The Infonomics *Letter*
Plain Language about Digital Leadership and Governance of Information Technology
March 2013 Edition

Breakthrough!

Hello and welcome to The Infonomics Letter on Digital Leadership and Governance of IT for March 2013.

It's been five long years since ISO 38500 was signed off for publication as an International Standard, and eight years since the original AS 8015 was published.

We saw Sir Peter Gershon reference AS 8015 in his landmark review of the Australian Government's use of IT and thought that would mark the first major adoption – but we are still waiting in that space.

Several nations have adopted ISO 38500 as a national standard. There have been spurts of interest in the guidance it offers from all over the world, but none of that has resulted in a major move to adoption. We know of organisations (we helped some) that use the standard to guide their own activities, but none of them will talk about it because it gives them a competitive advantage. A while ago, I found a small consulting company which has built its methodology around ISO 38500. More recently, I've come across independent consultants who use ISO 38500 and my book, Waltzing with the Elephant, to help their clients. One of them wrote a very nice endorsement for me on LinkedIn recently.

Then the Victorian Government adopted a new ICT strategy which mandates best practice governance of IT and mentions ISO 38500 in the same sentence. Perhaps this is a pointer to widespread adoption of the standard in Australia. But now we have discovered that South Africa is months ahead of Victoria! In what I believe is an immense breakthrough, the Government of South Africa has adopted and will implement, throughout government, a new model for governance of IT that has ISO 38500 at its core. There's an extensive review of the published material in Clear, Specific Instruction.

Boardroom Skills tells of a plea for help from an academic researcher. We look at the potential negative impact of poor and outdated advice for directors about how they can govern the use of IT.

Strategy South Australia announces the opportunity to comment on a new draft IT strategy for the state.

Extended Reach announces that our Questions for Directors are being republished by a highly respected international journal.

Remember the Queensland Health Payroll debacle? The Commission of Inquiry is under way!

Don't miss your opportunity for Developing Digital Leadership and Governance Skills.

Best wishes to those celebrating Easter and Passover. Until the end of April – enjoy!

Mark Toomey 28 March 2013

Clear, Specific Instruction

The South African Government, under the authority of the Cabinet and through the Department of Public Service and Administration, has issued a directive requiring "Implementation of the Corporate Governance of Information and Communication Technology Policy Framework in the South African Public Service.

This announcement is a major breakthrough for advocates of ISO 38500. Not only does the directive explicitly require all agencies to adopt ISO 38500, it also accurately positions the standard in the context of overall corporate governance and the widely used framework for IT Management processes, COBIT.

The directive and three key supporting documents are readily accessible at the DPSA web site. They reflect a deeply considered and rational set of instructions to the political and executive leadership of government in South Africa, at the climax of a journey which began as early as 1998. It was then that the Presidential Review Commission identified a *"poor culture of good governance, lack of political and strategic leadership of ICT, and that ICT is not being viewed on the same strategic level as other resources…"*. Clearly, corrective action arising from that review and specific instruction given in a Cabinet Memorandum issued in 2000 were ineffective. Reports by the Auditor General of South Africa since 2008 have highlighted *"a significant weakness in the governance of information technology in the public service"*. In 2011, only 21% of departments had any arrangements for Governance of ICT, and these were not sustainable and lacking engagement of senior management. The directive therefore addresses a clearly stated concern that: *"the value of ICT as an enabler of service delivery will not be realised without incorporating Governance of ICT in the corporate governance regime of a department"*.

Explicit Responsibility

The directive is wonderfully clear and specific. It begins by confirming responsibility for ICT, using language that comes directly from core messages embedded in ISO 38500:

"It is the responsibility of the head of department that the acquisition, management and use of information technology by the department improves:

(a) direct or indirect service delivery to the public, including, but not limited to, equal access by the public to services delivered by the department;

(b) the productivity of the department; and

(c) the cost efficiency of the department".

Imagine that – the head of the department is responsible for the acquisition, management and use

of ICT. In the business world, that's the CEO. There's no ambiguity. And just in case the department heads don't like the idea, the directive continues with a demand for accountability: *"departments are required to annually report to the Department of Public Service and Administration"* using a prescribed assessment standard. Non-conformance is clearly sanctioned as well – the directive concludes with a reference to Section 16A of the Public Service Act (no, I haven't read it yet, but given the directness of the rest of the documents, it's not hard to imagine what it says).

Governance Framework

Along with the directive, South African Public Service Agencies have been given a framework for Corporate Governance of ICT, developed by DPSA. This 37 page document is written in very clear, precise and explicit language that appears intended for use by the Head of Department as well as personnel working at lower levels.

It contains the result of what must have been a substantial effort to properly understand not just ISO 38500, but the interplay of three key guiding documents – the King III code for Corporate Governance in South Africa, ISO 38500 and COBIT 5. It's well worth reading, but for the time-poor, I've summarised and commented on it as it is laid out.

Governance Context

Legislation gives the Minister of Public Service and Administration ultimate responsibility for governance and management of ICT in South Africa. Regulations require those at the top of each department to prepare and be responsible for plans. Identified problems with ICT however reflect a lack of involvement of top management.

