DRAFT INTERNATIONAL STANDARD ISO/IEC 29382

Attributed to ISO/IEC JTC 1 by the Central Secretariat (see page iii)

Voting begins on	Voting terminates on
2007-02-01	**2007-07-01**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

FAST-TRACK PROCEDURE

Corporate Governance of Information and Communication Technology

Gouvernance d'entreprise des technologies de l'information et de la communication

ICS 03.100.99; 35.020

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

© International Organization for Standardization, 2007
International Electrotechnical Commission, 2007

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2007 — All rights reserved

Not for Resale

NOTE FROM ITTF

This draft International Standard is submitted for JTC 1 national body vote under the Fast-Track Procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 29382 to JTC 1/SC 7.

"FAST-TRACK" PROCEDURE

1 Any P-member and any Category A liaison organization of ISO/IEC JTC 1 may propose that an existing standard from any source be submitted directly for vote as a DIS. The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide.

2 The proposal shall be received by the ITTF which will take the following actions.

2.1 To settle the copyright and/or trade mark situation with the proposer, so that the proposed text can be freely copied and distributed within JTC 1 without restriction.

2.2 To assess in consultation with the JTC 1 secretariat which SC is competent for the subject covered by the proposed standard and to ascertain that there is no evident contradiction with other International Standards.

2.3 To distribute the text of the proposed standard as a DIS. In case of particularly bulky documents the ITTF may demand the necessary number of copies from the proposer.

3 The period for combined DIS voting shall be six months. In order to be accepted the DIS must be supported by 75 % of the votes cast (abstention is not counted as a vote) and by two-thirds of the P-members voting of JTC 1.

4 At the end of the voting period, the comments received, whether editorial only or technical, will be dealt with by a working group appointed by the secretariat of the relevant SC.

5 If, after the deliberations of this WG, the requirements of 3 above are met, the amended text shall be sent to the ITTF by the secretariat of the relevant SC for publication as an International Standard.

If it is impossible to agree to a text meeting the above requirements, the proposal has failed and the procedure is terminated.

In either case the WG shall prepare a full report which will be circulated by the ITTF.

