, “territorial” strife and inefficient service operations

Employees - Avoids confusion regarding who is responsible for what decisions and how the decisions are made. This results in happier employees focusing their energies on their primary job responsibility. Overlapping or confusing governance can lead to intra company “poaching”, competition, and attrition. Effective governance leads to improved employee satisfaction and retention.

Customers - Effective governance enables the customer to influence the management decisions made by their service providers and therefore service delivery that is responsive

to customer and business needs and concerns. Transparency in governance reduces frustration and enables customers to know how to influence their service providers when they are dissatisfied or have a desire for a change to services.

External IT Service Providers and Partners - Clear direction on the optimum use of and desired strategic impact of IT enabling an effective, efficient and adaptable relationship. Without effective governance, external relationships are typically marked by low value and high "churn" often due to confusion over who is directing and controlling the various aspects of the relationship and the desired value and nature of the relationship itself. These characteristics lead to higher expenses, lower margin and lower returns on investment.

ANNEX C. PLACEMENT OF IT GOVERNANCE WITHIN THE STRUCTURE OF ISO/IEC

Alison Holt

John Graham

This annex investigates the options available for the placement of ICT governance within the structure of ISO and IEC:

Option 1. – Join/Create a group within ISO only

Option 2. – Join/Create a group within IEC only

Option 3. – Join/Create a group within ISO/IEC JTC 1:

a. Remain in SC7 (Software and Systems Engineering Standards)

b. Move to another related Sub Committee (such as SC27)

c. Propose the establishment of a new Sub Committee.

Issues

The audience for standards in the IT Governance area has a different structure to the core Software and Systems Engineering standards of SC7. The typical primary audience of these standards will be senior managers and directors of organisations of all sizes. The typical primary audience of core SC7 standards is typically IT practitioners and consultants. It is however agreed that standards in the IT Governance area will have the core SC7 standards typical audience as a secondary audience.

One of the major consequences of the different primary audience is that it is an audience that will be considering IT Governance as a subset of their primary responsibility, which is Corporate Governance. The predominant defining agency of Corporate Governance, as accepted by the IMF, is the OECD, which defines the detail of Corporate Governance in terms of principles. This is consistent with the IASB and accounting standards. It could also be argued that it is a direct consequence of disturbances to the economic order such as Enron and the reactions of regulators.

The August 2004 issue of The CPA Journal carried a very useful article by Rebecca Toppe Shortridge and Mark Myring – "Defining Principles-Based Accounting Standards". This article encapsulates the advantages of principles based standards in accounting and, particularly, makes a statement that, in an accounting context, "principles-based accounting provides a conceptual basis for accountants to follow instead of a list of detailed views". The important message is the primacy of concepts rather than detailed prescriptions. This is becoming an increasingly important characteristic of the environment that our primary audience is working in.

Another important aspect to consider is the relative importance of "IT" and "Governance" in our work. If we are to regard our work as being primarily within the IT domain we come away with an implication that our work is correctly located in the JTC1 area. If, on the other hand, we regard our work as being primarily in the "Governance" domain then we need to consider the ISO option.

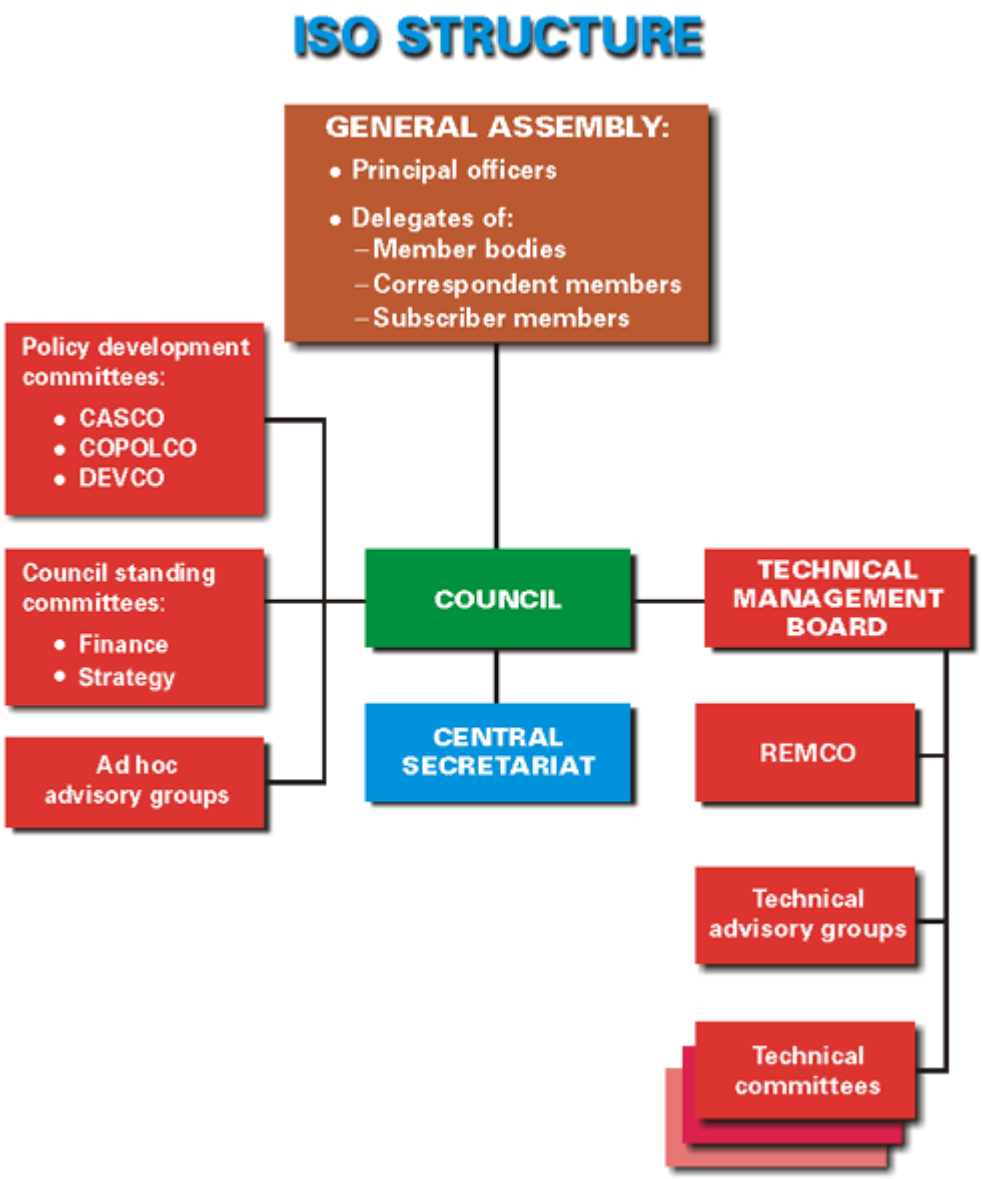
One of the issues with either a new SC in JTC1 or an ISO TC is provision of secretariat services. While this is an issue I am convinced that there is some interest in providing such services.

