The Infonomics *Letter*
Plain Language about Leadership and (Corporate) Governance of Information Technology
September 2011 Edition

Unexpected Interlude

Hello and welcome to The Infonomics Letter for September 2011. Those who are paying attention will realise that there has been a gap: the August Letter did not materialise. Sometimes when operating as a one-man-band, circumstances crop up that just make it impossible to deliver everything, and when that happens, the freebies have to make way.

The Australian team that originally developed ISO 38500 is preparing a submission relating to its future work. Your thoughts will help guide that submission. Please give us a few moments now to respond on twelve points in the *Survey on Governance Standards*. There is a little more information at right, and more again in the introduction to the survey.

This month, we begin with *Governance and Management: Further Perspective.* Regular readers will remember that in the last edition I expressed disappointment about the draft of the COBIT 5 framework. COBIT 5 is a product of ISACA, an international membership organisation for IT professionals. ISACA was an early influencer in governance of IT and its COBIT framework is frequently referenced as a guide on governance and management of IT. In its latest incarnation, we had been led to believe that COBIT would align to and integrate ISO 38500. The outcome is disappointing, as explained in the July edition. Since then there has been a great deal of debate around the subject on various internet discussion groups. I have used some of that discussion to frame *Governance and Management: Further Perspective*, in a further effort to explain just how the concepts of governance and management are related.

Inexorably, Information Technology is becoming a topic of boardroom discussion. However, some of the discussion is not about the organisation's use of IT – rather it focuses on the board's own use of IT. The topic became newsworthy recently when the legal specialists at ANZ Bank asked its board to not use iPads, due to concerns about the handling of notes directors might make on the device when using it to read board papers and participate in the work of the board. *Technology in the Boardroom: A Governance Perspective* aims to answer some of the questions originally raised by a journalist exploring the issue for a future edition of the Company Director magazine.

Finally, I will be in London for the latter part of September, attending a meeting of the international working group on standards for governance of IT. In *Thanks for the Help*, I recognise those who are helping me get there.

I trust that you enjoy this edition.

Mark Toomey 13 September 2011

Survey on Governance Standards

Like all investments, work on developing and maintaining standards requires a business case that demonstrates why the work is important. While most of the work done in Australia on standards for governance of IT is voluntary, there remain some costs that are incurred by Standards Australia in administering the work.

The time has come when agreement to support work on governance of IT must be renewed. In the coming couple of weeks, the Australian committee must present a submission through the Standards Australia Project Prioritisation Process.

A brief survey developed and conducted by Infonomics aims to provide some additional perspective on why and how Australia should keep contributing to international body of knowledge. All readers of The Infonomics Letter are welcome to participate. Click here to complete the survey now.

[top]

Governance and Management: Further Perspective

The last Infonomics Letter (July 2011) was mostly focused on the Exposure Draft of the COBIT 5 framework developed by ISACA. I presented then, and persist with, the view that the draft of COBIT 5 has serious problems in its presentation of the related but separate concepts of governance and management, and that rather than clarifying matters, it adds considerably to the confusion. I also had the temerity to suggest that while COBIT 5 claims to be aligned to ISO 38500, it fails by confusing governance and management, by incorrectly describing the core governance tasks of evaluate, direct and monitor, and by not referencing the principles, without which ISO 38500 would be of little use.

Naturally my comments generated some push-back, but perhaps not as much as anticipated. They also generated a fair amount of agreement – I don't think that I am alone in my concern. There was extensive debate on several LinkedIn forums – and some of that was quite robust!

Reflecting on those discussions, I took the opportunity to stand back a little and explain how I see the relationship between governance and management. It seems that one of the most difficult concepts to grasp when discussing governance of IT is the interplay, or mesh, between governance and management.

In summary, we must recognise (and there seems to be very little dispute) that the governing body (the board of directors) has ultimate accountability for the organisation. To be accountable and effective, the governing body must ensure that there are appropriate management systems in place and that tasks are appropriately delegated to management. The routine tasks delegated to management can be seen as being carried out in the management systems. To an appropriate degree, the governing body guides decisions by management, typically by establishment of policy that is then used within the various management systems. The governing body then provides oversight to confirm that management is doing the job properly.