6 If the proposed standard is accepted and published, its maintenance will be handled by JTC 1.

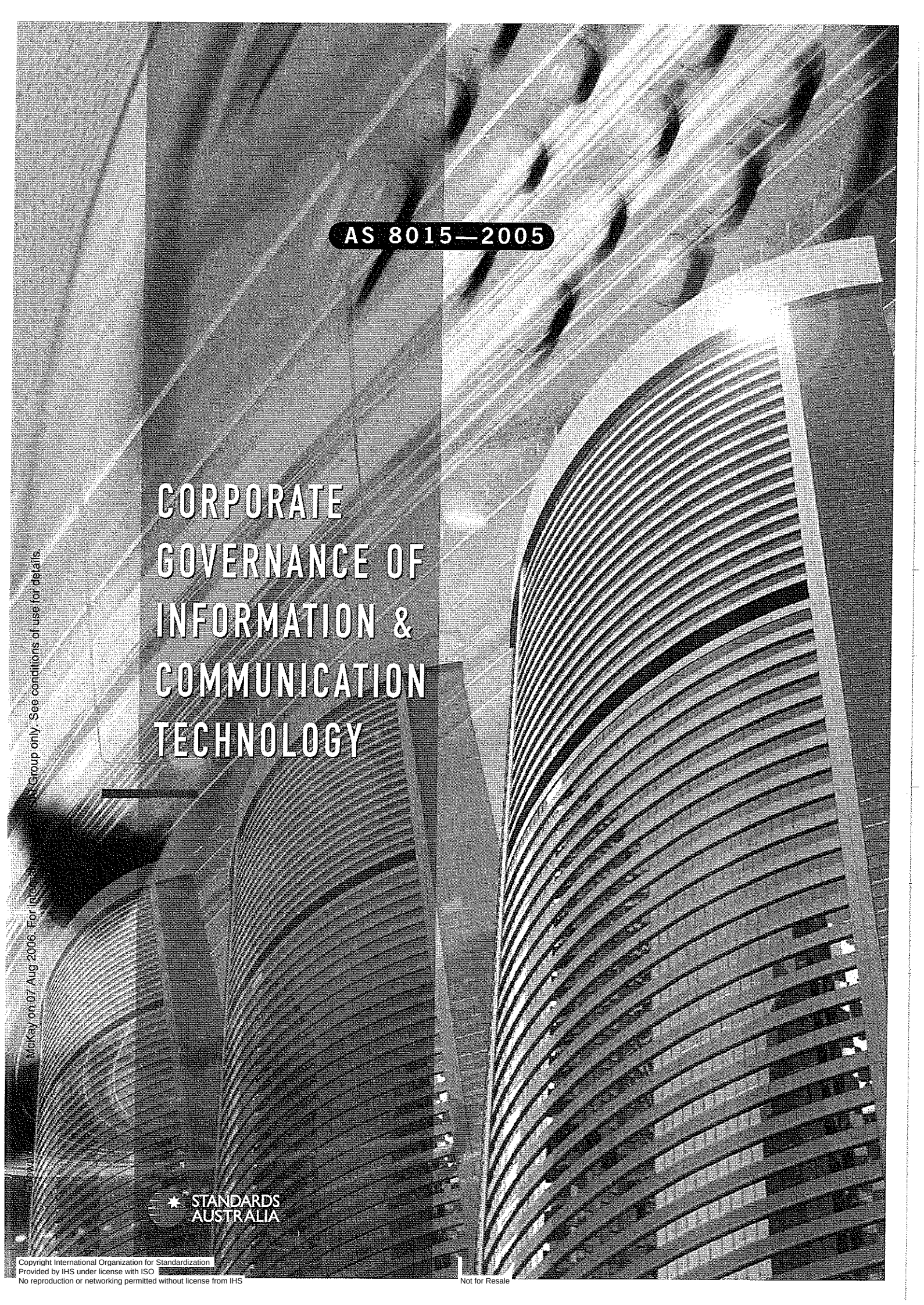
© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

AS 8015—2005

CORPORATE GOVERNANCE OF INFORMATION & COMMUNICATION TECHNOLOGY



STANDARDS AUSTRALIA

Downloaded from SAI Global by McKay on 07 Aug 2006. For personal use only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This Australian Standard was prepared by Committee IT-030, IT Governance. It was approved on behalf of the Council of Standards Australia on 21 December 2004.
This Standard was published on 31 January 2005.

The following are represented on Committee IT-030:

Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Computer Society
Australian Electrical and Electronic Manufacturers Association
Australian Institute of Company Directors
Australian Institute of Project Management
Consumers' Federation of Australia
Department of Defence (Australia)
Information Systems Audit and Control Association
Project Management Institute
RMIT University
Society of Consumer Affairs Professionals
University of New South Wales

Additional Interests:

Adacel Technologies
Attorney General's Department
Australian Defence Force Academy
Catalyst Consulting
Centrelink
Central Queensland University
Codarra Advanced Systems
Curtin University of Technology
Decisions
Department of Innovation, Industry and Regional Development
DGJ Consulting
DISplay
Educad
Garry Blair Consulting
Gartner Australasia
Infonomics Pty Ltd
Information Project Services
Kiscom Consulting
Macquarie Graduate School of Management
Max Shanahan and Associates
Nationwide News
NSW Department of Commerce
Phillips Fox
Ramin Communications
SIFT
SingTel Optus
Software Quality Institute
Synergy Management Solutions
System Integration Services International
Tenix Datagate
The Art of Service
The Frame Group
Workcover New South Wales

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 04198.

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Australian Standard™

Corporate governance of information and communication technology

DRAFT 2007

First published as AS 8015—2005.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia, GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 6438 X

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PREFACE

This Standard was prepared by the Standards Australia Committee IT-030, ICT Governance and Management.

The objective of this Standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the information and communication technology (ICT) portfolio in their organizations.

