ISO/IEC JTC 1 N 9059

2008-05-13

ISO/IEC JTC 1
Information Technology

Document Type:	**Other Document(Defined)**
Document Title:	**Standards Framework v5 final draft**
Document Source:	**JTC1 Study Group on IT Governance Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for information**
Action ID:	**Information**
Due Date:	
No. of Pages:	**10**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1 Study Group on IT Governance N0021

DATE: 2008-05-09

ISO/IEC JTC 1

Study Group on IT Governance

Secretariat: SA (AU)

DOC TYPE:	**Document for discussion**
TITLE:	**Standards Framework v5 final draft**
PROJECT:	
STATUS:	**This document was produced by Mark Toomey on the request of the JTC1 SGITG at meeting 001. This document was informally circulated to JTC 1 SGITG members on 6 May, and is now formally circulated to JTC 1 SGITG members and JTC 1 National Bodies and Subcommittees for use by the delegates to the second meeting of the JTC 1 SGITG, Berlin, 17-19 May 2008**
ACTION ID:	**FYI**
DUE DATE:	
DISTRIBUTION:	**JTC1 Study Group on IT Governance**
MEDIUM:	
NO. OF PAGES:	**9**

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

Final draft for Study Group approval.

A Framework

for

Organising and Categorising Standards

related to

Governance of Information Technology

Prepared for the ISO/IEC JTC1 Study Group
on
Corporate Governance of IT

by Mark Toomey
Managing Director, Infonomics Pty. Ltd.

February/March 2008

Requirement for the Framework

The Study Group on Corporate Governance of IT was established by the Joint Technical Committee (JTC1) of the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) in November 2007. The Study Group is to report to the 2008 Plenary Meeting of JTC1 on "the need and feasibility of additional standardization and/or guidance in the area of ICT Governance".

During its initial meeting in Sydney in February 2008, the Study Group identified the need to understand clearly the orientation of standards relating to Information Technology and Corporate Governance, so that it can properly understand the extent and depth to which existing standards and standards development organizations address matters of IT Governance, and which existing standards address matters of Corporate Governance that do not pertain to IT.

The author proposed a framework for classification of the standards, comprising five categories, and was requested by the Study Group to formalize the framework.

This document presents the framework, explaining its basis in established academic theory, and proposing extensions where necessary.

The framework establishes:

- Seven or more "domains" in which governance and management related standards may have been developed, one of which is Information Technology.
- Five categories at which standards may be classified. It is acknowledged that some standards may span multiple categories.

It also presents an initial assessment of data required for classification of the standards.

Acknowledgment: I am grateful to fellow JTC1 SG member John Graham, of Educad, for his thoughtful review of this work.