ISO Option

ISO is the standards organisation with the most general scope. It also shares with IEC a very flexible definition of a standard which is very compatible with principle based standards:

"document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context"

The following table shows the structure of ISO. ISO technical committees cover a vast range of areas however the list is interesting for its omissions rather than its inclusions. There is no Technical Committee covering Governance and Management. If the study group wishes to emphasise Governance rather than IT then this option should be investigated further. A possible title would be Governance and Management of Organisations.



IEC Option

IEC is focussed on a particular set of technologies and emphasises products rather than more abstract ideas such as Governance and Management. The mission and objectives of the IEC are technology centric and would appear to be a poor fit for the Governance of IT.

ISO/IEC JTC1 Option

Options within JTC1

Within JTC1 there are three options for the placement of ICT Governance, as follows:

1. Remain in SC7

2. Move to another existing SC within JTC1 – e.g. SC27
3. Establish a new SC

Option 1 – Remain in SC7

The Study Group is already established within SC7 with:

- Links to other Working Groups within SC7
- Resolutions already set up within SC7 for the establishment of a governance Working Group
- Existing Secretariat structure

The issue of different core audiences is the most compelling reason for moving out of SC7. The intended harmonisation of SC7 standards is also an issue given the likely differences between Governance and Software Engineering standards.

Option 2 – Move across to another existing Sub Committee in JTC1 – e.g. SC 27 or SC 22

Other Sub Committees of JTC1 have made a bid for owning work on an IT governance standard, but their proposals have been rejected, so far.

Option 3 – Propose the establishment of a new Sub Committee

The third option is for the Working Group to be established as part of a new SC within JTC1.

The scope of this new SC could be IT Governance and Management rather than just IT Governance. There are strong arguments for keeping Governance and Management together as the interface between these two ideas is still rather fluid.

A possible scope would be:

To develop standards in the area Governance and Management of IT within organizations.

While this approach may have many difficulties and overheads there is no doubt that they could be overcome with appropriate assistance and support.

ANNEX D. GOVERNANCE IN EXISTING ISO STANDARDS

Hella Shrader

Max Shanahan

ICT Study Group – Summary Report

Remit:

The remit of the sub-group was to review of existing SC7 standards that cover the area of, or have relationship with ICT Governance.

Governance Definition (AS8015)

"The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization."

Governance Definition (UK's "Combined Code of Corporate Governance")

"The Board should at least annually conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance

Standards reviewed:

ISO/IEC 27000 family of standards – Information Security Management System

(incuded are. ISO/IEC 27000, 27002, 27006, 27005, 27004, 27003)

ISO/IEC 17799:2005 – Information Technology – Security techniques – Code of practice for information security management (to be ISO/IEC 27002)

ISO/IEC 9000:2000, Quality management systems Fundamentals and Vocabulary

ISO/IEC 20000 - *Information Technology - Service Management*

ISO/IEC 16085 - Systems and Software Engineering – Life Cycle Processes – Risk Management

ISO/IEC 14000 series - Environmental management systems (No formal review received)

Summary

All reviewed standards have a relationship with ICT Governance and many sections overlap not only in comparison to the AS8015 standard but also amongst the individual reviewed standards. Any drafting of a new international ICT Governance standard needs to take the above existing standards into account and ensure that a) there are no conflicts and b) all governance related sections are covered. A weakness of all reviewed standards is around the need for strategic direction and the implementation of controls to support and manage this area.

Although no formal review was received for ISO 14000, some key points are included in this summary report highlighting the fact that through increased awareness to environmental issues and emerging legislations any new international ICT Governance standard must include control objectives around environmental standards .

Key points:

ISO 27000 - The standard specifies the requirements and processes to enable a business to establish, implement, review and monitor, manage and maintain effective information security. The standard overlaps with ICT governance in the areas of risk management, compliance with legal requirements, management responsibility, internal auditing, business continuity management and performance/capacity management. The 13 control objectives described in the standard all link to ICT Governance.

ISO 17799:2005 (to be ISO/IEC 27002) – The standard gives guidance on how to established guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation. The control objectives meet the requirements identified by a risk assessment. The standard gives more detail to the controls listed in ISO/IEC 27001 that link directly to ICT Governance. The controls objectives in ISO 17799 focus on Security, Information Security Management, Asset Management, Human Resources, Physical & Environmental Security, Communciations & Operations Management, Access Control, IS Acquisition, Development and Maintenance, Incident Management, Business Continuity Management and Compliance.

ISO 9000 series – The standard describes eight quality management principles defined which help improve an organisations performance. These are focused around customers, leadership, involvement of people, process approach, system approach to management, continual improvement, factual approach to decision making and mutually beneficial supplier relationships. Links with ICT Governance exists in the areas of continual improvement, decision making, supplier management, system and process approach.

ISO 20000 - The standard describes the controls needed to effectively deliver services that meet the needs of the customer and business requirements. Overlaps exist with the ISO 27000 and ISO 9000 series especially in the areas of business continuity management, supplier management, performance/capacity management and continual improvement. The processes described in ISO 20000 underpin an effective governance framework and therefore need to be closely aligned to any proposed ICT Governance standard.

ISO 16085 - The standard describes the necessity for continuous risk management within the IT and Communications environments. It provides the framework for implementing a risk management process however does not provide techniques or mechanisms for identifying key risks. The standard focuses on software of system issues and primarily references "project" initiated risks. Overlaps exist with ISO/IEC 27000 series. Any ICT Governance standard needs to be closely aligned with the policy points in ISO/IEC 16085 as the risk management process is vital to understanding key risks and business priorities.

ISO 14000 – The standards describes the controls needed to minimise harmful effects on the environment caused by the company's activities, and to achieve continual improvement of company's environmental performance. It is linked to ICT Governance through the requirement to comply with legislation and regulations. With the heightened focus on "green issues" and "carbon footprints" any international ICT Governance standard must include controls for environmental standards.

ANNEX E. WHAT TYPE OF STANDARD IS REQUIRED?

Alwyn Smit

Introduction

The following documents were considered to determine what type of document would be most suitable for an ICT Governance standard:

- ISO/IEC JTC1 Directives, 5th Edition, Version 2.0, 12 April 2006
- ISO/IEC Directives, Part 2, Rules for the Structure and Drafting of International Standards

ISO/IEC Directives, Part 1 was found not to be applicable in this case as it is superseded in JTC 1 by the JTC 1 Directives.

The options in terms of document types as given by the ISO/IEC JTC1 Directives are summarised in clause 0.

ISO/IEC JTC1 Directives, 5th Edition, Version 2.0, 12 April 2006 - Documentation Types

The options in terms of document types are given by the ISO/IEC JTC1 Directives as:

1. International Standards
   - Normal Processing
   - Fast Track Processing
   - Publicly Available Specification (PAS) Transposition Process
2. Technical Reports
   - Normal Processing
   - Fast Track Processing
3. International Standardised Profiles
4. Amendments
5. Corrigenda

International Standards – Normal Processing

ISO/IEC JTC1 Directives Clause 12.2.1: "The social and economic long-term benefits of an IS should justify the total cost of preparing, adopting and maintaining the standard. The technical consideration should demonstrate that the proposed standard is technically feasible and timely and that it is not likely to be made obsolete quickly by advancing technology or to inhibit the benefits of technology to users."