This Standard for the Corporate Governance of ICT is aligned with the set of standards headed by AS 8000—2003. The other standards in that set provide guidance to organizations on good governance principles, fraud and corruption control, codes of conduct, social responsibility and whistle blower protection.

Most organizations use ICT and few can function effectively without it.

Expenditure on ICT can represent a significant proportion of an organization's financial and human commitment. However, a return on this investment is often not realized and the adverse effects on organizations can be significant.

The main reasons for these negative outcomes are the emphasis on technical, financial and scheduling aspects of ICT activities rather than corporate governance of ICT.

This standard provides a framework for good governance of ICT, to assist those at the highest level of organizations to understand and fulfil their obligations. The framework comprises definitions, principles and a model.

Other standards and handbooks, covering implementation and development of governance structures, will support this standard.

Two Standards that are currently being developed deal with—

(a) ICT projects; and

(b) ICT operations.

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

CONTENTS

Page

SECTION 1 SCOPE,APPLICATION AND OBJECTIVES
1.1 SCOPE 4
1.2 APPLICATION 4
1.3 OBJECTIVES 4
1.4 BENEFITS OF USING THIS STANDARD 5
1.5 REFERENCED DOCUMENTS 5
1.6 DEFINITIONS 6

SECTION 2 OVERVIEW OF FRAMEWORK FOR GOOD CORPORATE GOVERNANCE OF ICT
2.1 PRINCIPLES 8
2.2 MODEL 8

SECTION 3 CORPORATE ICT GOVERNANCE FRAMEWORK
3.1 GENERAL 10

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

© Standards Australia

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

STANDARDS AUSTRALIA

Australian Standard

Corporate governance of information and communication technology

SECTION 1 SCOPE, APPLICATION AND OBJECTIVES

1.1 SCOPE

This Standard provides guiding principles for Directors of organizations (including owners, board members, Directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information and Communication Technology (ICT) within their organization.

The Standard applies to the governance of resources, computer-based or otherwise, used to provide information and communication services to an organization. These resources could be provided by ICT specialists, within the organization or external service providers, or by business units within the organization.

1.2 APPLICATION

This Standard is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. The standard is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of ICT.

It also provides guidance to those advising, informing, or assisting Directors. They include:

(a) Senior managers.

(b) Members of groups monitoring the resources within the organization.

(c) External business or technical specialists, such as legal or accounting specialists, retail associations, or professional bodies.

(d) Vendors of hardware, software, communications and other ICT products.

(e) Internal and external service providers (including consultants).

(f) ICT auditors.

1.3 OBJECTIVES

The purpose of this Standard is to promote effective, efficient, and acceptable use of ICT in all organizations by—

(a) providing stakeholders (including consumers, shareholders, and employees) with the confidence that, if the Standard is followed, they can trust in the organization's corporate governance of ICT;

(b) informing and guiding Directors in governing the use of ICT in their organization; and

(c) providing a basis for objective evaluation of the corporate governance of ICT.

DRAFT 07

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1.4 BENEFITS OF USING THIS STANDARD

1.4.1 General

This Standard provides guidance to Directors on the areas of risk associated with the implementation and use of ICT. This in turn minimizes the risk of them not fulfilling their responsibilities towards ensuring that their organizations conform with the law and perform in obtaining the best return on their investment in ICT. It also provides a common vocabulary for the Governance of ICT.

1.4.2 Conformance of the organization

Proper corporate governance of ICT can help Directors to assure conformance with obligations (regulatory, common law, contractual) concerning the acceptable use of ICT.

Inadequate ICT systems can expose the Directors to the risk of not complying with legislation. For example, directors could be held personally liable if an inadequate accounting system leads to tax not being paid.

Processes dealing with ICT incorporate specific risks that must be addressed appropriately. For example, Directors can be held personally liable for breaches of:

(a) Security standards (AS/NZS ISO/IEC 17799 and AS/NZS 7799.2).

(b) Privacy legislation.

(c) Spam legislation.

(d) Trade practises legislation.

(e) Intellectual property rights, including software licensing agreements.

(f) Record keeping requirements.

(g) Environmental legislation and regulations.