Proper Corporate Governance of ICT requires that all important decisions *"should come from the senior political and managerial leadership and not be delegated to ICT management"* – thus enabling alignment between ICT services and departmental strategy. *"Corporate Governance of ICT is a continuous function that should be embedded in all operations of a department, from Executive Authority and Executive Management level to the business and ICT service level".* This is wonderful scene-setting – it readies the reader for a message coming in subsequent pages – that Governance of ICT is a system that engages throughout the organisation.

Purpose, legislative context, scope, and audience

South Africa clearly enjoys a useful framework for managing its machinery of government, The Public Service Act of 1994 establishes the Minister for Public Service Administration to *prescribe uniform norms and standards for electronic government*. Having observed attempts at centralised control of government ICT in Australia and other nations, one might have expected that the DPSA in South Africa might have attempted to become the controlling authority for ICT in all agencies – prescribing and controlling the use and delivery of ICT. However, this is not the case, and evidently never has been. Instead of prescribing solutions which may or may not work, the DPSA is positioned in this directive as requiring effective governance in which departments will make sound decisions in their own right. It's a very sensible move – instead of trying to boil the ocean, the plan is to have numerous well-managed kettles boiling just what is required for its environment – be it water, oil or something else!

Variability in purpose, scale and other characteristics between departments is addressed by an expectation that departments will *"develop their own system for Corporate Governance of ICT by adopting the principles and practices put forward in this Policy Framework"*. This is important. The framework prescribes some aspects of the system – mainly elements that are essential to making it work – but leaves much of the detail open so that departments can implement arrangements that work for them.

Key Drivers

South Africa has identified a political mandate for its use of ICT. This mandate is anchored in 12 outcomes (effectively, goals for the nation) and an ICT House of Value model (a table in the document shows how the ICT House of Value maps to the 12 outcomes).

From these complementary anchors political and executive level leadership identifies strategic direction and goals which then feed into the individual department arrangements for Governance of ICT. In essence, this is highlighting a key point in ISO 38500, that Governance of ICT includes setting the strategy for use of ICT. The Policy Framework document emphasises at this stage, and on several subsequent occasions, that: *"All ICT decisions of importance should come from Senior Political and Managerial Leadership and should not be delegated to technology specialists"*; and *"the management of information should be carried out on the same level as the management of other resources such as people, finance and material in the public service"*. However, it also recognises that despite this philosophy being established more than ten years ago, it has not been taken up as intended. As part of the subsequent investigation, South Africa has found that creation of a Government Information Technology Officer (GITO) role has not been effective, and that many GITOs are *"not functioning as strategic managers largely due to inadequate accountability structures"*.

Fundamentals for Governance of ICT

The Policy Framework identifies ICT as "an enabler of public service delivery". It goes on to say: *"Political and Executive Management leadership of departments need to extend Corporate Governance, as a good*

management practice, to ICT. This should be done by evaluating the current business strategic goals and future use of ICT, by directing the preparation and implementation of plans to ensure that the use of ICT meets business needs which, when implemented, must be monitored for performance and conformance purposes to ensure that the departmental strategic goals are achieved". This paragraph is significant – it embodies the core of ISO 38500 and accurately positions the three tasks for Governance of ICT set out in the standard – Evaluate, Direct and Monitor. The instruction in the framework goes on to insist that: *"Executive leadership and management should understand the strategic importance of ICT and should assume responsibility for the Corporate Governance of ICT and place ICT on the strategic agenda".* It then identifies

Benefits of Governance

It's pointless doing anything that doesn't deliver beneficial outcomes, directly or indirectly. ISO 38500 identifies a range of potential benefits arising from good Governance of ICT, and the South Africa's Policy Framework builds on that list. The list of 18 benefits includes:

- improved delivery on 12 strategic outcomes;
- improved achievement of strategic goals;
- more effective delivery of public services;
- better use of ICT as a business enabler;
- improved return on ICT investment;
- improved management of business-related ICT projects;
- improved management and use of information.

Foundation Guidance

When South Africa first tried to establish good Governance of ICT in 2000, there was little formal guidance available. Now, the Policy Framework is informed by three complementary works: The King III Code, ISO 38500 and COBIT. The document sets out the relationship between these, emphasising that the King III guidance includes explicit discussion of how and why governing bodies should pay attention to ICT. It positions King III and ISO 38500 as together providing the relevant guidance for the political and executive leadership of each department, and then positions COBIT as a process framework.

One aspect of the guidance is curious. It makes a distinction between two related concepts: "Corporate Governance of ICT" and "Governance of ICT". It is clear from reading that "Corporate Governance of ICT" is what happens at the top level – the political and executive leadership level – while "Governance of ICT" is what happens in the lower levels of the management space and is subject to Corporate Governance oversight. It's intriguing that the framework doesn't refer to this as the management layer, as this would be more accurate. Indeed in one sentence, it does say that Governance of ICT is *"The efficient and effective management of ICT service delivery".* However, it must also be said that the framework also identifies an "operational management" layer which is guided by what it calls "operational frameworks" such as ITIL (service management) and ISO 27000 (information security). It seems that it is regarding the "higher level" of management decision-making as governance, which is consistent with the views expressed by many COBIT aficionados, but which can still be confusing for the non-IT specialist, simply because no other aspect of business management uses the same distinction.