International Standards – Fast Track Processing

ISO/IEC JTC1 Directives Clause 13.1: "Any P-member of JTC 1 or organisation in Category A liaison with JTC 1 may propose that an existing standard (or amendment with the approval of the responsible SC) from any source be submitted without modification directly for vote as a DIS (or DAM). The criteria for proposing an existing standard for the fast-track procedure is a matter for each proposer to decide."

International Standards – The PAS Transposition Process

ISO/IEC JTC1 Directives Clause 14.1: "A technical specification is called a Publicly Available Specification (PAS) if it meets certain criteria, making it suitable for possible processing as an international standard. These criteria (see clause 4.3) have been established in order to ensure a high level of quality, consensus and proper treatment of Intellectual Property Rights (IPR) related matters."

Comment: PAS is intended to be used for documents that are not the property of national bodies, for example, documents owned by consortia or other organizations. It is intended for documents that are not eligible for fast-track processing.

ISO/IEC JTC1 Directives Clause 14.3: PAS Criteria

"JTC 1 has established criteria that serve as a basis for the judgement as to whether a particular organisation can be recognised and whether its specification can be accepted as a candidate for transposition into an international standard. Such criteria may also be used by potential submitters to determine the level of suitability of their specification for the standardisation process. The PAS criteria are broadly classified into two categories and address the following topics:

- Organisation related criteria:
- Co-operative stance;
- Characteristic of the organisation;
- Intellectual property rights.
- Document related criteria:
- Quality;
- Consensus;
- Alignment.

Details can be found in the Management Guide for the Transposition of Publicly Available Specification which is included as Annex M."

Technical Reports – Normal Processing

ISO/IEC JTC1 Directives Clause 16.1: "The primary duty of JTC 1 is the preparation and review of ISs. The publication of TRs is an exception and should be considered only if the circumstances given in 16.2.1, 16.2.2 or 16.2.3 apply. TRs prepared by JTC 1 are

published as double logo ISO/IEC technical reports by ITTF and copies distributed to NBs.

16.2.1 Type 1 Technical Report

When, despite repeated efforts within JTC 1, the substantial support (or necessary approval, as the case may be) cannot be obtained for submission of an FCD for registration as an FDIS, or for acceptance of a DIS at NB voting stage, JTC 1 may decide to request publication of the document in the form of a TR. The reasons why the required support could not be obtained shall be mentioned in the document.

16.2.2 Type 2 Technical Report

When the subject in question is still under technical development or where for any other reason there is the possibility of an agreement at some time in the future, JTC 1 may decide that the publication of a TR would be more appropriate.

16.2.3 Type 3 Technical Report

When JTC 1 has prepared a document containing information of a different kind from that which is normally published as an IS (for example, a model/framework [note the word "framework" — refer to 00 where this is used as basis for the conclusion], technical requirements and planning information, a testing criteria methodology, factual information obtained from a survey carried out among the NBs, information on work in other international bodies or information on the "state-of-the-art" in relation to standards of NBs on a particular subject), JTC 1 may propose to the ITTF that the information be published as a TR."

Technical Reports – Fast Track Processing

ISO/IEC JTC1 Directives Clause 16.5.1: "Any P-member of JTC 1 or organisation in Category A liaison with JTC 1 may propose that an existing technical report from any source be submitted without modification directly for vote as a DTR of Type 3. The criteria for proposing an existing technical report for the fast-track procedure is a matter for each proposer to decide."

International Standardised Profiles

ISO/IEC JTC1 Directives Clause 17.1: "An ISP (see Form G24) is an internationally agreed-to, harmonised document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions (see ISO/IEC TR 10000-1).

An ISP includes the specification of one or more Profiles. Each Profile is a set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options and parameters of those base standards, necessary for accomplishing a particular function.

Profiles define combinations of base standards for the purpose of:

- Identifying the base standards, together with appropriate classes, subsets, options and parameters, which are necessary to accomplish identified functions for purposes such as interoperability;
- Providing a system of referencing the various uses of base standards which is meaningful to both users and suppliers;
- Providing a means to enhance the availability for procurement of consistent implementations of functionally defined groups of base standards, which are expected to be the major components of real application systems;
- Promoting uniformity in the development of conformance tests for systems that implement the functions associated with the Profiles."

Amendments

ISO/IEC JTC1 Directives Clause 15.5.1: "A published IS may subsequently be modified by the publication of an amendment (see Form G21). If it is decided that an IS is to be amended, either an NP shall be balloted or an appropriate project subdivision shall be added to the programme of work. Approval shall be in accordance with 6.2.1 or 6.2.2 respectively. Amendments are published as separate documents, the edition of the IS affected remaining in print."

ISO/IEC JTC1 Directives Clause 15.5.2: "An amendment is issued to publish a technical addition or change. The procedure for developing and publishing an amendment shall be as described in 12. Processing is the same as for a standard except for the terminology. At Stage 3, the document is called a proposed draft amendment (PDAM) or a final proposed draft amendment (FPDAM). At Stage 4, the document is called a final draft amendment (FDAM)."

Corrigenda

ISO/IEC JTC1 Directives Clause 15.4.5: Defect Reports – Submission:

"A defect report may be submitted by an NB, an organisation in liaison, a member of the editor's group for the subject document, or a WG of the SC responsible for the document.

The submitter shall complete part 2 of the defect report form (see Form G5) and shall send the form to the Convener or Secretariat of the WG with which the relevant editor's group is associated."

ISO/IEC JTC1 Directives Clause 15.4.9.4.1: "If the response to a defect report has resulted in correction of a technical defect, it shall be processed as a technical corrigendum. The WG Convener or Secretariat shall forward the defect report, response and draft technical corrigendum to the SC Secretariat, requesting a letter ballot on the draft technical corrigendum by the SC (see Form G19). In the case where maintenance of a standard is not assigned to a specific SC but to a National Body or a JTC 1 Category A Liaison body, the actions placed on an SC Secretariat by this clause shall be taken to refer to the Secretariat responsible for the maintenance of that standard."

Conclusions and Recommendations

Conclusions

From clause 0 International Standards – Normal Processing: **An IS will be a definite possibility for an ICT GOV standard**.

From clause 0 International Standards – Fast Track Processing: This is the process followed with AS 8015, because it is owned by a national body – Standards Australia. **Obviously a possibility for ICT GOV**.

From clause 0 International Standards – The PAS Transposition Process: PAS is intended to be used for documents that are not the property of national bodies, for example, documents owned by consortia or other organizations. It is intended for documents that are not eligible for fast-track processing. Unless such documents are identified, this is not an option. **Could be considered for ICT GOV**

From clause 0 Technical Reports – Normal Processing:

Type 1: To be considered only if IS route does not succeed. **Possible but not preferable.**

Type 2: Only to be used if ICT GOV is considered to be a subject still under "technical development". Type 2 TR is very useful for publishing a "trial use" standard. You can publish it, promote it, get users to provide feedback, incorporate the feedback, and then publish an IS. That's what was done with IS 15504, process assessment. **This is definitely an option**.