Directors using the guidelines in this Standard are more likely to meet their obligations. Compliance programs are addressed in AS 3806:1998 and should be considered in assuring conformance.

1.4.3 Performance of the organization

Proper corporate governance of ICT assists the Directors to assure the required performance of the organization, through—

(a) ensuring business continuity and sustainability;

(b) alignment of ICT with business needs;

(c) efficient allocation of resources;

(d) innovation in services, markets, and business;

(e) encouraging good practice in relationships with stakeholders;

(f) reducing the costs for an organization; and

(g) ensuring the approved benefits are actually realized from each ICT investment.

1.5 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS	
3806	Compliance programs
8000	Corporate governance—Good governance principles
AS/NZS	
4360	Risk management

© Standards Australia

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

DRAFT

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

AS/NZS 7799.2	Information security management—Specification for information security management systems
ISO/IEC 17799	Information technology—Code of practice for information security management

1.6 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

In some instances, a particular organization will adapt the terminology used within this Standard to suit their circumstances or structure.

1.6.1 Corporate governance

The system by which entities are directed and controlled (AS 8000).

1.6.2 Corporate governance of ICT

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.

1.6.3 Director

Member of the most senior governing body of an organization. Includes owners, board members, Directors, partners, senior executives or similar, and officers authorized by Acts of Parliament.

1.6.4 Entity

A company, corporation, government, not-for-profit or other legally constituted organization.

1.6.5 Human factors

The understanding of interactions among humans and other elements of a system with the intent to insure well being and systems performance.

1.6.6 Information and communication technology (ICT)

Resources required to acquire, process, store and disseminate information.

1.6.7 Investment

Allocation of human, capital and other resources to achieve defined objectives and other benefits.

1.6.8 Organization

Any corporate entity including associations, clubs, partnerships, government agencies, publicly listed companies, private companies and sole traders.

1.6.9 Proposal

Compilation of benefits, costs and risks and other factors applicable to decisions to be made by the board. Includes business cases.

1.6.10 Resources

People, procedures, software, information, equipment, consumables, facilities, capital and operating funds, and time.

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1.6.11 Risk

The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood (AS/NZS 4360).

1.6.12 Risk management

The culture, processes and structure that are directed towards the effective management of potential opportunities and adverse effects (AS/NZS 4360).

1.6.13 Stakeholder

Those people or entities who may affect, be affected by, or perceive themselves to be affected by, a decision or activity (AS/NZS 4360).

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

© Standards Australia

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECTION 2 OVERVIEW OF FRAMEWORK FOR GOOD CORPORATE GOVERNANCE OF ICT

2.1 PRINCIPLES

This section sets out 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.

2.1.1 Principle 1—Establish clearly understood responsibilities for ICT

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

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 Principle 5—Ensure ICT conforms with formal rules

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

2.1.6 Principle 6—Ensure ICT use respects human factors

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

2.2 MODEL

Directors should govern ICT through three main tasks:

(a) Evaluate the use of ICT.

(b) Direct preparation and implementation of plans and policies.

(c) Monitor conformance to policies, and performance against the plans.

Figure 1 shows the ICT Governance model of the cycle of Evaluate-Direct-Monitor. The text following Figure 1 explains the elements and relationships depicted.