Governance Layers and Model

Section 11 in the Policy Framework briefly reviews overall Corporate Governance in the public service, positioning it as the key to creating value for each department's stakeholders. Importantly, it identifies that Corporate Governance is a system which includes all the means and mechanisms that enable the department's Executive Authority, Head of Department and Executive Management to have a structured say in evaluating elements leading to identification of strategic goals and measures, directing execution of strategic goals to realise value and monitoring attainment of the goals. It's interesting to note that, while the discussion here is focused on the overarching Corporate Governance, as we would see in the boardroom of any significant business enterprise, the three tasks are identified using key words from ISO 38500 – Evaluate, Direct and Monitor. It becomes quite clear that the people who devised this framework really do understand corporate governance and the positioning of ISO 38500.

The discussion of Corporate Governance continues by pointing out that it is also concerned with individual accountability and responsibilities, and with directing and controlling the organisation, management and policies of the organisation. It also presents a model for Corporate Governance which is remarkable in its synergy with the model that is used in ISO 38500, and the expansions on that model that I have developed in my work subsequent to publication of the standard. It also includes an element that has been a concern in debate about companion documents to ISO 38500 addressing the locus of authority and accountability for Corporate Governance. The framework places the locus of authority and accountability with what it calls the "Executive Authority Ownership / Leadership" – where "Executive Authority is a defined term meaning, according to context, the President, Minister, Premier, Commissioner and in some cases, members of an Executive Council". In corporate equivalent terms, these entities would be the owners, and where in government the specific details are contained in Acts, the corresponding corporate equivalent would be the constitution, articles of incorporation and like documents.

The model for Corporate Governance used in the Policy Framework resolves a weakness (which I explained in my book, Waltzing with the Elephant) in the model originally used for ISO 38500. In that model, governance oversight was depicted as being applied to "business process". That's inadequate – governance oversight applies to much more than the business process – it also deals with every other aspect of management. In the South Africa model, governance oversight is applied to Management Business Execution, as well as the Organisation Value Chain and Infrastructure. Intriguingly, the model does not specifically identify development of new and improved business capability, which is one of the primary areas of concern for Governance of ICT. On the other hand, it identifies a series of six topics in the management space subject to governance oversight: organisation structure, information, people, process, technology and finance. Four of these – structure, people, process and technology – are aspects of the Leavitt Model for organisational change, published in 1964. Their inclusion suggests that, while the diagram may stand some minor improvement, the authors clearly understand the issues in Governance of ICT-enabled business change.

Section 12 drops down a level, to describe Corporate Governance of ICT in the Public Service. It restates in the clearest possible terms the responsibility (as necessary to confirm with the first principle in ISO 38500) of the Executive Authority (political leadership), the Head of Department (strategic leadership and accountability for implementing Corporate Governance of ICT) and Executive Management (ensuring that Corporate Governance of ICT works). The Head of Department and Executive responsibility and accountability is further detailed in a list of 7 points that broadly correspond to the expectations of the ISO 38500 model and principles.

While the Policy Framework does allow departments freedom in the detailed design of their arrangements for Corporate Governance of ICT, it does identify some essential elements of the system. It expects the system to be based on the framework provided, and to include principles, practices and policies for governance, clear sponsorship, clear statements of roles and responsibilities, decision making structures, processes and practices. Clearly, each department will have quite a deal of work to do, not just to establish its governance model, but to integrate it into the fabric, culture and capability of the department.

Corporate Governance of ICT Objectives

Section 13 is brief. It sets out seven objectives, of which four are focused on ensuring that there is in fact a system for Governance of ICT. This includes ensuring that the Government Information Technology Officer (GITO) role is an integral part of executive management – as was intended when the role was introduced, but clearly not achieved. It also includes mandatory use of COBIT for the next layer, which the Policy Framework refers to as "Governance of ICT" but which in reality is the upper layer of management decision-making. Information elsewhere in the documents shows that this is the third time that South Africa has attempted to introduce COBIT for management of ICT. The key difference in this attempt is that implementing COBIT comes after implementing the ISO 38500 layer for "Corporate Governance of ICT". It means that there will be a supervisory context to follow up on the implementation, and it means that essential behaviours should begin to be inculcated at the executive level, easing the task of adding process rigour and transparency.

Three of the points listed in the Objectives section relate to business outcomes. Strategic alignment leading to business value is at the top of this list, backed by provision of the ICT capabilities needed to deliver what is required, and an ability to deliver sustained performance and conformance.