Type 3: Perhaps to be used for information on the "state of the art" of available standards on ICT GOV. Information other than what is normally published in an IS. **A type 3 TR might be applicable in this case.**

From clause 0 Technical Reports – Fast Track Processing: Fast track version of Technical Reports

From clause 0 International Standardised Profiles: To be used only if we have a group of base standards from which we can select options and parameters for an ICT Governace function. This is really only applicable to a Type 3 TR. **N/A for ICT GOV**.

From clause 0 Amendments: **N/A for ICT GOV** – we are not doing an amendment.

From clause 0 Corrigenda: **N/A for ICT GOV** – we are not doing a defect report.

Recommendations

The recommended document type for an ICT Governance standard will thus be decided by the level of "maturity" of the content and may be any of the following:

- Option 1: The **PAS Transposition process** or **International Standards – Fast Track Process** if we can find suitable documents. I suggest the ICT GOV Study Group do a search of possible available specifications (if it has not already been done).

- Option 2: A **TR Type 2** if ICT GOV is considered to be a subject still under "technical development". **Then later an IS** once the subject has matured.
- Option 3: An **IS** if the subject meets the criteria for an IS.
- Option 4: A **TR Type 3** to adopt interesting documents that are not yet ready for international standardization because they are unsuitable or because they have a problematic fit with existing standards. (The AS 8015 standard calls itself a "framework" in its preface. Although it uses the word "conformance", it means conformance to laws and such. It contains no conformance requirements of its own. A type 3 TR might be the perfect niche for this document and might be a satisfactory way of initially adopting it despite its problematic fit with other SC7 standards.)

ANNEX F. BEYOND AS 8015: WHAT NEEDS TO BE ADDED TO THE STANDARD?

Edward Lewis

As part of the Study Group's deliberations, there is a need to consider what would or could be done to further good corporate governance of ICT beyond the adoption of AS8015 as an international standard.

A sub-set of the membership of the Study Group considered some initiatives that could be taken up to extend the range and reach of governance standards. These initiatives are given below.

Standards

One of the first steps in going beyond 8015 is to rewrite 8015. The contents needs to be changed to reflect the comments received through the voting process. As well, we should take the opportunity to tidy up some of the wording, especially in Table 1.

AS8016 *Corporate Governance of Business Projects involving ICT investment* is still being prepared by Standards Australia. Once produced, it could become the basis for another ISO Standard (perhaps not fast tracked, however).

A standard that has been considered but not taken further is the *Corporate Governance of the Use of ICT*. This Standard would cover the development of policies governing how end-users work with ICT.

Background Books

There are two books that could be produced to provide a background the deliberations about good ICT governance. They could serve as an introduction to the relevant literature, a exposition of the arguments about philosophy or practice that colour the deliberations, and a collection of information about what should be taken into account when forming standards in this area.

The first book could be about similarities and differences in the national jurisdictions concerning governance. It could consist of a series of chapters, one for each jurisdiction, describing legislative environment and other drivers for governance, extent of use of governance mechanisms (standards etc), and issues concerning implementation of better governance practices.

The second book could present the background to the discussions about principles and practice of good governance. It could contain chapters covering the theory underlying the principles of governance, links to related disciplines, and lessons learnt from case studies. It could also contain the discussions, drawing upon the literature as well as experience, of the theory and good practice for preparing the essential documents of

governance – strategic plans, policy statements, business cases, and enterprise architecture.

Accreditation Schemes

There are two possible accreditation schemes for determining whether sound governance of ICT is in place in an organization. The first approach is the obvious accreditation of the organization's practices, as in ISO 9000. The second approach is to accredit the assessors of governance, as in the ISACA Certified IS Auditor scheme.

The first approach could be undertaken in the same way as CMMI. That is, an approved (as in the second approach) assessor uses an established checklist or set of indicators to determine the extent to which the organization follows sound practices in a variety of areas. Of course, these practices should be derived from the principles given in AS 8015. The work by Infonomics P/L (www.infonomics.com.au) is an example of how governance practices could be diagnosed to show where there are shortfalls in the practices.

This approach depends upon the existence of authorized/ accredited/ certified people who could carry out the accreditation of organizations or could provide trusted advice about governance of ICT. The question then is, "who accredits the accreditors"? There is a need for a professional body or society, accepted by others, who could establish an accreditation arrangement. This body then could establish the training and examination processes that are necessary to establish the competence of these governance advisors.

Perhaps a national Standards body could help to form this body? It then could recruit officers and members of the body based upon the recommendations of people that it accepts as having some expertise in the area.

EDIFICE

There are Web-based Portals that have been built to provide information to people interested in a standards topic. Examples include the Risk Management portal that was once provided by Standards Australia. There are Portals established by the formal bodies such as the Treasury Board of Canada (www.tbs-sct.gc.ca/rm-gr/site/home-accueil.aspx?Language=EN&id=021) that show pointers to useful information can be assembled and made more readily available to others as a public service. Such a Portal could be established to support ICT Governance.

A Portal might not be enough. Just as an edifice is an imposing building that includes portals, so an EDIFICE (Ed's Interface For Information, Communication, and Education) contains a traditional Portal but also includes 'learning paths' that suggest pages to read or sites to visit to those who wish to learn more about the tools and techniques in a discipline. An example of an EDIFICE for Planning is given at www.itee.adfa.edu.au/~ejl/Portal.

Additional Documents

There have been a number of suggestions about documents that should illuminate the process and principles of ICT governance. Some of these documents are already listed in the 'family' that the Australian IT-030 Committee has been developing since 2004. The members of the Study Group have proposed other documents.

In general, it is suggested that these documents still be aimed primarily at Board members and their immediate 'reports', including Chief officers. Accordingly, they need to be short (five to ten pages), in simple language, and in large format.

Brochures

Brochures are summaries of other documents. They point to further information or advice.

Possible brochures include:

Executive Summary of Handbook 280: 2006 How Boards and Senior Managers Have Governed ICT Projects to Succeed (or Fail).

This Handbook was written by Raymond Young of IT-030. It has been intended for some time to produce its Executive Summary as a separate brochure for Directors.

Checklist for Corporate Governance of ICT

The brochure will list 20 questions that Directors can ask to evaluate whether their organization is following the principles of AS 8015. These questions have been used in several reviews of governance in Government agencies. (It is possible that they will be included as an Annexure in the next version of that Standard.)

Handbooks

Handbooks provide detailed descriptions of procedures or techniques. They can introduce arguments or debates about terminology or philosophy where they set the context for the procedures.

Guidelines for use of Principles by Small to Medium Enterprises

This Handbook will give tasks and responsibilities for putting the principles of governance into practice in small to medium enterprises. In effect, it will give the 'next steps' that sole traders or small firms should take as they move through the process of governance.