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

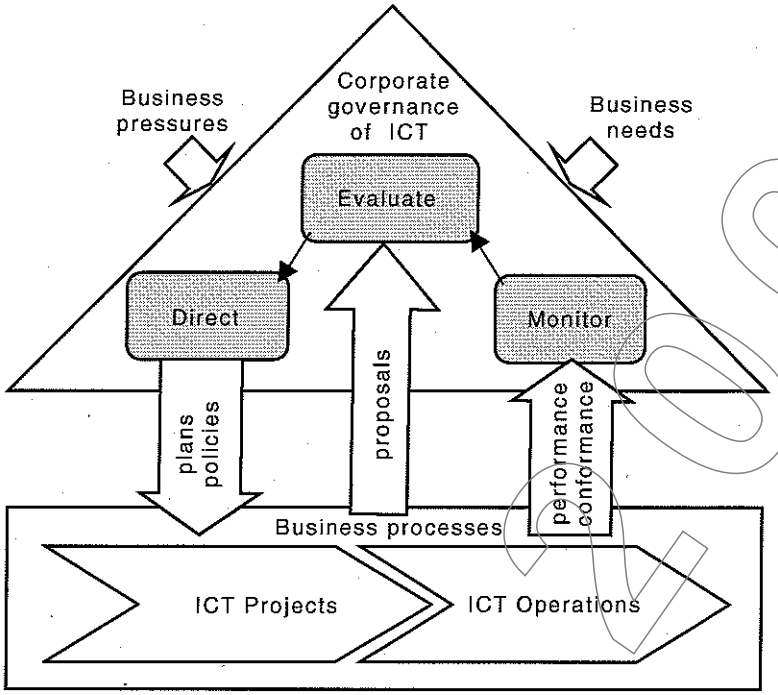


FIGURE 1 MODEL FOR CORPORATE GOVERNANCE OF ICT

In evaluating the use of ICT, Directors should consider the pressures acting upon the business, such as technological change, economic and social trends, and political influences.

Directors should also take account of the business needs—the organizational objectives that they must achieve, such as maintaining competitive advantages.

Directors should direct the preparation and implementation of plans and policies and assign responsibilities for this implementation. Plans should set the direction for investments in ICT projects or changes in ICT operations. Policies should establish sound behaviour in the use of ICT.

Directors should ensure that the transition from projects to operations takes into account impacts on operational practices and existing ICT infrastructure.

To complete the cycle, the Directors should monitor, through appropriate performance measurement systems, the performance of the ICT. They should reassure themselves that performance is in accordance with plans. They should also make sure that the use of ICT conforms with external legal obligations and internal work practices. If necessary, they should direct the submission of proposals for approval to address identified needs.

NOTE: Responsibility for specific aspects of ICT may be delegated, however, the accountability for the effective, efficient and acceptable use of ICT by an organization, remains with its Directors.

DRAFT 2007

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© Standards Australia
Not for Resale
www.standards.com.au

SECTION 3 CORPORATE ICT GOVERNANCE FRAMEWORK

3.1 GENERAL

Table 1 lists the general principles of sound ICT governance and the actions required by Directors to implement the principles. They are applicable to most organizations most of the time and any variation should be well considered.

TABLE 1

ICT GOVERNANCE FRAMEWORK

Ref No	Principle	Actions to implement the principle		
		Evaluate	**Direct**	**Monitor**
1.	Establish clearly understood responsibilities for ICT.	Directors should evaluate the options for assigning the responsibilities for the effective, efficient, and acceptable use of ICT. Directors should ensure that those given responsibility are competent. Generally, these will be business managers, assisted by ICT specialists who understand business values and processes. Directors should evaluate developments in ICT and business processes to ensure that ICT will provide support for future business needs.	Directors should direct that plans are carried out and policies implemented according to the assigned ICT responsibilities.	Directors retain ultimate responsibility for the execution of the plans and proposals. They should satisfy themselves that appropriate ICT governance mechanisms are established. Directors should monitor the performance of those given responsibility in the governance of ICT (for example, in serving on steering committees or in presenting proposals to Directors). Directors should ensure that they receive the information that they need to meet their responsibilities by establishing and appropriately reviewing measurement systems.
2.	Plan ICT to best support the organization	In formulating plans and policies, Directors should evaluate ICT activities to ensure they align with the organization's objectives for changing circumstances, consider better practices and satisfy other key stakeholder requirements. Directors should use prudent risk management procedures, as described in AS/NZS 4360.	Directors should direct that proposals are submitted for approval, in a timely fashion, to address gaps identified in the evaluation of ICT activities. Directors should also encourage the submission of proposals for innovative uses of ICT that enable the organization to undertake new businesses or improve processes. Directors should direct the preparation and use of plans and policies that ensure the organization benefits from developments in ICT.	Directors should monitor the progress of approved ICT proposals to ensure that they are achieving objectives in required timeframes using allocated resources. Directors should monitor the use of ICT to ensure that it is achieving its intended benefits.