ISO 38500 describes governance as being a system - a system of governance. Every organisation will be unique in the design of its system of governance, because the delegation of authority will vary, because the policy that guides decision making will vary, because the management systems will vary, and because the level and intensity of monitoring will vary.

The notion that governance is a system comes from the widely known "Cadbury" definition of Corporate Governance, on which the ISO 38500 definition for governance of IT is based. The definition is very simple and clear: *Corporate Governance is the **system** by which an organisation is directed and controlled*. To understand a system in the context of an overall organisation, we can call on the work of H.J. Leavitt in 1964. Leavitt, an early expert in organisational change, said that a system in the context of business is made up of people who perform tasks (processes) in a structure (organisation, rules etc.) using tools (technology). Thus it can be said that the people involved in governance include the board, the executive and others, with the precise roles that each plays defined as part of the structure (delegations, policies etc.) and the actual tasks that are performed. The overall system can be decomposed into functional subsystems, where the subsystems themselves may also be decomposed. Consider finance – a subject that is always understood to be a core discipline for governance. The overall management system for finance readily decomposes into smaller units dealing with purchasing, sales, invoicing, collections, banking and so on. Further, when done properly, the decomposition also clarifies the means by which the governing body actually engages with these smaller units through its higher level perspective.

Following this logic, we should see that management systems are effectively the tools that the governing body uses to discharge its duties. Management systems are also the primary sources of information for the governing body, enabling it to judge whether the organisation is performing as it should, and conforming properly to all relevant internal and external rules, strategies, plans and so on.

The fact that the management systems are both driven by (however remotely) and provide information to (however indirectly) the governing body means that without management systems, the governing body is unable to function. Thus we can take the view that all management systems are necessarily part of the governance system. That does not mean that management should be confused with governance.

In their 2004 book "*IT Governance: How Top Performers Manage IT Decision Rights for Superior Results"*, Peter Weill & Jeanne Ross identified six asset classes that governing bodies oversee - financial, human, intellectual, physical, information and relationships.

We all know that boards have for a long time governed finance and HR. However, we do not see a great deal of marketing hype around these aspects of governance, as we do around the governance of IT. Yet Weill and Ross paint IT as being effectively in the same space, or context for governance, and we have extensive debate and confusion on the topic. Why is this?

Perhaps the answer is in the subtitle to the book – and its focus on decision rights. Weill and Ross effectively equate "IT Governance" to the assignment of decision rights and the design of the structure in which decisions are made. Indeed, for quite a few years, many advisers have followed this line, and described "IT Governance" as being about the making of decisions.

But is decision making the same thing as governance? Let's answer that by looking at other asset classes identified by Weill and Ross.

There can be no doubt that the management systems pertaining to the use (both demand and supply aspects) of IT involve extensive decision-making, and some of that decision-making can have far-reaching impact on the organisation. Now if we regard IT decision making within the management systems as "IT Governance", then we must also regard all HR decision making in the HR management systems as "HR Governance" and we must regard all finance decision making as "Finance Governance". Following that logic, there would be no management - only governance - as all decision making policy and authority comes from the governing body. Would that be a nonsense? Certainly! Thus we must conclude that using the governance label for management decisions regarding IT is also a nonsense. Moreover, it confuses both directors (how come managers are doing our job) and managers (the board doesn't have a role here). Both forms of confusion can be very dangerous.

The fact that a decision affects the entire organisation does not make it a governance decision. The sole determinant of whether a decision is a governance decision or a management decision is the determination, by the governing body, of whether the authority to make the decision is part of its reserved power, or part of the delegated authority. In the latter case (and ideally, also in the former), there should also be policy to guide decision making. This distinction is well understood in the context of finance (where there are usually clear thresholds to define whether a decision is a management decision (taken by management) or a governance decision (taken by the governing body). The same applies in the context of contracts and in human resource terms where, for example, the engagement of a single employee is usually the responsibility of management, but the engagement of the CEO is, unquestionably, the responsibility of the governing body.