Guidelines for use of Principles by Corporate Enterprises

This Handbook will give tasks and responsibilities for putting the principles of governance into practice in larger commercial enterprises. In effect, it will give the 'next steps' that senior managers should take to move through the process of governance to the satisfaction of the Board.

Guidelines for use of Principles by Public Sector Enterprises

This Handbook will give tasks and responsibilities for putting the principles of governance into practice in Government agencies (corporations or Departments). In effect, it will give the 'next steps' that senior managers should take to move through the process of governance to the satisfaction of the Board.

Procedural Implications of Principles

The Procedural Implication Handbooks will describe how Directors or senior business managers should check that they are being supported in their governance through a series of fundamental procedures. Examples of these procedures, perhaps with their own Handbooks, are:

- Acquisition
- Strategic planning
- Policies
- Service management

Implications of Principles for Different Roles

The Role Implication Handbooks will describe how different officers in an organization can support the Board. Examples of these roles, perhaps with their own Handbooks, are:

- Board members/ CEOs
- CIOs
- Enterprise Architects
- Chairpersons of Steering Committees for Programmes
- Security managers
- Service managers
- Project managers

Toolboxes

Toolboxes will provide brief guides about techniques that can be used by some of the roles to ensure that the principles will be met. Examples of such techniques include:

- General planning process
- Control of systems
- Coupling in design of enterprise resources

Glossary of Terms

There is a need for a Glossary of Terms concerning ICT governance. IT-030 intends to publish such a Glossary. It would include an ontology as well as a dictionary and

thesaurus. It should include some of the discussions of concepts that have led to different usage of terms, such as 'governance' vs 'management'.

Checklists

There is a need for simple checklists that Directors can use to evaluate the proposals put to them by their advisers. Examples of such checklists include:

- Preparing Business Cases (perhaps using the *Business Case Review* produced by the Australian Government Information Management Office, AGIMO)
- Preparing strategic plans
- Enterprise Architecture

Research Findings

There is a need for research to be carried out into several aspects of governance. Through the use of case studies, surveys, and meta-analyses of published studies, it is necessary to answer such questions as:

Does the corporate governance of ICT make a difference to the success of an enterprise?

Can Enterprise Architecture really be used to align ICT resources to business objectives?

This research needs sponsorship. The findings should be made widely available rather than just published in academic journals.

Other moves

Other initiatives that could be used to further the cause include:

Forming a professional body contributing to existing bodies, such as ISACA (see Accreditation above)

Hosting or contributing to academic or professional conferences

APPENDIX 1 TO ANNEX F. PROPOSAL FOR A TECHNICAL REPORT ON ICT GOVERNANCE

Dennis Ravenelle

The following is a proposed Technical Report (Type 2) concerning ICT Governance.

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote. In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR xxxxx, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information and Communication Technology (ICT) Governance Study Group*.

Introduction

The purpose of this Technical Report is …

It is oriented toward a variety of audiences …

It is applicable to … [public, private, for-profit and not-for-profit, and governmental entities and institutions of any size.]

In June, a ballot was cast to accept or not accept the Australian National Standard 8015 for ICT Governance as a Fast Track ISO/IEC Standard on ICT Governance. The outcome of that ballot …

IT governance and associated issues have been reported as a top 10 CIO management problem area in the Gartner EXP annual CIO survey for at least the past five years.[1] Gartner's report goes on to say:

> *Many definitions and explanations of IT governance exist in the industry, press and academia, but they tend to reflect the perspective of the observer and not necessarily the practical needs of practitioners, in particular the CIO.*

Ultimately, at the highest level the goal of good governance is:

- Oversight of management:

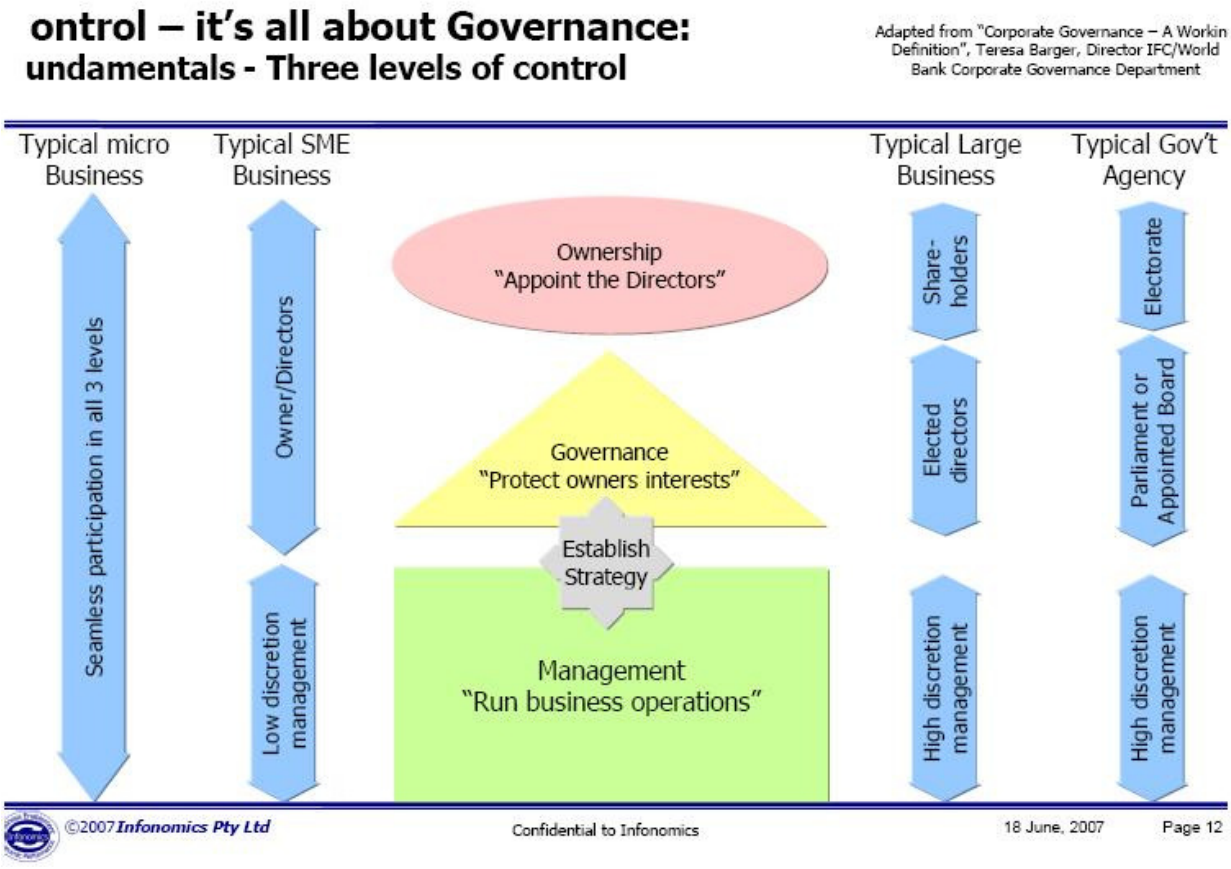
---

[1] Gartner Research, "Defining IT Governance: Roles and Relationships," ID Number G00139986, October 16, 2006

- The Right People
- Doing the Right Things
- For the Right Reasons
- In the Right Way
- To get the Right Results.[2]

With contributions drawn from numerous resources, this Technical Report offers both basic guidance on what constitutes good governance and essential components of the processes, frameworks and metrics that demonstrate that an organization is subject to it.

