



**Department of Broadband, Communications and the Digital Economy
Digital Economy Future Directions Consultation Paper**

**Submission in response by Standards Australia
February 2009**

Introduction

Standards Australia (SA) recognises the rising interest and importance of IT governance to increase the effective use of networked information and communication technologies (ICT's), especially the internet, by consumers and businesses to drive higher productivity growth and community participation in the digital economy.

Because inadequate information technology (IT) systems can hinder the performance and competitiveness of organisations or expose them to the risk of not complying with legislation, SA has developed a suite of standards designed to meet this growing requirement which provide broad guidance on the role of top management in relation to the corporate governance of IT.

For example, AS 8015, the Australian Standard for Corporate Governance of ICT, defines Corporate Governance of ICT as "*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 organisation.*"

SA is aware that many changes have occurred in the technology environment since the beginning of the digital economy and we are currently working on a range of initiatives and standards to ensure Australia remains competitive and sets best practice guidelines in this field.

SA notes that the following issues should be of particular importance in this review:

1. Security and privacy of information and encryption; and
2. The need to drive consumer confidence and usage of the internet to achieve higher productivity.

Standards Australia and Australian Standards™

The Federal Government recognises Standards Australia as the nation's peak non-government standards development organisation. Standards Australia prepares voluntary, technical and commercial standards for use in Australia and accredits other Australian Standards Development Organisations (via the Accreditation Board for Standards Development Organisations (ABSDO), a separate entity within Standards Australia). It meets national needs for contemporary, internationally aligned standards and related services that enhance Australia's economic efficiency and international competitiveness.



To ensure this, a Memorandum of Understanding has existed between Standards Australia and the Commonwealth Government since 1988. Among the principal accords, are that no Australian Standard will contravene the World Trade Organisation's requirements that national standards should not be used as non-tariff barriers to free trade; and agreement that no new Australian Standard will be developed where an acceptable international standard already exists.

Standards Australia is also Australia's member of the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Council of Societies of Industrial Design (ICSID), providing a direct link to international best practice and creating further standards development efficiencies.

Australian Standards™ are developed by Standards Australia via voluntary participation from industry, government and other interested parties via technical committees. They are living documents that reflect progress in science and technology and encourage innovation.

They are voluntary documents (mechanisms for self-regulation) with which compliance is not mandatory unless the standard is incorporated into law (quasi-regulation or co-regulation) or called up in contractual arrangements. The decision on whether a standard will be given regulatory effect is usually made at the commencement of the standards development process and this may be due to regulatory arrangements managed by various Commonwealth, State and Territory government bodies.

Standards are developed according to due process which provides them with their authority and widespread acceptance, and that due process is centred on two main pillars:

- *Consensus*: meaning general agreement, characterised by the absence of sustained opposition to substantial issues by any important part of the concerned interests, arrived at by a process that takes into account the views of all parties concerned while reconciling any conflicting arguments
- *Transparency*: meaning that notification and all information on current work programs and proposals is available to all interested parties. Transparency also includes the concepts of openness, participation on a non-discriminatory basis and impartiality.

Standards Australia has well-established links into all areas of Australian business, professions, academia and the community with more than 9,000 experts drawn from over 1,000 nominating organisations. It has developed standards across most sectors of the Australian economy, in traditional industries such as goods and services, engineering and construction; in other technical areas such as health and food; in emerging new areas of technology such as e-health; as well as in less technologically based subjects such as complaints handling and risk management.



Standards Australia: A New Era

Standards Australia has undertaken a significant business transformation in order to ensure that its activities and those of its technical experts on standards committees can sustainably continue well into the future to serve the Australian community at large.

With effect from October 2008, Standards Australia implemented its New Business Model. The central concepts to the new model are Net Benefit and choice of pathways. Net Benefit can be summarised as 'having a positive effect on relevant communities'. Quite simply, all projects now developed under the Standards Australia banner must deliver demonstrable Net Benefit to the Australian economy.

All project proposals are assessed by the same criteria. Delivery of standards and related consensus documentation into the marketplace can be fast-tracked by adopting one of the five 'Alternative Pathways' now available to stakeholders. The 'Pathways' provide flexibility and choice, acknowledging that stakeholders may be able to assist with the resources required to develop standards.

The model ensures that the limited resources of both stakeholders and Standards Australia are utilised to the very best effect. This is consistent with our status as the peak standards body and the Memorandum of Understanding that we hold with the Commonwealth.

International Policy

Standards Australia has a policy of adopting International Standards wherever possible. This policy is in line with Australia's obligations under the World Trade Organization's Code of Practice, which requires the elimination of technical Standards as barriers to international trade. As a result approximately 33% of current Australian Standards are fully or substantially aligned with International Standards.

The principal benefit to Australia of basing Australian Standards on the equivalent International Standards is the benefit to the Australian economy by facilitating the international exchange of goods and services. Other benefits include the following:

- International (IEC and ISO) Standards generally reflect the best experience of industry and regulators worldwide and cover conditions in a variety of countries.
- Australia's obligations under the WTO TBT Agreement are supported.
- Participation in international certification schemes is facilitated.

ISO (International Organization for Standardization)

ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards.



ISO is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

Australian Standards are voluntary (unless they are referenced in regulation) and they are intended to apply across the nation.

Consequences of a lack of IT governance

Most organisations use IT as a fundamental business tool and few can function effectively without it. However, a return on the investment made in IT is often not fully realised. The adverse effects on organisations of a lack of IT governance can be significant including security breaches, inferior disaster recovery processes, safety and privacy issues or a huge impact on customer service.

For this reason, SA developed a suite of standards to assist establishing markers of success. Such standards are also important to grow and maintain consumer confidence as consumers will feel safer purchasing online, banking and social interaction when they know that a business adopts practices that respect user privacy and security.

National and International Activities in the IT Governance Sector

Following Corporate Collapses in Australia in 2000, working groups were established to develop standards for Corporate Governance. A series of Australian Standards for Corporate Governance were published in 2003, these were:

- Good Governance Principles (AS8000)
- Fraud and Corruption Control (AS8001)
- Organisational Codes of Conduct (AS8002)
- Corporate Social Responsibility (AS8003)
- Whistle Blower protection programs (AS8004)

AS8015 Corporate Governance of ICT was published in January 2005. It was fast-track adopted as ISO/IEC 38500 in May 2008.

Corporate Governance of information technology	ISO/IEC 38500	2008
Corporate governance of information technology	ISO IEC 38500-2008	2008
Corporate Governance Collection (Includes 8000, 8001, 8002,	AS 8000 C-	2007



8003, 8004 plus all Amendments)	2007	
Corporate Governance of Information and Communication Technology	ISO IEC DIS 29382	2007
Interoperability infrastructure governance requirements	HB 316-2006	2006
Corporate governance of information and communication technology	AS 8015-2005	2005
Governance, risk management and control assurance	HB 254-2005	2005
Corporate governance of information and communication technology	AS 8015-2005	2005
Corporate governance - Corporate social responsibility	AS 8003-2003 AMDT 1	2004
Corporate governance - Fraud and corruption control	AS 8001-2003 AMDT 1	2004
Corporate governance - Good governance principles	AS 8000-2003 AMDT 1	2004
Corporate governance - Organizational codes of conduct	AS 8002-2003 AMDT 1	2004
Corporate governance - Whistleblower protection programs for entities	AS 8004-2003 AMDT 1	2004
Corporate governance - Good governance principles	AS 8000-2003	2003
Corporate governance - Organizational codes of conduct	AS 8002-2003	2003
Corporate governance - Whistleblower protection programs for entities	AS 8004-2003	2003
Corporate Governance standards (CD-ROM)	AS 8000-2003 (CD)	2003

Standards Australia and Corporate Governance

Good corporate governance promotes best practice, of which IT governance is an importance component.

Australia to lead international working group on corporate governance of IT



In recognition of Australia's leadership and expertise in the area of corporate governance of IT, Standards Australia has been appointed secretariat and convenor of a new international working group to drive development and harmonisation of International Standards on corporate governance of IT.

A resolution to establish the working group was approved at the 23rd meeting of ISO/IEC Joint Technical Committee for Information Technology (JTC1) in Nara, Japan on 18 November, 2008.

Reporting directly to JTC1, the primary role of the new working group will be to develop Standards and related documents to assist business leaders with the corporate governance of their IT systems and networks.

Key tasks will include the standardisation and harmonisation of IT terminology and the ongoing maintenance of ISO/IEC 38500, which as previously mentioned is based closely on the Australian Standard for Corporate Governance of Information and Communication Technology (AS 8015:2005).

Background to JTC1

JTC1 is a joint effort between ISO and the IEC and is responsible for the development of International Standards for computer-related areas. Key areas of work include IT security, IT governance and harmonisation of IT terminology.

Standards Australia Committee IT-030 ICT Governance and Management first initiated a work program focusing on ICT governance and management in 2002. AS 8015 was published in 2005 and attracted international attention. It was the first Standard to deal with corporate governance of IT and it set new benchmarks in ICT governance best practice and professionalism.

In June 2008, the ISO/IEC published ISO/IEC 38500 which is based closely on the Australian Standard, with minor changes. Both Standards set out six principles for good corporate governance of IT.

AS 8015:2005

The AS 8015:2005 standard for *corporate governance of information and communication technology* was published in 2005 by Standards Australia. The standard provides principles, a model and vocabulary as a basic framework for implementing effective corporate governance of ICT within any organisation. The committee which drafted and recommended the publication included representatives from the Australian Computer Society, The Australian Bankers Association, the Australian Institute of Company Directors, Academia and Government Agencies.

AS8015 was submitted for fast track ISO adoption and published largely unchanged, in May 2008 as ISO/IEC 38500, as a standard for corporate governance of information technology, which is further elaborated on below.

ISO/IEC 38500:2008

As we are aware, most organisations use IT as a fundamental business tool and few can function without it. IT is also a significant enabler in the future business plans of many organisations. ISO/IEC 38500 will help the governing body to evaluate, direct and monitor the use of IT. It will also assist directors in assuming conformance with obligations – regularly, legislation, common law and contractual obligations concerning the acceptable use of IT and to have a proper corporate governance of IT.

ISO/IEC 38500:2008, Corporate governance of information technology, is applicable to organisations of all sizes, including public and private companies, government entities and not-for-profit organizations. The standard will provide a framework for effective governance of IT to assist those at the highest level of organisations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organisations' use of IT.

The framework comprises definitions, principles and a model. It sets out six principles for good corporate governance of IT that express preferred behavior to guide decision making:

1. Responsibility;
2. Strategy;
3. Acquisition;
4. Performance;
5. Conformance; and
6. human behaviour.

The purpose of the standard is to promote effective, efficient, and acceptable use of IT in all organisations by:

- assuring stakeholders that, if the standard is followed, they can have confidence in the organisation's corporate governance of IT;
- informing and guiding directors in governing the use of IT in their organisation; and
- providing a basis for objective evaluation of the corporate governance of IT.

The standard is targeted at the Board of an organisation, to assist the Board in delivering the maximum value from IT and information assets across the organisation.

The standard is aligned with the definition of corporate governance that was published as a Report of the Committee on the Financial Aspects of Corporate Governance in 1992, also known as the Cadbury Report. The Cadbury Report provided the foundation



definition for the Organization for Economic Cooperation and Development's Principles of Corporate Governance.

ISO/IEC 38500:2008, *Corporate governance of information technology* was developed by the joint technical committee ISO/IEC JTC1, *Information technology*, subcommittee SC 7, *Software and systems engineering*.

National and International Activities in Information Security Management and Privacy Principles

Standards Australia is playing an important role in developing infrastructure security standards.

There are a myriad of information security management standards and standards covering privacy matters. A subset of these is detailed below.

Information technology — Security techniques — Information security risk management ISO/IEC 27005:2008

This International Standard is designed to assist the satisfactory implementation of information security based on a risk management approach.

This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organisation's information security.

Information Technology – Security Techniques - A privacy framework	ISO 29100	Not Yet Published - At Committee Draft Ballot Stage
Information technology -- Security techniques -- A privacy reference architecture	ISO 29101	Not Yet Published - At Working Draft Stage
Health informatics - Information security management in health using ISO/IEC 27002	ISO 27799-2008	2008
Health informatics - Information security management in health using ISO/IEC 27002	ISO FDIS 27799	2008
Information technology - Security techniques - Information security risk management	ISO IEC 27005-2008	2008
Information technology - Security	ISO IEC FDIS	2008



techniques - Information security risk management	27005	
Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	ISO IEC 27006-2007	2007
Information technology - Security techniques - Code of practice for information security management	AS NZS ISO EC 27002-2006	2006
Information technology - Security techniques - Code of practice for information security management	AS NZS ISO IEC 27002-2006	2006
Information technology - Security techniques - Information security management systems - Requirements	AS NZS ISO IEC 27001-2006	2006
Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	ISO IEC FDIS 27006	2006
Information technology - Security techniques - Code of practice for information security management	ISO IEC 27002-2005	2005
Information technology - Security techniques - Information security management systems - Requirements	ISO IEC 27001-2005	2005

IT Governance and Green Sustainability

As we are aware, ICT has a substantial impact on carbon emissions with 2% of carbon emissions coming from the ICT sector and ICT devices comprise an increasingly large proportion of the world's waste.