Corporate Governance of ICT Principles

Both ISO 38500 and the King III Code establish principles for good Governance of ICT. Annexure A to the Policy Framework maps the relationship between the six ISO 38500 principles and the seven principles in King III. This mapping evidently forms the basis of the adopted seven principles for Corporate Governance of ICT set out in section 14. They are (paraphrased):

1 Political Mandate – Governance arrangements must deliver on the department's political mandate;

2 Strategic Mandate – Governance arrangements and the Head of Department must deliver on the department's strategy;

3 Corporate Governance of ICT – Head of Department responsible for enabling the governance arrangements;

4 ICT Strategic Alignment – Requires that Executive Management ensures alignment and that the business accounts for current and future capabilities of ICT.

5 Significant ICT Expenditure – Executive Management must ensure expenditure is for valid business reasons and must monitor and manage benefits, opportunities, costs and risks;

6 Risk Management and Assurance – Executive Management must ensure that ICT risk and audit are managed in line with departmental practice;

7 Organisation Behaviour – Executive Management must ensure that ICT use demonstrates understanding and respect for behaviour and culture.

There is a great deal of emphasis in these principles on the role of executive management. Given past failure in efforts to establish effective governance of

ICT, it seems that the executive engagement has been identified as the weakness, and considerable attention is being given to ensure that the executive does engage in an effective and positive manner. There is a risk associated with this approach – the principles may not be giving enough attention to other aspects of good governance and they may have been narrowed too much by focusing them on the executive. The ISO 38500 principles are the product of many hours of debate and crafting that maximised their applicability. For example, ISO 38500 Principle 6 focuses on Human Behaviour and requires that ICT use respects the behaviour of "all the people in the process". There are many more "people in the process" than just those in the organisation, so the Policy Framework principle 7 may inadvertently reduce consideration for other human communities, such as "customers" of the department. Notwithstanding, there are significant elements of all six ISO 38500 principles within the Policy Framework, and refinement over time should fill the gaps. Further, it is entirely feasible as each department implements its own system of governance that further attention can be given to bringing through the full weight of the ISO 38500 principles in department-level policy and practice.

Corporate Governance of ICT Practices

Speaking of practice, the Policy Framework follows the Principles with a discussion of Practices for Corporate Governance of ICT.

First it mandates the Executive Authority (remember – this is the Minister or equivalent) to provide political and strategic leadership, with oversight, ensure that the arrangements for Corporate Governance of ICT are effective, and to assist the Head of Department deal with issues beyond their direct control.

Then it mandates that national departments must ensure that any necessary arrangements are in place for Governance of ICT in a cross-functional/sector context. This would seem to be focused on ensuring that there are neither gaps nor conflicts in directing and controlling the use of ICT. It is perhaps an aspect of overarching system design that will require more attention during implementation, to ensure that the potential gaps and overlaps are identified.

Responsibility of the Head of Department is given further attention in a list of obligations, including: strategic leadership; strategic alignment of business and ICT plans; establishment and ongoing effectiveness of the arrangements for Corporate Governance of ICT including appointment of a Governance Champion from within the Executive Management team; delegation of ICT-related responsibility and authority to Executive Management; realisation of ICT value with effective management of risk; ensuring provision of appropriate ICT capacity and capability, including appointment of a GITO who must function at Executive Management level. A Risk and Audit Committee is mandated, and is required to assist the Head of Department in Corporate Governance of ICT.

This section then winds up with a long list of obligations for the Executive Management of each department. Some of these are shared with the Head of Department, and are clearly intended to maximise executive management engagement in directing and controlling the use of ICT. The obligations include: alignment of ICT and business strategic goals cascading throughout the department; establishment and embedding of arrangements for Corporate Governance of ICT, including delegation of responsibility to both business management and ICT management; comprehensive and effective planning and adherence to the plans; sound understanding and engagement in maximising the linkage between ICT and business strategy; maintaining necessary ICT security; and building the culture in which the use of ICT respects organisational and human behaviour.

In effect, this section continues the message that has been seen in earlier sections – that Governance of ICT is the task of those at the top of the organisation, and that they have to do certain things in order to ensure that the governance arrangements for ICT become an integral part of business as usual, at the top of the organisation. No doubt, there is a steep learning curve, and there will be a need for considerable support and engagement from the Executive Authority, the Head of Department and the Governance Champion.

Enabling and Oversight Structures

South Africa has avoided the temptation to centralise control of ICT, while retaining structures that promote effective use of ICT across government. These include the role of the Government Information Technology Officer and the GITO Council, which provides inter-departmental liaison on advancing the use and sharing of ICT. The State IT Agency exists to provide systems integration capability for "Transversal Information and Communication Systems for Government", while the DPSA's Public Service ICT Management arm has responsibility for ICT-enabled improvement in Public Service delivery.

To eliminate any unintended transfer or avoidance of responsibility, the Policy Framework makes it absolutely clear that the enabling structures do not negate accountability and responsibility of Executive Authority, Head of Department or Executive Management for evaluating, directing and monitoring the use of ICT in their departments.