1.1 Boundaries of ICT Governance



[2] Mark J. Toomey, Managing Director, Infonomics Pty. Ltd., "Corporate Governance of Information and Communication Technology: A business Usage Perspective," Presentation to ISO/IEC JTC1 ICT Governance Study Group, May 22, 2007

Annex A – Related Standards

ISO/IEC 12182 – Vocabulary

ISO/IEC 15026 – Risk & Integrity

ISO/IEC 16085 – Risk & Integrity

Annex B – Related Resources

Organization for Economic Co-operation and Development:

http://www.oecd.org/

OCEG Foundation:

http://www.oceg.org/landing/Foundation.aspx

IT Governance Institute (part of ISACA)

http://www.itgi.org/

APPENDIX 2 TO ANNEX F. PROPOSAL FOR A RESEARCH FRAMEWORK FOR ICT GOVERNANCE

Brian Cusack

K.T. Hwang

A Research Framework

The major objectives of a research framework are two-fold. One is to systematically classify the past and present research on IT governance. Second is to identify and propose the areas that need our future research efforts.

Proposed Research Outputs

A. It is proposed that several books can enhance the literature available in the area of ICT Governance:

a. One is to concern the variations within the different jurisdictions. This edited book is to be archival and to consider the jurisdiction regulatory environments, standards adoption, ITG standard impact, and variations of interpretation, linguistic turn, and so on. The process will be to invite by recommendation a representative group of qualified persons to write one factual chapter each of approximately 6 - 8,000 words. A template shall be available and a publisher is ready.

b. A second book was proposed to communicate to a more general audience the intention and advantage of ICT Governance, its Standard and implementation opportunities. A work Day in Canberra on August 12 is proposed.

c. Another set of books can concern the practitioner and the implementer. These books have been discussed and are to be followed up once the direction and timelines for the new ICT standard are finalised.

B. It is proposed to build knowledge regarding two pressing issues in the standards life-cycle. One is concerned with the adoption of a Standard, and the other with the value of a Standard.

It was proposed that two independent models are tested with a questionnaire survey cycle, and then presented in the initial report as structural (& metric) models. Further research can then follow using other approaches and generic inquiry.

ANNEX G. A MATURITY FRAMEWORK FOR ICT GOVERNANCE

Mark Toomey

Christophe Feltus

Introduction

It is reasonable to expect that organisations using a standard to guide their approach to governance of ICT would wish to measure their performance, understand their strengths and identify areas where their governance should be improved. Stakeholders in organisations, such as investors and business partners, may also find value in an accurate, effective way of assessing the organisation's performance.

The question of measurement

The crucial question in regard to measuring ICT Governance performance is: "What does one measure". Two supplementary questions follow: "How does one measure?"; and "What constitutes a good result?".

Many methodologies for assessment and improvement focus on process. Process is readily identified and modelled, and weakness in process can be identified and resolved. In many organisations, improvement in process has resulted in demonstrably improved performance. In terms of ICT Supply, a widely known and highly credentialed approach to process improvement is CMMI, developed and controlled by the Software Engineering Institute at Carnegie Mellon University. Six Sigma and ISO9000:2000 are further examples of widely used and frequently successful methodologies for improving process performance. One application of the ISACA/ITGI-owned CoBiT framework is for assessment of processes used in management of IT.

However, highly developed process models do not necessarily mean that organisations are successful with ICT. Effectiveness of ICT governance in terms of business performance correlates strongly to the proportion of the organisation's management that can accurately describe how ICT governance works (Weill & Ross, 2004) – pointing not only to the efficacy of the process model but also to the need for proper management engagement. The Australian Customs Service claimed to have exemplary governance, but its Cargo Management Re-engineering project caused massive disruption when it was installed on 12 October 2005 (Australian National Audit Office, 2006). Young asserts that the engagement of senior management is a critical factor in the success of ICT investments (Young, 2006). KPMG found that while many organisations have well-developed processes for preparing investment business cases, few follow through to confirm that intended benefits are actually fully delivered (KPMG, 2005).

All of these illustrations suggest that assessing an organisation's IT Governance needs to address behaviour of the organisation and its personnel, as well as its processes.

A third possible dimension for assessment is performance. One might expect that a sustained high performance (in the use of ICT) is reflective of an effective system of governance. Weil makes a strong connection between corporate performance and effective IT Governance (Weill & Ross, 2004), by saying that good IT governance can result in substantially higher corporate performance. However, it does not necessarily follow that high corporate performance is indicative of good IT Governance. On the other hand, poor control of IT can result in severe damage to corporate performance, as was the case with Australian Pharmaceutical Industries (Toomey, 2006). The experience of Coles Ltd in its efforts to arrange a corporate takeover demonstrate that poor governance of IT can also lead to diminished corporate value (Jury, 2007).

Performance of projects (investments IT to increase business capability and capacity) is only one of two critical dimensions for measuring the effectiveness of IT Governance. Sustained operational performance and the capability to accommodate ongoing business demand is also vital. There is no assurance that organisations which get projects right also get operational controls right – though anecdotal experience is that many larger organisations have moderately good operational stability while regularly experiencing problems with projects.

AS8015 as a measurement framework

IT Governance requires a structured framework of planning, policies, structure and processes (Doughty & Grieco, 2005). But, Doughty and Grieco go on to say: "Corporate governance is not just about rules and regulations. Fundamentally, it is about corporate culture and the way the company conducts its business in an ethical, responsible way". The emphasise that poor culture will overcome the best efforts in planning and control.

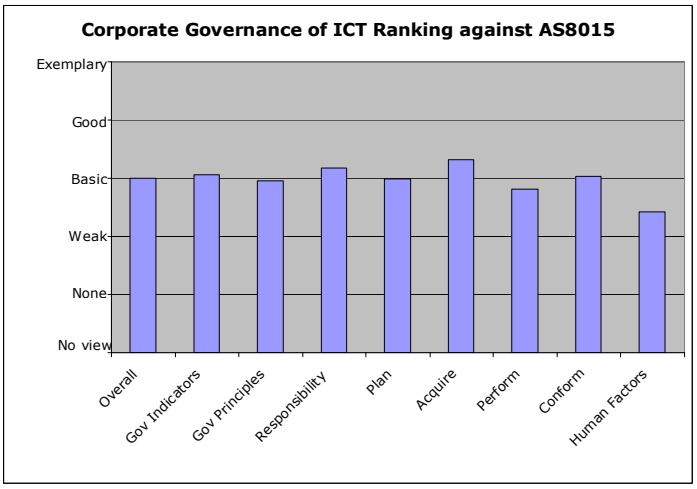
As a principles-based standard, AS8015 specifically addresses behaviour, or culture of the organisation. While not prescribing any specific process model, its emphasis on appropriate behaviour effectively demands that organisations establish appropriate processes, structures and controls that enable and encourage appropriate behaviour at individual and corporate levels.