The above discussion makes it clear that all delegated decisions are management decisions. Notwithstanding, they are always taken in the context of the system of governance, subject to oversight in the form of guidance and monitoring.

This view of the relationship between governance and management fits HR and Finance very well, and thus should also be applied in IT. It allows that governance failures can originate deeply in the management systems; it allows that all management decisions and actions are guided by policy and strategy; it allows that responsibility delegated by the governing body can be further delegated unless the higher levels of authority have limited the right to delegate; and it allows that in different areas of concern, the level of delegated authority can be set quite differently.

When an early draft of the above discussion was posted on an Internet discussion forum, a number of questions were asked. These, and the answers, may further help understanding of the topic.

Q: Does governance include leadership and entrepreneurship?

A: The system of governance must include leadership and must ensure that leadership is working properly. The governing body provides leadership for the CEO and through the CEO for the rest of the organisation. Many aspects of leadership detail will probably be delegated, though in many cases this delegation is not particularly formal.

Entrepreneurship is an interesting topic. What is entrepreneurship? I think an entrepreneur is just one who drives forward new investment to create new outcomes; so an entrepreneurial business would be one that invests for new outcomes. Isn't that part of the lifeblood of business? Why would we see it as part of governance? Should we instead note that the risk appetite and strategy settings adopted (often on management recommendation) by the governing body will influence the approach to entrepreneurship?

Q: The ISO 38500 definition of governance is "The system by which organizations are directed and controlled." On the other hand, my undergraduate management textbook said management had five components. These included Directing and Controlling, but also included Planning, Organising and Staffing. Would you consider governance including the other three as well?

A: Indeed, the system includes directing and controlling the organisation and these fundamental tasks can be delegated in greater or lesser degrees to management. Thus your undergraduate text would be accurate in listing directing and controlling as management tasks, though it might have been more accurate had it also noted that management is subject to oversight from the governing body. As for planning, organising and staffing: What is planning, if it is not adding detail to the direction and enabling finer control? What is organising if it is not implementation of plans? What is staffing if not one particular aspect of organising? I tend to describe management activity as planning, building and running the organisation's business, where planning, building and running are subject to oversight by the governing body. Directing provides the overall context and limits (such as budget and risk appetite) for the plan, build and run activities, while controlling ensures that the organisation achieves objectives within those parameters.

Q: One of the problems of consensus based definitions such as this is that it becomes a catch-all phrase meant to satisfy everybody (Security is a classic catch-all phrase). Are you able to scope governance by what it is not?

A: It's a tall order. One has to distinguish between governance - the act of governing, and the governing body. I've seen organisations with governing bodies, but poor governance. I've seen organisations with no separate governing body, but with excellent governance. One cannot say that governance includes this and excludes that, because what is right in one situation is not right in another. There are contradictions - governance is ensuring that managers do their jobs properly, but governance does not necessarily include specifying the manager's job - except through the formal delegations of authority.

Perhaps the best way to tackle this is from the converse: Everything that is done by management, is management, even if it is a task delegated formally or informally by the governing body. Whatever is left, is governance. Governance in this context is at the very heart of the organisation, taking the decisions that define the organisation, and ensuring that these decisions are implemented.

[top]

Technology in the Boardroom: A Governance Perspective

A recent story circulating on the web tells of a CEO who storms out of a board meeting, to confront his Personal Assistant with the question: "How come I am the only person in there who does not have an iPad"? This contrasts with a recent press report that the board of ANZ Bank has been effectively denied permission to use iPads. Perhaps the most interesting aspect of this intervention is that it does not come from the IT department, but from the legal office, where there are concerns about matters such as capture and retention of notes made by the directors as they work through their board papers and meeting agenda.

