AIIA Representation at Standards Australia

Nominee report – Geoff Clarke

Status report – May 2021

Contents

Introduction 1
Artificial Intelligence 2
Information Security, Cybersecurity and Privacy Protection 3
IT Service Management and IT Governance 4
Cloud Computing and Distributed Platforms 5
Governance of Organizations 6

Introduction

The AIIA nominates several experts to collaborate on national and international standards to ensure such standards are of value to Australia, its people and AIIA member organizations.

Geoff Clarke, an employee of Microsoft Australia, is one such expert and represents AIIA on various Standards Australia committees as outlined below:

Standards Australia Committee	**International Equivalent**	**Description**
IT-012	ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection
IT-030	ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance
IT-038	ISO/IEC JTC 1/SC 38	Cloud Computing and Distributed Platforms
IT-043	ISO/IEC JTC 1/SC 42	Artificial Intelligence
JTC 1 SAC	ISO/IEC JTC 1	Information Technology
QR-017	ISO TC 309	Governance of Organizations

This report is a summary of the activities and current status of that representation.

Standards Australia is the country's leading independent, non-governmental, not-for-profit standards organisation. Its committees work with government, industry and academia to develop national, joint Australia/New Zealand, and international standards. As Australia's National Body member in ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), Standards Australia's committees help ensure that Australia's needs are included in international standards. Such standards offer guidance and, in many cases requirements against which organizations can receive certification of conformance through independent audits.

The usual practice of the international standards committees is to conduct many virtual meetings (using Zoom) throughout the year and meet in person every six months. However, for the past year, all meetings have been virtual.

Artificial Intelligence

ISO/IEC JTC 1/SC 42 has 47 national body members, 8 published ISO standards, and another 22 standards in progress. It covers topics relating to Artificial Intelligence and data used in AI.

Australia is well represented in SC 42 with members of industry, government and academy all providing significant input.

Of particular interest to Australia and the AIIA are the following ISO/IEC projects:

DIS 22989 Concepts and terminology

- This standard provides the basic terms and concepts of AI – and has been the subject of much debate (including long discussions of the definition of AI)
- Currently in Draft International Standard (DIS) stage

DIS 23053 Framework for artificial intelligence (AI) systems using machine Learning (ML)

- Another 'foundational standard', this standard is also in DIS stage.

20547 Big data reference architecture

- This is a multi-part project that was originally separate to the AI sub-committee but has now been included because of the requirement of large datasets for much of the work of AI. It is the subject of continuing work, with many parts already published.

5259 Data quality for analytics and ML

- This relatively new 4-part project includes terminology, data quality measure, management requirements and other topics to help improve the quality of the resulting machine learning models.

TS 6254 – Explainability of ML models and AI systems

- This technical specification will offer guidance on objectives and approaches for explainability so people can understand more about the resulting predictions from AI systems.

CD 23894 AI – Risk Management

- This is an extension of *ISO 31000 Risk Management – Guidelines* to give guidance on risk management for AI systems.

TR 24027 Bias in AI systems and AI aided decision making

- This Technical Report is nearing completion.
- It describes how to account for unwanted bias in data, algorithms and decision making

TR 24028 Overview of trustworthiness in artificial intelligence

- This Technical Report was recently published and is a summary of many of the "trustworthiness" topics across SC 42 projects. It briefly surveys the existing approaches that may assist trustworthiness in technical systems and discusses their potential application to AI systems.

24029 Assessment of the robustness of neural networks

- This two-part project looks at statistical, formal and empirical methods to extend software validation methods to the new challenges of AI. Part 1 has been published.

TR 24368 Overview of ethical and societal concerns

- This document provides a high-level overview of the programme of work in SC 42 in the area of ethics and societal concerns relative to Artificial Intelligence (AI) systems and applications. It provides information in relation to principles, processes and methods in this area, and does not intend to advocate for any specific set of values (value systems).

38507 Governance implications of the use of Artificial Intelligence by organizations

- This is standard is the only project in the Joint Working Group between SC 42 and SC 40 (see below).
- It is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of information technology – including the use of artificial intelligence.
- Currently in the Draft International Standard stage.

Information Security, Cybersecurity and Privacy Protection

ISO/IEC JTC 1/SC 27 has 80 national body members, 210 published standards, and another 82 projects in progress. It covers topics including security controls, application security, incident management, privacy, identity and encryption.

SC 27 has a huge programme of work, but of particular interest to Australia and the AIIA are the following ISO/IEC projects:

27002 - Code of practice for information security controls

- This is part of the 27000 series of standards about Information Security Management Systems.

- This is in the process of being revised – currently in the Draft International Standard stage. For example, adding 'themes' to controls for greater clarity.

27014 - Information security governance

- Aligning this standard with governance topics from other subcommittees helps the governing body understand the ISMS and what the organization should expect from it.
- This was published in 2020.

27034 – Application security

This is a large 7-part family of standards that describes the security development lifecycle.

27035 – Information security incident management

This 4-part family of standards outlines the organizational structures and processes for managing security incidents. Part 3, which describes principles of incident management, was published in 2020. A new part on coordination across organizations is currently underway.