Since its publication in January 2005, Infonomics has used AS8015 as the basis for formal, structured assessments of IT Governance in a variety of organisations, ranging from medium tertiary institutions to multi-national listed companies. The Infonomics proprietary assessment tool is derived from the standard, and uses a set of 84 assertions regarding behaviours, practices and characteristics that would be expected in an organisation that has good governance of ICT. It is structured as a set of 12 general indicators, followed by 12 specific assertions for each of the six principles defined in AS8015. The tool has proven remarkably effective in demonstrating to top management and boards of directors the root cause of problems with ICT. All of the organisations that have undertaken comprehensive assessments have identified significant scope for improvement.

Abbreviated versions of the Infonomics assessment tool have been used since early 2005 to profile the IT Governance performance of dozens of organisations which have participated in briefings on AS8015. These point to a generally low performance across

organisations in all sectors, and are consistent with the results of the comprehensive assessments. A recent research project undertaken with RMIT University uses a 34 point version of the framework to survey twenty organisations. The following is an excerpt from the survey report:

> *The survey indicates that Australian organisations are substantially dependent on IT for their day to day operations, and that achieving strategic intent also depends on success with IT. However, the systems of governance are basic, and not likely to prevent failures. Directors do have a view on the effectiveness and operation of their organisation's IT Governance, but they are less positive in their views than their Chief Executives. While they see IT as important, the engagement models for involving directors in IT Governance vary considerably. Some directors are concerned that they do not have the required experience and knowledge of IT to be effective in this capacity. They place a great deal of reliance on management.*



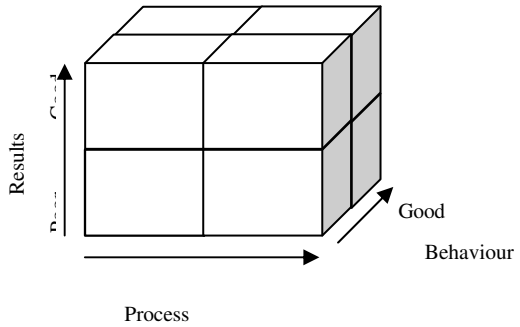
> *Considerable scope exists for organisations to deliver more value from investing in IT and for using IT in business innovation. These improvements, along with better business alignment of IT, better allocation of resources and more demonstrated capacity to successfully deploy new initiatives should correspond to development of more effective systems of governance, in which all managers understand and perform their appropriate roles in relation to the use of IT. Within the system of governance, particular attention should be given to establishment of clearly understood responsibility, to planning IT use to best support the organisation, being more deliberate and precise in deciding to invest in IT, ensuring that IT performs well whenever required, ensuring that IT conforms with formal rules and, most particularly, ensuring that human factors, including communication, engagement, training and support are properly considered.*
>
> *Improving IT Governance should begin with a proper understanding of the role of IT in the organisations business. It should clearly establish the role of the board, and the directors should establish the overall tone of the governance system by emphasising its goals.*

The purpose of this excerpt is to illustrate the way in which AS8015's principles based approach to standardisation can be used to assess an organisation's ICT Governance.

A Prospective Measurement Model

In the discussion above, three potential dimensions for measurement or assessment were identified: process, behaviour and results. Although not rigorously developed as such, the Infonomics assessment model combines elements of these three dimensions.

It would seem appropriate that further effort to develop a measurement model for IT Governance should address the three dimensions. The model represented below proposes a capability/maturity framework in which an organisation's ICT Governance effectiveness can be plotted and compared with other organisations.



The model provides for eight major categorisations of an organisation's IT Governance performance, and offers a basis for "labelling" competence. Tentatively, these could be referred to as:

Process	**Behaviour**	**Results**	**Label**
Poor (1)	Poor (1)	Poor (1)	Incompetent
Poor (1)	Poor (1)	Good (2)	Lucky
Poor (1)	Good (2)	Poor (1)	Process-impaired
Poor (1)	Good (2)	Good (2)	Driven
Good (2)	Poor (1)	Poor (1)	Behaviour-impaired
Good (2)	Poor (1)	Good (2)	Regimented
Good (2)	Good (2)	Poor (1)	(TBD)
Good (2)	Good (2)	Good (2)	Exemplary

Of course, a developed approach to measurement would provide finer granularity in each dimension, and would probably result in expressions of competence that reflect the three dimensions individually. Results of an assessment would ideally include discussion of what is required to improve process and behaviour, and would reflect how these changes should influence performance.

Development of a formal measurement model will require significant effort, to identify factors that can be readily assessed and consistently scored, in order to generate a

meaningful, comparable result, regardless of the scale and orientation of the organisation being assessed. It is entirely legitimate for both small and large organisations to score "good" in all three dimensions, although they will almost certainly have greatly differing process models.

Although process is in many ways the easiest thing to assess, because it is generally formalised, it is in fact the element that is likely to create the greatest complexity in any attempt to develop the full assessment model. This is because the process designs, and even the existence of process, will vary considerably from organisation to organisation. The thinking behind CMMI should be a useful guide in this area – with the focus being on the characteristics of process rather than on the exact detail of the process itself. The questions should look at whether the necessary processes are in place, and with the appropriate level of formality and rigour, rather than demanding any particular model.

An Interim Measurement Model

Development of a rigorous, formal model for measurement of ICT governance performance will take some time, will depend on the final form of the international standard, and will be subject to evolution. Many stakeholders will seek earlier access to a useful tool for assessing organisation's conformance to the standard and identifying the areas in which improvement is needed. Demand for such resources may be driven by increasing regulatory demands for evidence of effective controls and by developing recognition in organisations of the opportunity, and need, for improved performance in the use of ICT.

As has been the case with the Infonomics assessment tool in Australia, it is likely that an effective interim measurement tool could be established through creation of a set of assertions that describe the desirable characteristics of organisations that conform to the intent and instruction in the ISO standard. The standard would provide a framework in which the characteristics would be defined. It is likely that the characteristics would describe controls, behaviours and results, without going into specifics of processes.

To accommodate perceptions of variability between organisations of different orientation and scale, national and industry regulation environments, and any other areas of difference, the defined characteristics could be structured into subsets, so that the relevant characteristics for any organisation could be selected from the total. Care would be needed in this scenario to ensure that the selection was not oriented to obscuring important aspects of assessment in an organisation.

ANNEX H. REVIEW OF THE BENEFITS OF THE STUDY GROUP LIAISON RELATIONSHIPS

Max Shanahan

Dennis Ravenelle

Craig Pattison

ISACA

ISACA/ITGI will work within the SC7 community in a number of working groups to contribute their expertise in regard to business control, performance indicators and capability assessment. ISACA/ITGI will also utilize its strong research base to assist by commenting on other standards as appropriate. ISACA will seek avenues to assist in promoting standards through its Journal, Conferences and training in all regions.

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 (Val IT 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.