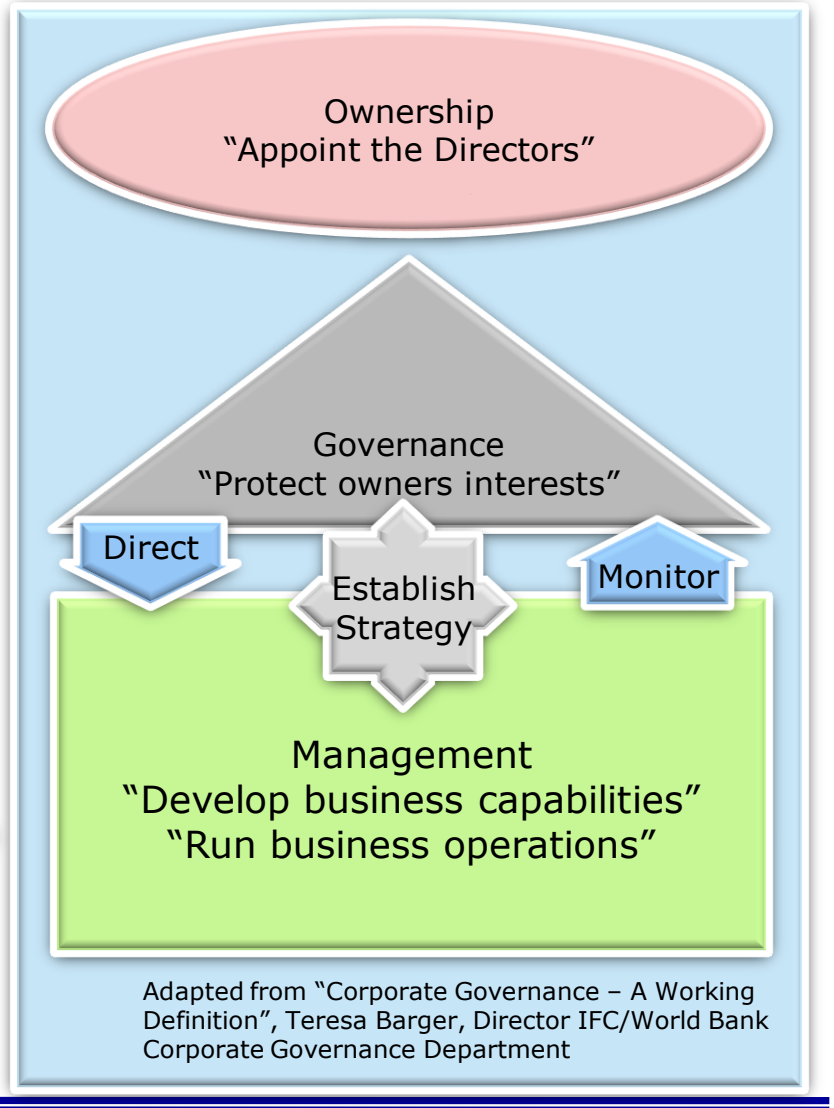
Design of the Framework
1: Corporate Governance Defined

The framework is centred on the fundamental notion of Corporate Governance, and builds on this notion in two ways – by identifying that there are several "domains" for detailed attention in Corporate Governance and by strongly separating the concept of "governance" from "management".

The definition of Corporate Governance is well established and clearly articulated. These three illustrations make it clear that corporate governance and management are separate, but closely related:

Corporate Governance: The System by which entities are directed and controlled.
(Report of the Committee on the Financial Aspects of Corporate Governance, London, 1992)

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, minority 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. (International Finance Corporation, 2005)



Adapted from "Corporate Governance – A Working Definition", Teresa Barger, Director IFC/World Bank Corporate Governance Department