(*continued*)

DRAFT ISO

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
www.standards.com.au
Not for Resale

DRAFT 2007

TABLE 1 (*continued*)

Ref No	Principle	Actions to implement the principle		
		Evaluate	**Direct**	**Monitor**
3.	Acquire ICT validly	Directors should evaluate options for providing ICT to realize approved proposals, balancing risks and value for money of proposed investments.	Directors should direct that ICT assets (systems and infrastructure) are acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided. Directors should direct that their organization and suppliers develop a shared understanding of the organization's intent in making any ICT acquisition.	Directors should monitor ICT acquisitions to ensure that they do provide the required capabilities. Directors should monitor the extent to which their organization and suppliers maintain the shared understanding of the organization's intent in making any ICT acquisition.
4.	Ensure ICT performs well, whenever required	Directors should evaluate the risks to the integrity of information and the protection of ICT assets from damage, abuse, or misuse. Directors should evaluate options to ensure that ICT will support business processes with the required capability and capacity.	Directors should direct those responsible to ensure that ICT supports the business, when required for business reasons, with correct and up-to-date data while protected from loss or misuse, in accordance with AS/NZS ISO/IEC 17799 and AS/NZS 7799.2. Directors should direct that resources be allocated sufficiently to ensure that ICT meets the needs of the organization, according to the priorities that they have set.	Directors should monitor the extent to which ICT does support the business. Directors should monitor ICT to ensure that assets are decommissioned and disposed of in accordance with environmental and data management requirements. Directors should monitor the extent to which the policies for data accuracy and the efficient use of ICT are followed properly.

(*continued*)

© Standards Australia

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

TABLE 1 (*continued*)

Ref No	Principle	Actions to implement the principle		
		Evaluate	**Direct**	**Monitor**
5.	Ensure ICT conforms with formal rules	Directors should regularly evaluate the extent to which ICT satisfies internal obligations including legislation, internal policies, standards and professional guidelines.	Directors should direct those responsible to establish regular and routine mechanisms for ensuring that the use of ICT complies with relevant legislation. Directors should direct that policies are established and enforced to enable the organization to meet its internal obligations in its use of ICT. Directors should direct that ICT staff follow the guidelines set by their professions. Directors should direct that all actions relating to ICT be ethical.	Directors should monitor the manner in which managers are reviewing ICT compliance and conformance to ensure that the reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of internal obligations.
6.	Ensure ICT use respects human factors	Directors should evaluate ICT activities to ensure that people's concerns are appropriately considered and their needs identified.	Directors should direct that ICT activities are consistent with identified needs. Directors should direct that risks may be raised by anyone at any time. They should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.	Directors should monitor ICT activities to ensure that identified needs remain relevant. Directors should monitor work practices to ensure that they are consistent with the appropriate use of ICT.

DRAFT 2007

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© Standards Australia

Not for Resale

www.standards.com.au

DRAFT 2007

Standards Australia

Standards Australia is an independent company, limited by guarantee, which prepares and publishes most of the voluntary technical and commercial standards used in Australia. These standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth government, Standards Australia is recognized as Australia's peak national standards body. For further information on Standards Australia visit us at

www.standards.org.au

Australian Standards

Australian Standards are prepared by committees of experts from industry, governments, consumers and other relevant sectors. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia is responsible for ensuring that the Australian viewpoint is considered in the formulation of international Standards and that the latest international experience is incorporated in national Standards. This role is vital in assisting local industry to compete in international markets. Standards Australia represents Australia at both ISO (The International Organization for Standardization) and the International Electrotechnical Commission (IEC).

Electronic Standards

All Australian Standards are available in electronic editions, either downloaded individually from our web site, or via On-Line and DVD subscription services. For more information phone 1300 65 46 46 or visit Standards Web Shop at

www.standards.com.au

Downloaded by Andrew McKay on 07 Aug 2006. For internal use within SAI Group only. See conditions of use for details.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DRAFT 2007

ISBN 0 7337 6438 X

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale