

Standard issue

Thanks to Standards Australia, managers will be able to express their requirements of ICT with confidence, writes Kevin Fitzgerald.



Standards Australia has just published for comment its much anticipated 'Corporate Governance of Information and Communication Technology' draft standard. The purpose is to assist senior officers of organisations in meeting their legal and organisational obligations. In particular, it will assist in improving the risk management of ICT, establish confidence in an organisation's corporate governance of ICT, and develop effective and efficient use of ICT.

The standard will be of great interest to directors, partners and shareholders, as well as ICT management, middle management, external advisers, vendors and auditors. It highlights the performance expected of ICT. It provides a vocabulary that will help non-ICT-literate management at all levels to express their requirements with confidence. It will also telegraph to ICT management any new levels of discipline required to satisfy business expectations.

ICT is the largest budget item for most organisations. In the beginning, management struggled with the jargon, the

high cost, and the ever-present failures and threats to security, which have continued to trouble ICT for decades now. Amazingly we have seen the technology reinvent itself time and again. And every time it brought with it a new promise of better performance. Yet nothing has changed. We still have the jargon, the high cost, the failures, and the uncertainties about security.

Perhaps it has been the technology gap between business management and ICT management, or even the age gap, but ICT has had a dream run over the last three or more decades in terms of delivering to expectations. No doubt this has been aided by a lack of rigour from senior executives who simply do not know what questions to ask of ICT. From both the ICT and the senior executive side there has been a lack of accountability, stewardship, leadership, control and monitoring in relation to ICT performance. Perhaps such gaps have been closed a little in some larger organisations of late, but for most organisations there is still

a lack of effective governance over the ICT environment.

When finalised, the ICT governance standard will provide the ammunition for both ICT and business management to operate with much higher levels of accountability, stewardship, leadership, control, and monitoring.

The draft standard lists seven valuable principles of sound ICT governance:

- 1 Establish clearly understood responsibilities for ICT.
- 2 Plan ICT to best support the organisation.
- 3 Acquire ICT validly.
- 4 Ensure that ICT is of the required quality.
- 5 Ensure that ICT performs when required.
- 6 Ensure that ICT conforms with formal rules.
- 7 Ensure that ICT use respects human factors.

Each of the principles above are accompanied by a specific checklist, which arms all managers involved with a clear line of inquiry on matters ICT.

This assistance will give more power to all managers in relation to improving not only the delivery from ICT but also the security aspects that this column is focused upon.

For instance, principle 4 in the above list in effect asks: 'Are there arrangements in place to ensure the availability of information services at all times required by the business? Are the ICT resources safe from natural hazard? Are the data holdings secure from attack or theft or misuse in storage and in transmission? Are there tested plans for ensuring business continuity after failure of public utilities, natural disasters or human attack?' Such questions are aimed at proactively evaluating and monitoring the risks to the integrity, confidentiality and availability of all information in the care of ICT.

Principle 6 asks: 'Is conformance with external regulation, such as privacy or financial

fidelity legislation, monitored?' And principle 7 asks: 'Are there policies in place to govern the use of key ICT resources?'

This draft standard (freely available at <http://www.standards.com.au/catalogue/script/details.asp?DocN=MSWD04198ATCRD>) is just the beginning. Comments will be reviewed and a final standard published. Following this we can expect to see additional related standards implementation guides, and supplementary reading materials emerge.

Already, one such book has been published by Infonomics (www.infonomics.biz), entitled *The Director's IT Compass* by Steve Moir and Mark Toomey.

This book poses the question: 'Why do we still hear that information technology is inflexible, that the products of expensive IT projects remain unused, and that IT systems are threats to corporate survival?' It addresses these vital issues by tracing the IT management lifecycle: strategy, plan, deliver, and operate. Each section contains explanations around the lifecycle stage under the headings of characteristics, symptoms, and remedies, and finishes with a dozen hard questions for directors to raise.

Like the emerging standard, this powerful little book empowers the board room by arming it with ICT understanding and language. It empowers management to clearly telegraph business expectations. In this way, the level of debate and resultant performance can be expected to improve in those organisations wise enough to take ICT governance to heart. □

KEVIN FITZGERALD
is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.
kevinfitzgerald@ozemail.com.au