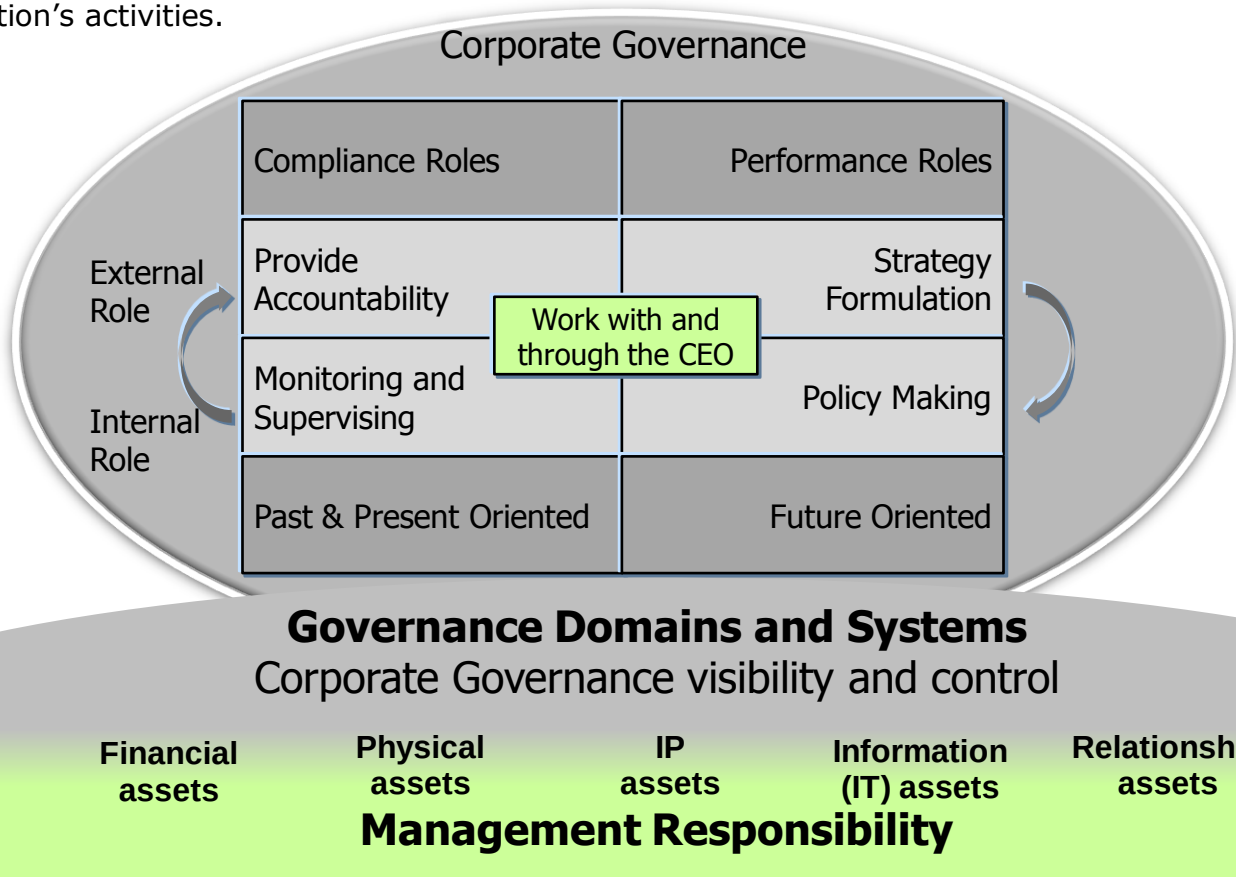
Design of the Framework
2: Corporate Governance Roles and Domains

Tricker established that corporate governance involves both internal and external perspectives, considering past, present and future aspects of the organisation. It includes formulation of strategy and making of policy. Corporate Governance works with and through the CEO to direct and monitor the organisation's activities.

Weill and Ross identified that corporate governance focuses on six domains, or asset groups, one of which is Information. For clarity, we view the terms Information and IT synonymously, focusing on the notion that IT is a resource used not just to manage information, but to enable current and future activities.