Further reinforcement and clarity regarding responsibility for ICT is provided in section 17, addressing the oversight structures. The section begins with a reminder that the Policy Framework and its assignments of responsibility are a direct consequence of multiple prior investigations finding that ICT was not effectively managed. A substantial

diagram of oversight arrangements is provided, with Cabinet as the highest level of authority and oversight. Specific oversight arrangements and responsibilities are described in terms of:

- Ministerial Cluster for Governance and Administration – foster an integrated approach to governance;
- Minister for Public Service and Administration – overall responsibility for ICT in the Public Service, able to establish norms, standards, regulations and directives to improve Public Service function and service delivery;
- Department of Public Service and Administration – Support and advice on Public Service transformation, excellence and good governance.
- DPSA Public Service ICT Management Branch – development, oversight and compliance monitoring of Corporate Governance of ICT;
- Department of Performance, Monitoring and Evaluation – monitoring and evaluating the performance of government, including performance against the Corporate Governance of ICT Policy Framework;
- GITO Council – coordinate, advise and facilitate adoption and implementation of arrangements for Corporate Governance of ICT;
- Auditor General – audit and report on Corporate Governance of ICT;
- Individual Departments – Internally monitor, continuously improve and report on Corporate Governance of ICT.

Implementation Approach

If you want a message to stick, it's probably necessary to repeat it, consistently, in a way that it becomes unavoidable and persistent. This is what the authors of the Policy Framework do – repeatedly positioning the importance and top level responsibility for Corporate Governance of ICT and establishing its relationship to the next layer – Governance (Management) of ICT. The approach acknowledges the unique circumstances of departments, allowing them to craft their approach within the principles and practices defined in the Policy Framework.

Three phases of work are prescribed – first to establish the Corporate Governance and Governance (Management) of ICT arrangements; second to orchestrate strategic alignment; and third to continuously improve.

Phase 1 involves substantial work, much of which will be ongoing. It includes strategies, architectures, plans, frameworks, policies, structures, processes, procedures, mechanisms, controls and an ethical culture. The work is to be guided by the Policy Framework and a framework for Governance (Management) of ICT to be prepared by DPSA.

Creating a Departmental Charter for Corporate Governance of ICT appears to be the first major task for each department. This charter should be based on analysis of departmental requirements and should enable creation of the detailed arrangements for Corporate Governance of ICT. Six topic areas are listed, covering: alignment; service delivery for business value; management of risk; enabling structures; capacity and capability; key roles; and plans for implementation and maintenance of the arrangements for Corporate Governance of ICT and Governance (Management) of ICT.

The discussion of key roles is particularly noteworthy, and introduces an important additional concept that has not been mentioned previously in the framework – that of the Enterprise Architect. This is *"a person knowledgeable in the business of the department who will be responsible for structured planning to articulate the business and related processes of the department in an interrelated and standardised way"*. Imagine that – each government department is expected to have an officer operating at a high level who knows how the department works (and therefore how it uses ICT) and who can plan change in an orderly manner. What an excellent idea!

The Governance Champion role is reiterated in this section as well. It must be assigned to an individual at executive management or directly reporting to executive management level, with a mandate for decision making as well as selective escalation. The Champion must understand the department, has a key role in design, implementation and ongoing conduct of arrangements for Corporate Governance and Governance (Management) of ICT, and is supported by a cross-functional team with business and ICT representation.

A reinforced GITO role is also mandated, with the role firmly positioned as part of Executive Management. The key responsibility of the role is alignment. It does not include operational management of ICT, which is allocated to an ICT Manager.

Establishing effective Governance of ICT also requires a enabling frameworks. The list of ten elements touches on: Departmental Enterprise Architecture and ICT Architecture; Risk Management; Internal Audit; ICT Management; ICT Portfolio Management; Information Security; and Business Continuity.

Just as the mandating of an Enterprise Architect role is a welcome development, the requirement for Departmental Enterprise Architecture and ICT Architecture will be significant tools in managing ongoing development and improvement of business and ICT capability in each department. While the Policy Framework states that the Enterprise Architecture is required to articulate stakeholder and business needs, it should also become a useful means, together with the ICT Architecture, for identifying opportunities for improvement in a department, and in time, for identifying opportunities for rationalisation, standardisation and sharing across departments.

Discussion of Phases 2 and 3 in the Policy Framework is quite limited. It does seem that the main effort has gone, quite appropriately, to developing Phase 1 to an actionable state which will enable transition into subsequent activities. However, it may be advisable for South Africa to consider the potential for some overlap, as work to establish some aspects of the capability in Phase 1 will present an opportunity to draw forward some aspects of Phase 2 – especially in the context of describing the enterprise architecture and, perhaps, the management frameworks.

Implementation timeframes are also set in the Policy Framework. Phase 1 should be under way now, and should be complete by March 2014 – one year away. Phase 2 is then allowed an additional year, with Phase 3 – the continuous improvement phase – commencing in March 2015. However, continuous improvement will not be just about process – the critical factor for success in this initiative will, without any shadow of doubt, be commitment and engagement at the top – at Executive Authority, Head of Department and Executive Management levels, and South Africa would do well to give attention to this engagement on a continuing basis from the outset of the project.