ISACA/ITGI will have a representation with the following workgroups:

Table 1 ISACA Liaison A

Group	Description of ISACA Contribution
Study Group on ICT governance (and proposed Working Group for this)	Contribute ISACA/ITGI expertise in the area of Governance of IT.
WG 25.	Contribute to the development and implementation of a process maturity model and the use of performance indicators. Work to harmonise and map ISO /IEC 20000, ITIL and COBIT.
WG 10	Participate on the invitation of WG10 in the work of proposed Ad-Hoc Group to investigate the parameters and issues that impact on the future evolution of the ISO/IEC 15504 set of

Group	Description of ISACA Contribution
	Standards.
WG 21.	Contribute to the development of process maturity model and key performance indicators for Software Asset Management. Examine options for market research regarding ISO/IEC 19770 though ISACA membership base.

ISACA/ITGI will monitor and seek to contribute as appropriate to the following groups:

2. WG 24 Software Life Cycles for Very Small Enterprises
3. WG 7 Development of standards and technical reports on Life Cycle Management.
4. WG 2 Development of standards for the documentation of software and systems.
5. WG 22 Software and Systems Engineering Consolidated Vocabulary.
6. WG 23 Systems Quality Management.
7. WG 42 Architecture
8. WG 6 Development of standards and technical reports for software products evaluation and metrics for software products & processes.
9. Ad hoc group on test management
10. Study Group on Software and Systems Benchmarking and Measurement.

As a category A liaison, ISACA/ITGI will engage and work with INCOSE, IEEE, and itSMF.

---

itSMF

Proposed letter from Craig Pattison, itSMF International Liaison to ISO/IEC JTC1 SC7 ICT Governance Study Group Convener Alison Holt

Dear Alison, August 2007

The itSMF International is pleased to contribute to the work of the ICT Governance Study Group in our capacity as Type A Liaison to ISO/IEC JTC1 SC7.

We believe that we can contribute to the work of the study group in three important ways:

1. The itSMF International represents the leading association of practitioners in the domain of IT Service Management 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 bring 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. The itSMF International, through its communications channels that includes a network of over forty six (46) national chapters around the world provides a valuable medium for disseminating information, performing research, and marketing the work of the ICT Governance Study Group.

We look forward to continuing to work with you and the members of the group as we progress our work-plan from the Moscow Plenary.

Best regards

Craig Pattison

Vice Chairman and Director of Certifications and Qualifications
itSMF International
www.itsmf.org
craig.pattison@itsmf.org

ANNEX I. REVIEW OF THE STATUS OF ICT GOVERNANCE ACROSS DIFFERENT NATIONS

Brian Cusack

Mikhail Pototsky

Christophe Feltus

Written and oral reports were presented to the ICT Study Group reviewing the state of different ICT Standards environments within the different jurisdictions.

A general movement towards compliance frameworks was reported in terms of legislation, Standards adoption and control framework adoption (eg. CobiT, ITIL, and so on). Several reports noted that regulatory requirements were pending and that there is considerable momentum gathering for comprehensive directives (both explicit and implicit). The importance of ICT Governance and the current opportune moment in time for ICT Governance advancement was reported in each case.

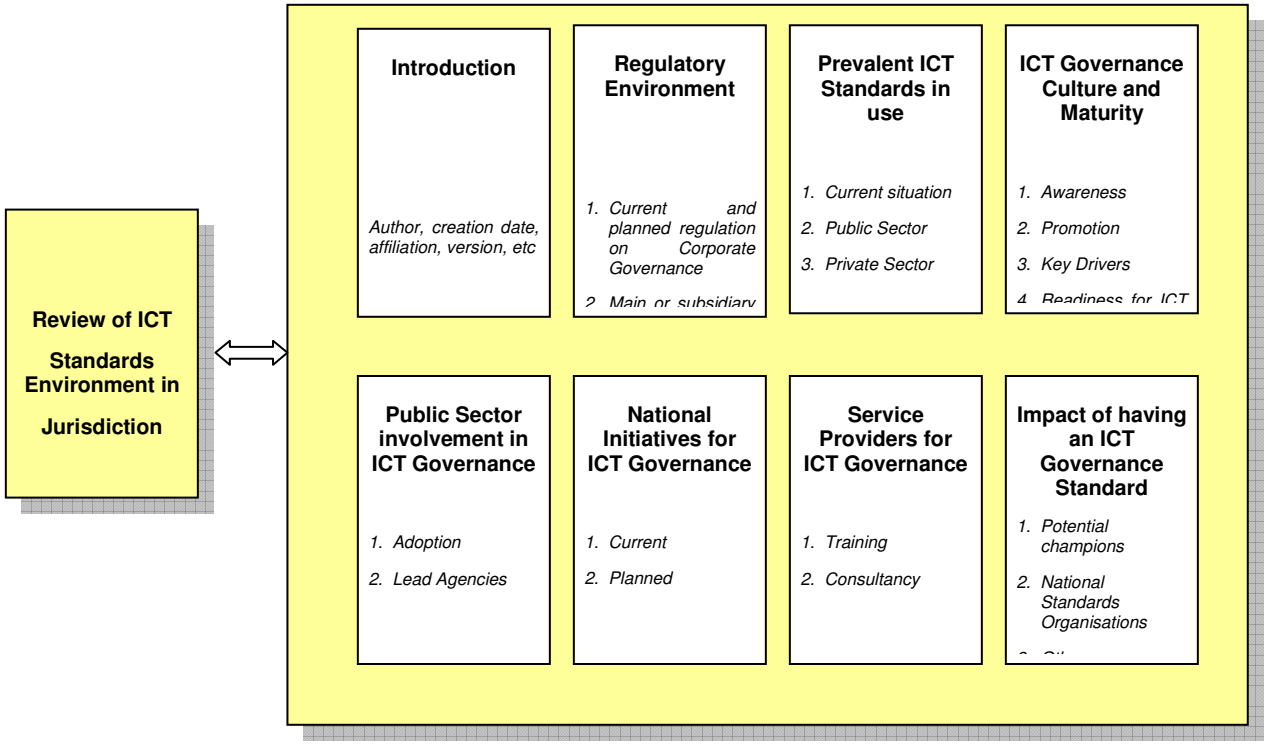
The variations included definitions of ICT Governance in different jurisdictions, the interpretation of ICT Governance, and the expectations for ICT governance practice. Two reports developed the conceptual framework of maturity and commented on the progressive positioning and advancement of adoption within the jurisdiction. These reports were particularly instructive as to the achievements being made.

A brief review of each jurisdiction variation follows in alphabetical order.

Jurisdiction	Overview
Australia	**Having an ICT Governance Standard (AS8015) 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) has established in May 2006 and will enact it in 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 view regulator, the CSSF (National supervisory body of the financial institutions) is the main actor for the financial institutions.**

Jurisdiction	Overview
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 discernable 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 proposed 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.**

Report Structure



ANNEX J. NEW WORK ITEM PROPOSAL

Melanie Cheong

New Work Item Proposal

Please see ISO/IEC JTC1/SC7 3895 for the final New Work Item Proposal