27701 – Privacy information management

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This was published in 2019 and is used to formalize privacy management within an organization. It can be mapped to various privacy regulations including GDPR and the Australian privacy laws. The Standards Australia committee is working to adopt the international standard by adding annexes that map the standard to Australian and New Zealand privacy laws.

15408 Evaluation criteria for IT security

- This 5-part standard includes methodology for IT security evaluation, functional and assurance components and pre-defined packages of security requirements.
- It is in Draft International Standard (DIS) stage.

IT Service Management and IT Governance

ISO/IEC JTC 1/SC 40 has 57 national body members, 25 published ISO standards, and another 9 standards in progress. It covers topics including Governance of IT, IT Service Management and Business Process Outsourcing.

Note that Australia holds the Chair and Secretariat for SC40.

Of particular interest to Australia and AIIA are the following ISO/IEC projects:

38500 – Governance of IT for the organization

- This is the 'cornerstone' standard of the governance of IT and is based on previous Australian standards.
- It is in the process of being extensively revised.

38503 – Assessment of the Governance of IT

- This project, largely driven from Japan and South Africa, is the subject of many comments from the Australian delegation as we believe it needs more work. Currently in the DIS stage.

38505 – Governance of Data

- This is a 3-part project, that provides guidance on the strategic nature of data for boards and management. Parts 1 and 2 have been published, with part 3, on data classification, currently in progress.

38506 - Governance of IT enabled investments

- This document has now been published
- Note that Trish Kenyon (AU) is the editor

38507 - Governance implications of the use of Artificial Intelligence by organization

- This standard has been assigned to a Joint Working Group with SC42 (See above)

38508 – Governance of the use of shared digital service platform

- This is a new project

20000-13 Guidance on the relationship between ISO/IEC 20000-1:2018 and service management frameworks: COBIT

- 20000 is management system standard series with 13 parts (though some have been withdrawn). It is used by organizations seeking to use services or to provide services themselves. It covers requirements such as plan, establish, implement, operate, monitor, review and improve a service management system.
- This part describes the relationship between this series of standards and ISACA's Cobit framework for IT governance and management.
- A practical Guide to 20000 has been produced. More details can be found at https://www.iso.org/news/ref2459.html

30105 IT enabled services – Business Process Outsourcing lifecycle process

- This is an 8-part series of standards, most of which are now available
- The topic of Part 8 is Continual Performance Improvement and this topic is also the subject of other related standards in SC40.

Cloud Computing and Distributed Platforms

ISO/IEC JTC 1/SC 38 has 49 national body members, 22 published standards, and another 7 standards in progress. It covers topics including cloud computing definitions and architecture, service level agreements, interoperability, portability, data flow and use statements.

Of particular interest to Australia and AIIA were the following ISO/IEC projects:

19944 Cloud services and devices: Data flow, data categories and data use:

- Now split into two parts, this standard outlines data usage statements and how they explain the categories of data and their intended use

22123 Cloud Computing Concepts and Terminology

- Originally, the "delta" from the original work of 17788/17789 on the core concepts and reference architecture of cloud computing, this project has now split into two standards, with a third part likely to be started on reference architecture. Cloud computing has changed significantly since the 2014 concept standards.

5140 Concepts for multi-cloud and other interoperation of multiple cloud services

- As cloud service customers increasingly use services from multiple cloud service providers, explaining the concepts and interoperation of these services becomes important.

5928 Taxonomy for digital platforms

- This technical specification, currently in development, outlines the different types of 'platforms' that exist – both from an economic and technical perspective.

7339 Overview of platform capabilities type and platform as a service

- The different "something-as-a-service" approach to explaining cloud computing is becoming less relevant as the various cloud capabilities morph into different forms. This technical specification aims to examine this topic.

TR 23187 - Interacting with cloud service partners (CSNs)

- This Technical Report, published in 2020, describes the relationships between cloud service providers, customers and cloud service partners.

23751 - Framework for Data Sharing Agreement (DSA)

- Led by the US, this project describes how to set up data sharing agreements and in particular, data lake options for industries where industry-wide data is useful, but data from individual organizations is confidential.
- Currently in Draft International Standard stage.

Governance of Organizations

ISO TC 309 has 77 national body members and many liaison organizations including OECD, the International Integrated Reporting Council and the World Business Council for Sustainable Development. It has 2 published standards (on Anti-Bribery and Compliance Management), with 3 more under development. Its scope is the standardization in the field of governance relating to aspects of direction, control and accountability of organizations.

The following projects are of interest to Australia and AIIA members:

37000 Guidance on the governance of organizations

- This project is in the Final Draft International Standard stage and describes the principles, practices and framework on organizational governance.

37001 Anti-bribery management system

- Published in 2016, this standard allows organizations to certify their anti-bribery management system.

37002 Whistleblowing management systems – Guidelines

- This standard describes how to establish and operate a whistleblowing system within the organization. Australia has had significant input to this work which is currently in the Final Draft International Standard stage.

37003 Anti-fraud controls

- This is a relatively new project that is progressing slowly.

37301 Compliance management systems – requirements with guidance for use

- This is a "requirements" version of a previous standard, 19600, and therefore can be the subject of audit and possible certification. It has now been published, so 19600 has been superseded.

This report was prepared by Geoff Clarke (geoc@microsoft.com). May, 2021.