Can it Work?

This is the most comprehensive and thorough plan for wide scale implementation of ISO 38500-oriented governance arrangements yet produced – it is a lighthouse beacon that many should watch carefully.

South Africa has a history, documented in its own reviews and audit reports, of limited success in establishing effective control of ICT. It seems evident that there has been a culture of non-engagement at the executive levels, which will have inhibited success in the past. This plan depends very heavily on, and aims to establish substantial engagement at the top. If that engagement is established successfully, and is sustained, the plan has a good chance of working. If the engagement does not happen, or if it comes in an initial burst and then fades, the chances of success will diminish accordingly.

The critical message about Governance of ICT that underlies the Policy Framework is that ICT is a crucial and integral part of current business activity and will play a vital part in design and delivery of future capability. I would be looking to articulate this message much more strongly, to build understanding at the executive level that the capability of ICT and the way ICT is used in the economy by organisations and individuals have a dramatic impact on the design and delivery of government service – even to the point of influencing what service is delivered. When the executive ranks fully understand that ICT significantly impacts their own role and performance, there is a greater likelihood of engagement than when it is thought of as a black box that can be ignored as somebody else's problem.

Hand in hand with the messages about the part played by ICT, I would be looking to build deeper understanding of the integral nature of business capability, which Harold Leavitt described in his diamond model as being the product of people, process, organisation and technology. Planning, designing and delivering future business capability requires balanced attention to the four dimensions. The guidance in the Policy Framework for Phase 2 contains an embryo of this notion, with the Enterprise Architecture spanning business and ICT strategy lines. What is missing from the model is clear articulation that new capability comes not from ICT implementation activities, but from combined business capability initiatives that simultaneously address the four points of Leavitt's Diamond.

As you would expect, I will be watching with interest, and hoping to provide advice, support and resources to help this effort achieve the success it deserves. Top

Strategy South Australia

One might be forgiven for thinking that it's the season for government strategy on ICT. Hard on the heels of the strategy announced in Victoria on 12 February (we published commentary on the draft of that strategy in October 2012) comes release for public comment of a draft strategy for ICT in South Australia. I spent some time with ICT leaders in South Australia late in 2011, and am now looking forward to commenting on the draft strategy. Look for more on that in the April Infonomics Letter.

Queensland Health Inquiry

Many readers of The Infonomics Letter will remember the June 2010 edition, in which we explored catastrophic failure of a new payroll system implemented for the Queensland Department of Health. Following several audit and external consultant reports, the Queensland Government has now launched a high level Commission of Inquiry into the project. The Commission is quite transparent, with copies of submissions and transcripts of proceedings available from the Commission web site. Hearings have been under way for a couple of weeks now, with the initial focus being on the tender process and selection of IBM as prime contractor. Some of what has been said to date might well make the hair of reasonable people stand on end – and the press has gleefully reported on some aspects of what happened that seem, in the cold light of a courtroom, to be quite unbelievable.

Infonomics is urging the Commission to inform itself about the guidance in ISO 38500, and to form views on whether or not conformance to the standard might have resulted in a different outcome. We don't know whether that will happen, but we certainly hope it will be the case. Regardless, when the Commission delivers its findings, there will be a summary and analysis in The Infonomics Letter.

Extended Reach

The Infonomics Letters of September, October and November 2012 delivered discussion of questions that Directors might ask in the boardroom, to ascertain whether or not their organisations are effective in directing and controlling their use of ICT. Feedback on these questions was strong and positive, and they were picked up and republished, with permission, by Matrix on Board and then by the Institute of Chartered Accountants.

Now the questions have gone global. A lightly revised version of the strategy oriented questions has just been published in EDPACS, a prestigious journal with global circulation and an editorial board that contains a who's who of experts in all aspects of governance, audit and security for IT. The published article is here – the first 49 people to click this link get it for free.

Boardroom Skills

It seems that many company directors continue to feel disadvantaged when it comes to asking questions about IT in the boardroom, even as they are under increasing pressure to engage more strongly on aspect of IT use. Academic attention to the topic is shifting from analysing whether or not boards should engage, to understanding the expertise needed by directors to enable their engagement.

A researcher seeks help

Recently, Shafi Mahomad, a PhD Student at Griffith University in Brisbane sought some input for his work on the competencies required to enable effective oversight of IT by a board of directors. He's been developing a capability model that, when complete, aims to inform directors on what they need to know about in order to engage effectively on IT. He hasn't plucked ideas out of the air on this – he's sought input from diverse sources, including academic journals and industry experts.

And receives interesting advice

One source that Shafi has engaged is a member of ISACA, the international organisation for professionals involved in governance, audit and security of IT. ISACA, through its affiliated IT Governance Institute, has conducted extensive research into governance of IT over more than a decade, and has published many useful papers on the subject. However, much of what ISACA publishes under the heading of governance is, in reality, management. This unfortunately results in board members being told that to govern IT, they need to have the expertise and do the work of managers (note how the South African Policy Framework clearly designates the ISACA guidance published in COBIT as management).