Broadbent combined these models to show that the system of governance is sustained by management activity, while providing appropriate visibility and control to the overall governing body.

We have extended the Weill and Ross list of Governance Domains to include Environment Assets, which are of increasing relevance in corporate governance for many organisations. The model allows for further extension when required.



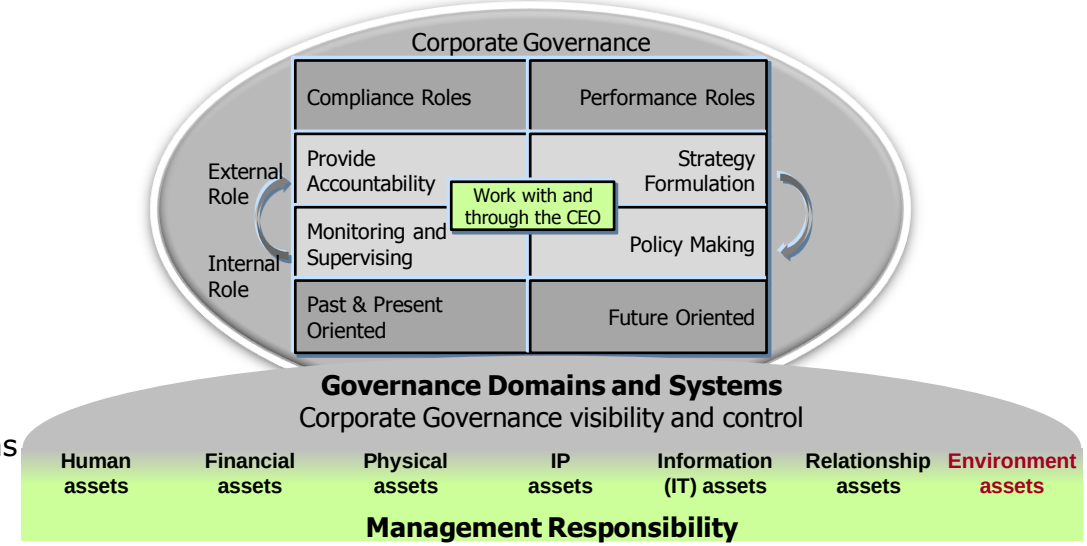
Sources: R. Tricker: *International Corporate Governance* (1994); P. Weill & J. Ross: *Don't Just Lead, Govern!: Empowering Effective Enterprise Use of Information Technology*, Harvard Business School Press, 2004; and M. Broadbent: *IT Governance: Who cares and does it matter?*, Australian Institute of Company Directors Annual Conference, May 2004