As such Standards Australia promotes sustainability and undertakes all efforts to produce standards which assist the nation and indeed the world, to reduce carbon emissions.

Standards Australia has therefore developed a range of standards which deal with reducing the carbon footprint from:

- eWaste;
- road transport;



- videoconferencing technologies; and
- reducing green house gases to name a few.

Standards Australia is also working on and has completed several initiatives to reduce the impact of digital economy device and infrastructure. One of these is involving 'green' buildings and sustainability in building construction. A selection of relevant standards and related documents in this area is detailed below.

Sustainability in building construction - General principles	ISO 15392	2008
Sustainability in building construction - General principles	ISO FDIS 15392	2008
Sustainability in building construction - Environmental declaration of building products	ISO 21930-2007	2007
Sustainability in building construction - Environmental declaration of building products	ISO FDIS 21930	2007
Sustainability in building construction - Framework for methods of assessment for environmental performance of construction works - Part 1: Buildings	ISO TS 21931-1-2006	2006
Sustainability in building construction - General principles	ISO DIS 15392	2006
Sustainability in building construction - Sustainability indicators - Part 1: Framework for development of indicators for buildings (Technical Specification)	ISO TS 21929-1-2006	2006
General guidelines on the verification, validation and assurance of environmental and sustainability reports (Technical Specification)	AS NZS 5911(INT)-2005	2005

Standards Australia is also heavily involved in energy efficiency and performance. Another area we are working on is in relation to smart meters. We realise that monitoring energy use and demand could assist in addressing climate change. Smart meters can provide major benefits for consumers, empowering them to take control of their energy bills by providing them with better information, new choices in off-peak pricing to save money and new services to manage appliances and increase their energy efficiency.

In fact, there is currently significant international activity on this topic in the standards arena. The technical committee ITU-TSG12 are continuing work on the Home Area Network System (HAN) to develop a single international standard for home networking transceivers using any metallic media in the home – phoneline wiring, data cable (e.g. CAT 5), coaxial cable or powerline wiring.



Household connectivity is growing rapidly with more and more electronic devices and networks within the home distributing and using digital information and media. In addition, remote control of lighting, heating, appliances, remote metering and security systems attached to the home are making the digital home a reality.

International standards that enable interoperability and security in the field of home networking are seen as key to bring value and versatility to consumers, making possible the use of diverse products, services and sources, and therefore accelerating market development.

Standards Australia is involved in consultation with committees such as the one above. We are also taking a proactive response to the sustainability issue across all industry sectors as and we would be more than happy to engage with government on this issue.

Digital Forensics Standard in Development

Digital forensics addresses data after a crime has been committed, reconstructing it to help understand how an attack occurred so that defences can be adjusted. Digital forensics also relates to legal evidence found in computers and digital storage mediums and the management of digital data for courtroom evidence. Digital courtroom evidence can span cases such as sexual harassment, criminal violations, child pornography possession, tracing the origin of virus attacks and other security breaches.

An international digital forensics study group has been set up to address these issues and Australia is involved among other countries such as South Africa, New Zealand, the USA, Luxembourg, South Korea and Spain.

This international approach is needed as many digital forensics cases cross borders. For example, a money launderer living in South America, using servers in China to spam, solicit and use bank accounts in New Zealand.

The writing of a new digital forensics standard is timely, as the requirement for digital evidence has increased globally. Standardisation will provide consumers with the ability to assess their professional forensic supplier – improving their consistency and confidence in services.

The international digital forensics study group is investigating the possibility of additional standards or guidance for IT governance. The group will review existing standards and work with other international standards bodies – and will take into account any relevant developments in the area of corporate governance for digital forensics.

A report by the group, including recommendations on further international standards for IT governance, will be presented to the ISO Plenary in May 2009, which will lead the way for further development work.



Conclusions

IT is essential to manage the transactions, information and knowledge necessary to initiate and sustain economic and social activities. In most enterprises, IT has become an integral part of the business and is fundamental to support, sustain and grow the business.

It is the goal of Standards Australia and its underlying technical committees to understand and manage the risks and constraints of IT and produce standards to assist in creating and maintaining successful enterprises.

Standards Australia is proud of its work to date in the field of IT Governance standardisation and the role it has played in contributing to international IT Governance standards.

Standards Australia looks forward to working collaboratively with State and Commonwealth agencies, organisations and industry groups towards utilising these standards as a benchmark for best practice.

Standards Australia appreciates the opportunity to participate in this consultation process.