The input provided to Shafi by his ISACA contact is, in my opinion, stunning in its lack of comprehension of the role of a company director. Here it is, de-identified, but verbatim:

"…for their own use as part of the board.

> *office automation (wp, ss, pp), collaboration software(groupware, project management, web content management software, knowledge management software, document management) internet, intranet, extranet, Conferencing (video conferencing, webinar, data conferencing, audio conferencing), communication (email, unified communications, social media), business process modelling, security software, Board self-service systems (accounts and expenses).*

There are other competencies that (directors) may need to know in order to be able to evaluate IT selection choices within the organisation.

> *Cross Functional software e.g. erp , crm, scm or single function (finance (payroll, financial accounting, management accounting), HR (recruitment, time and attendance, absenteeism), Sales (sales order system, payments), procurement (purchase order system), Marketing (market research), production (CIM, CAD, CAE, CAM), distribution (supply chain planning, supply chain execution), IT (help desk software, testing software). As well as decision support systems, expert systems, strategic information systems, executive information systems. Also – audit software, asset management, risk management, quality assurance, governance software, software acquisition methodologies, testing software, asset replacement software etc.*

They would need to know IT infrastructure / architecture (people, software, hardware, data, network, policies and procedures)…

What can one say? It's no wonder that board directors throw their hands up in horror when they are told that governance of IT requires them to have such extensive capability.

This is a classical demonstration of how little understanding many IT professionals have of boards! Not only is it utterly impractical for a board member or even a collection of members to understand all the topics listed, the greater sin in this list is its complete failure to mention strategy development, planning for IT-enabled business capability implementation, delivery of IT-enabled change and operation of an IT-enabled business!

Think of a person planning a three month tour of the Australian Outback in a 4wd vehicle. The advice provided above regarding board savvy on IT would translate into knowledge of engine design, satellite navigation systems, tyres, lights and maybe cargo carrier systems. It would fail to include anything about desirable destinations, navigation, seasonal weather, bushcraft and survival techniques, emergency procedures, catering and replenishment of

supplies! The traveller might start out with a great 4wd vehicle, but would soon be dead!

A well-aged perspective

Another input used by Shafi is a "Information Technology and the Board of Directors" by Richard Nolan & F. Warren McFarlan, published in Harvard Business Review in October 2005. As part of my input to Shafi, I re-read the HBR article. It was interesting to reflect on how much has changed since then… I had just bought my first smartphone, and was way out there compared to my peers; social media was emerging, online shopping was in its infancy… I wonder if they had any idea of what it would all evolve to.

Hindsight can be cruel. One thing I noticed this time was their claim in October 2005 that there were no standards for IT Governance. Of course, they had missed AS 8015, and that's a pity because had a journal such as HBR reported on it, the standard might have gained earlier traction. Another thing I was concerned about was that they might have been writing from a strong US perspective – where many boards, especially prior to 2008, were dominated by executives. I'm not so concerned now because they do emphasise the desirability of independent members for the IT Governance committee. Notwithstanding, some of what they said is, in my view, a little coloured by the US thinking of the time.

One aspect of IT use that I think Nolan and McFarlan missed – unsurprising as it has only really been recognised in recent times – is the depth of integration that exists today between IT and business. It's a subtle shift, but significant, as boards now need to satisfy themselves not just that the technology is in good shape, but that it's being used properly to deliver intended value. Another element that has changed radically is that much of the technology agenda has now been wrest from the individual company's control and is now being driven by customers, suppliers and even by employees. The latter aspect is exacerbated by the opportunity for employees to now bypass IT departments through use of cloud based services. Taking these things into account, I would be revising their strategic impact grid somewhat.

The article proposed a number of things that the board or IT committee should do – like *"understand the overall architecture of its company's IT application portfolio"*. Seriously? I wonder what would be the point of the board understanding the architecture if management doesn't. That would be pretty strange, wouldn't it? If they said that the board should ensure that management understands the architecture, and kept it in good health, I'd be a lot happier. Management would have to get familiar with the architecture and present it to the board, and if the board did not include enough expertise to understand and test what is presented, then it would be quite appropriate for the board to engage an independent adviser. Look again at what South Africa is looking for – in their approach to governance of IT, they clearly want top management to be completely across the architecture, and to manage change from an architecture perspective.

A similar problem occurs when the article says that *"boards of companies in factory and strategic modes should conduct regular reviews of their security and reliability measures…"*. OK, if they mean, get management to present on these topics and convince the board that it's up to scratch, that's fine – but if it means that the board reviews the measures (and the risks) at a hands-on level, then we have a problem.

But then the article makes a good point: *"A board will want to make sure that service outages don't occur…"*. It's a subtle but significant shift in language. The board can make sure not by going hands on, but by appropriately directing and monitoring management, so that the board can begin with an appropriate understanding of the risk (evaluate), put in place policies and plans (developed on the board's behalf by management – direct) and keep an eye on whether the future is unfolding as expected (monitor).

Later the authors tell boards to ensure that appropriate project management systems are in place, so they don't consistently expect the board to do things – there's an element of language that recognises the proper supervisory/oversight role of the board.

But then they talk about the board deciding about the economics of retaining or replacing technology. How does a board do this? Normally, it's by asking management to do the leg work and keep the board up to speed. The board doesn't need to know the detail – what it needs to know is that management is effectively on top of the situation and that appropriate choices are made – and the board can ask broad questions to test this without ever getting down to the nuts and bolts of particular technology elements.

The article continues with points that can be read as requiring the board to have specific knowledge. But the points that are made can equally be achieved by having management do the leg-work, as it should, with the board asking questions that will trigger that work. This is the context in which I posed my questions for directors to ask (as mentioned in Extended Reach). It's not so much that directors need to know the answers, as the directors needing to know that management is on top of the issue and has the right answers. So the points made about new products, competitive threats, breakout technologies and new entrants are all valid, but rather than expecting the directors to do the job, the focus needs to be on the management, with questions from the board steering management's efforts.

It's also interesting to consider the way that the paper looks at the business/IT context. The authors are looking for a fair bit of business expertise in the managers who are talking about IT, and they are looking for the board committee to have a fair bit of business savvy along with the IT expert. That may have been a radical view in 2005, but today it's insufficient. My advice to boards today is that the business executive should do ALL the talking about IT, and the CIO should be there to validate what they say. Again, it brings to the fore the important difference between boards being experts and boards being able to draw out the advice from the experts. Frankly, I think the latter capability is far more important as it gives the board access to a much broader range of perspective, while ensuring that the organisation's use of IT is being addressed properly in the context of strategy rather than being tacked on as an afterthought.

Distilling the essence

It's important to consider the advice in the HBR paper, and a lot of the contemporary advice, as needing interpretation between what a board should do in its own activity and what the board should have done by management.

Many authors write both sets of tasks using language that suggests a requirement for the board to directly perform the work when it is necessary and appropriate for the work to be delegated. With regard to IT, I believe that the board should actually delegate a great deal of the work, while retaining and building the capability to properly oversee the work that must be done.

In this context, I lean a little further away from a frequent recommendation that boards should include an IT expert, while at the same time recognising that, to develop the expertise that I seek, boards will need access, for a while, to people who already have the expertise and insight.

Shafi's work continues, as he strives to identify the capabilities that boards and board directors need to be effective in discharging their duty of oversight in respect of information technology. I'm sure that he would be most interested to receive thoughts and advice from readers of The Infonomics Letter, and I'll be more than happy to pass any comments to him.

Top

Developing Digital Leadership and Governance Skills

It's good to be able to announce a number of opportunities for Infonomics Letter readers and their colleagues to further explore the essential knowledge and skills required for effective Digital Leadership and Governance of IT.

18 – 19 April 2013: ACS Victoria Branch: ISO 38500 Foundation. The well-established two-day foundation class prepares business and IT leaders with insight to the key messages, principles and fundamental tasks presented in the standard. It is jargon-free and helps build clarity on the essential relationship between business and technology specialists for organisations navigating into the Digital Future. This event is especially relevant for people working in the Victorian Government, given that ISO 38500 is explicitly identified as best-practice guidance for governance of IT in the state's recently announced ICT Strategy. Details and registration are here, or email Daphne Kechagias or phone the ACS Branch at +61 3 9690 8000.

26 – 27 August 2013: ISACA South Africa IT Governance, Information Security, IT Assurance and Risk Management Conference at Emperors Palace, Johannesburg. I'm delighted to have been invited to speak at this event. My session abstract will read: *Digital Leaders are using IT to redefine not just their own business, but the markets and competitive landscapes in which they operate. They are seeing and harnessing the potential in IT to do business differently and to create new businesses from scratch. Rapid emergence of the digitally transformed market drives new questions: what are the essential skills and capabilities of a Digital Leader? How can Digital Leaders operate effectively? How can organisations put themselves on the front foot and be Digital Leaders, rather than Digital Disasters?*

Since agreeing to do this session, I've also agreed to do a second session, and a workshop.

Session two looks at *Behaviour vs Process – the underpinning power of ISO 38500. Research published in the UK and Australia in recent times validates the choice made in the original design of Australian Standard AS 8015 and its successor, ISO 38500. These standards focus on behaviour of the organisation and the people in it as they make decisions about its use of information technology. In this session we will look at anecdotal illustrations of how inappropriate behaviour has undermined what should have been effective process, while excellent behaviour has made up for weak and non-existent process. A brief history of debate that occurred during the development of AS 8015 is followed by discussion of how the principles presented in ISO 38500 can be used to drive appropriate behaviour in any organisation.*

The workshop will enable participants to Self-assess their organisations against ISO 38500. Participants will work through a 30 point self-assessment diagnostic to form a view of how effectively their organisations govern their use of IT. Each point in the assessment is discussed briefly, before participants score their perceived extent of alignment on the point. Aggregation of scores and examination of scoring patterns provides insight to performance in respect of the ISO 38500 model and principles, and suggests areas where improvement might be sought.