Design of the Framework
3: Definitions

Broadbent's integration of the Tricker and Weill/Ross models provides clarity for the notion that the **system of governance** embraces the roles and activities of both the governing body (the board of directors) and management. The extent to which the roles and activities overlap and interact is a matter for the governance design of the organisation.

Definitions contained in DIS29382 (which has completed all ballot processing and is shortly to be published as ISO/IEC 38015) provide clear distinction between the concepts of Governance and Management:

- **Corporate governance:** The system by which organizations are directed and controlled.
- **Corporate governance of IT:** The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.
- **Management:** The system of controls and processes required to achieve the strategic objectives set by the organisation's governing body. Management is subject to the policy guidance and monitoring set through corporate governance.
- It should be noted that, just as governance has both present and future orientation, management has present (operational) and future (projects) orientation. These aspects should be considered as complementary elements of each domain.



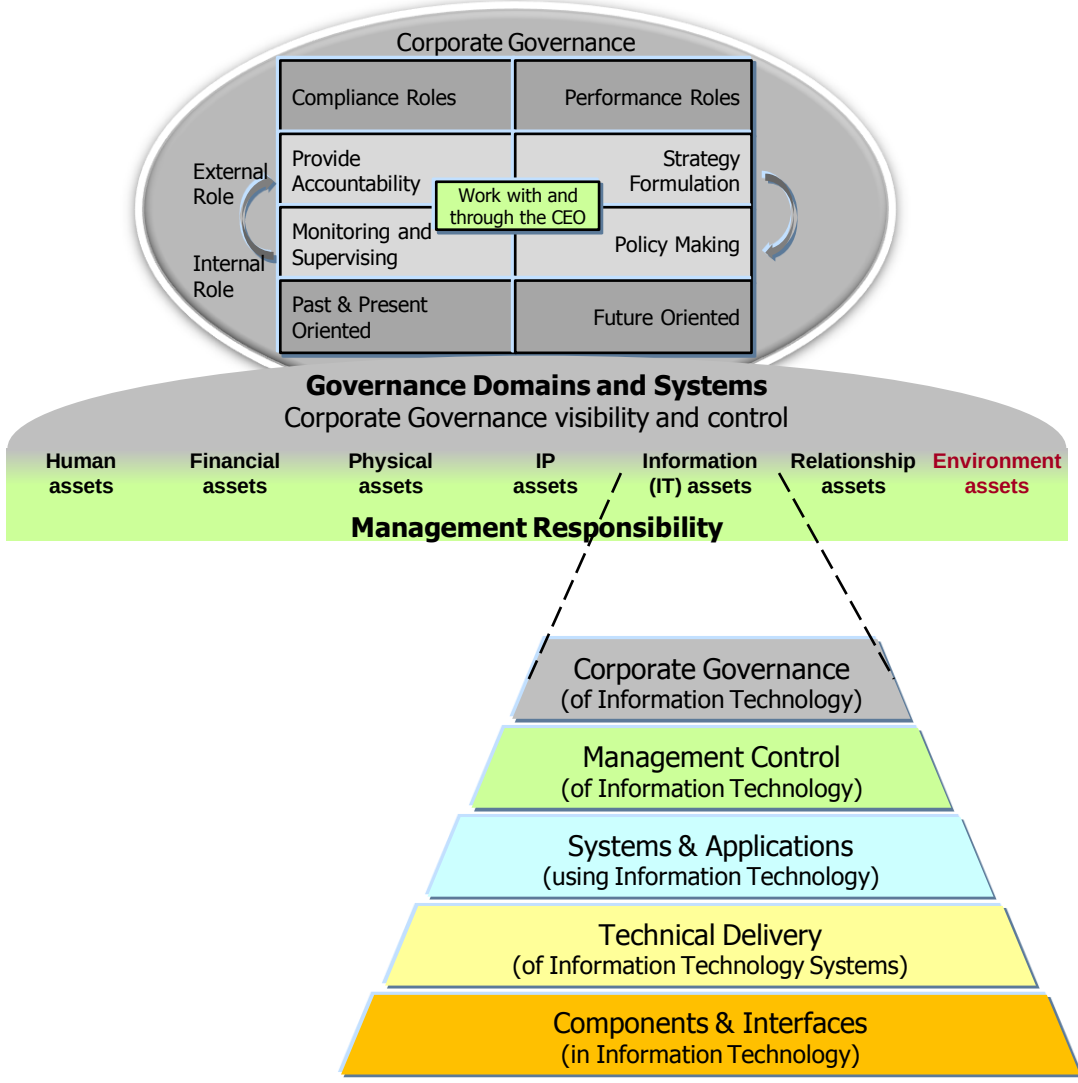
Design of the Framework
4: Categories

Extending the individual Governance Domains using a Category approach enables classification of standards and promotes understanding of the actual and potential relationships between standards in different categories. In particular, it assists in understanding the relationship between Governance Standards and Management Standards.

It is intended that standards will be categorised by their respective standards development organisations into one or more of the five categories depicted. It is accepted that some standards may span multiple categories.

The Corporate Governance Category contains those standards which fit the definition of Corporate Governance of IT as specified in DIS 29382 – that relate to "the system by which the current and future use of IT is directed and controlled". This includes DIS29382, its predecessor, AS8015, and the forthcoming Australian Standard AS8016.

The Management Control Category contains those standards that fit the definition of Management Control in DIS 29382 – that relate to "the system of controls and processes required to achieve the strategic objectives set by the organisation's governing body". There are likely to be numerous standards within the Management Control Category. There may also be management topics for which there are few current standards – and it is not unreasonable for contributors to note these topics. Some possible management fields in which there may or may not be standards at present are Operations, Security, Architecture, Configuration, Project, Resource, Risk, Quality and so on.



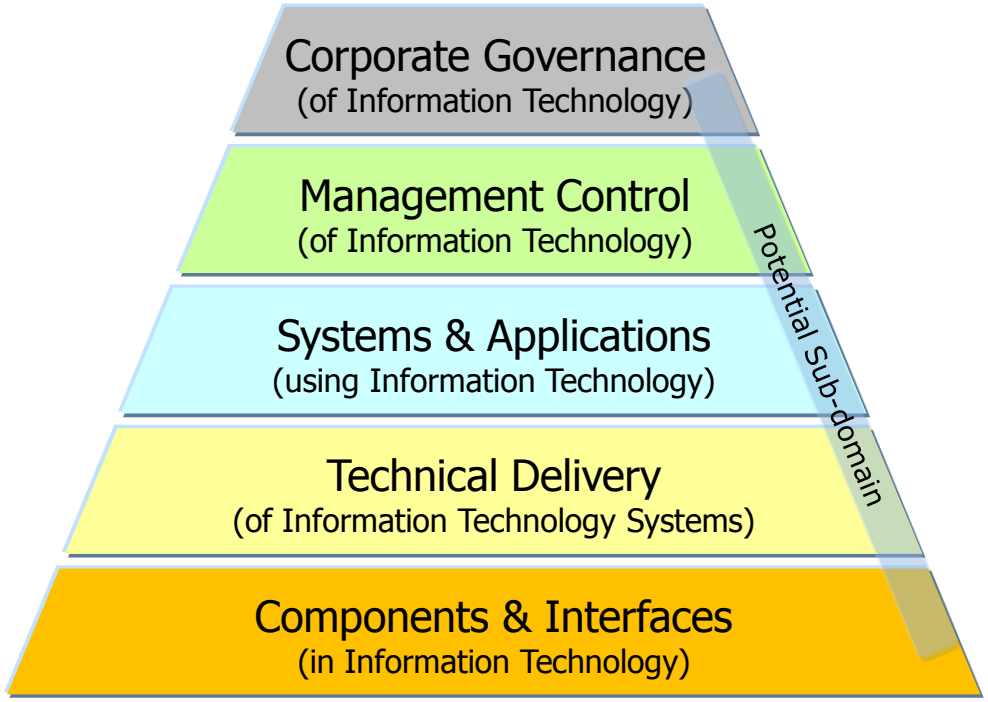
Design of the Framework
4: Categories (Cont)

Other topics that would be covered in Management Control include Enterprise Architecture, Project Management and Portfolio Management, Business Continuity and Disaster Recovery. Thus, the framework provides a way of positioning industry and defacto standards, frameworks and methodologies such as Prince2, COBIT, ValIT, TOGAF and ITIL relative to corresponding formal national and international standards.

The Systems & Applications Category contains standards that relate to a specific use of IT to provide a capability to an organisation. Examples of such standards are those relating to Electronic Funds Transfer (EFT) and Electronic Document Interchange (EDI). As standards are classified in this category, it may also be useful to cluster them into groups – though this step is not necessary for the purposes of the Study Group.

The Technical Delivery Category contains standards that relate to the design and construction of Systems and Applications. These include standards for design, construction and testing of business systems, communications networks and data centres, as well as standards for programming techniques, requirements modelling, data modelling and database design.

The Components and Interfaces Category contains standards that relate to the basic building blocks of Information Technology. These include standards for encoding data (whether in databases or in interfaces), standards for programming languages, standards for hardware components and standards describing communications protocols.



Within the IT Domain, there are also likely to be several broad fields in which standardisation has been undertaken in multiple categories. One field in which this is thought likely is Information Security. To promote fuller understanding of these fields, it is intended that Sub-Domains be identified as required. Standards should be allocated to a sub-domain on the basis of the topics they address, rather than on any assessment of whether they were planned to be related. This approach will give the best overall picture of the current standards landscape.

Populating the Framework
Data Required (Preliminary Discussion)

Classification of individual standards in the framework requires assessment of the standard by a knowledgeable person against the criteria for inclusion in each governance domain and category. For the purposes of maintaining a flexible and useable model, we intend to only classify standards that fit either partly, or wholly, into the Information (IT) domain. It is possible that some standards and similar instruments may actually span multiple domains, but this information is not required.

The data required to classify each standard that relates to the Information (IT) Domain is:

- Name of Standard
- Governance category
  - Extent of fit
- Management category
  - Extent of fit
- Specific Systems category
  - Extent of fit
- Technical Delivery category
  - Extent of fit
- Fundamental Components
  - Extent of fit.

To enable full understanding of the context of each standard, and to assist in follow-up where necessary, additional information which may be sought for each standard is:

- Details of person providing the information, including name, contact details, affiliation with the standard's Controlling Organisation;
- Details of the Controlling Organisation which is responsible for ongoing maintenance and development of the standard;
- Nature of the Standard (International Standard, National Standard, Industry Standard, Professional Standard, Framework, Methodology, etc);
- Principal Audience for the standard (by role) where applicable (Owners, Directors, Executive Managers, Business Managers, Technology Managers, Consultants and Advisors, Others)