The rising interest in use of technology in the boardroom has caught the attention of journalist Domini Stewart, who writes for Company Director magazine. Domini asked for some thoughts around the topic. As usual, I gave her far too much, and while she can't publish it all, I have no such restriction. Thus, here are some thoughts on governance of technology in the boardroom.

What are the latest trends in boardroom technology?

Many companies have, during the past few years, been adopting technology to assist in the conduct of board business. However, this has been relatively low-key, until recently. There has been a definite increase in interest in technology FOR the board since the advent of the iPhone and the iPad and similar technologies. It is almost unarguable that this is driven by the "ease of use" rather than any specific functional benefit, as prior and competing technologies had all the same basic capability. It is striking to note that one of the places where "consumerisation of technology" (where the consumer/user makes the choice about which technology is used and how) is being felt strongly in organisations appears to be in the boardroom.

What are the benefits of technology (in the boardroom) and how can we maximise the benefits?

Technology alone has no benefit other than to profit the people who manufacture and sell it. For the buyer of technology, benefit comes only from its use.

Any technology based alternative to manual process and paper carries many potential advantages and disadvantages. But the technology alone is not the issue – it is how the technology is used and integrated into the rest of the business (or in this case the boardroom) operating model. The technology can be used in its most basic form as a simple alternative to paper, or it can be taken into much more advanced scenarios where the whole boardroom process is revised.

Extracting the full benefit of technology in the boardroom requires exactly the same attention to detail, to innovation, to change management aspects of the way the board operates and the relevant skills of the people involved – again not just the directors but the managers and other personnel who are involved in the board processes. In other words, adopting technology in the boardroom should be treated as a business improvement initiative, just as any other IT enabled change to the business.

A poorly thought out and ad-hoc approach to introducing new technology in the boardroom will probably cause many problems. A well-thought out approach might greatly improve security of boardroom information, speed of delivery of information and compactness of information. Technology, when well used, may offer directors options to see board information in new, more compact ways, with the option of drilling in where needed. Technology can also help directors keep their own notes and do so in ways that may offer better legal protection than the old paper notes – but set up wrongly the same technology could create new legal risks. Again, careful attention to design, by people who truly understand the boardroom process, is essential.

What are the risks of technology in the boardroom, and how can we best mitigate them?

The recent cases where use of iPads has been blocked on security grounds have highlighted a very important set of issues – that replacing paper with computers is never a straight one-for-one transition, because the technology presents both new opportunities and new risks.

However, as with any technology enabled change, the big risks are not the ones purely of the technology. Rather, they are the risks of misusing the technology. For a board, the issue should not be having the best new toys – it should be having the best means of effectively governing the organisation. One significant risk is that individuals bring new toys into the office or boardroom, and everybody wants one simply because they are easy to use, leading to proliferation without understanding either the opportunity or the risk. What should be happening is a careful (if accelerated) and diligent process of working out how the board should operate in future, maximising the advantage and containing adverse risk associated with new technology. Clearly, as key stakeholders in this, the board itself should have significant input into the design of the approach.

What lies behind ANZ's decision to ban iPads because the company can't control annotations?

Ultimately only ANZ can answer this, and perhaps at some time they may explain themselves. But to explore the topic, we need to think about the distinction between what actually happens in the "pre-iPad" era, and what might, and should happen in the "post-iPad" era. We should start by understanding how ANZ (or any other organisation) currently "controls annotations"? If Directors write notes on paper – what happens to the paper next? Is it taken away from the directors and sealed in a vault in anticipation of some legal need? Are directors prohibited from changing or removing notes? Must directors always write directly on their board paper or might hey use sticky notes and blank sheets? What behaviours might directors indulge in when their papers are electronic and the notes are also electronic? Must the notes be captured and retained, or destroyed? Can they be changed? Can directors have some notes that are private, for their own use, while others are for wider use? The point here is – what exactly is it that the directors and others might do on the iPad that is so inconsistent with their established boardroom practice? It's quite possible that there are some genuine issues there – and the detail needs to be teased out to the benefit of all.

What sort of etiquette should apply with use of boardroom technology – for example, should people be messaging each other during board meetings?

This is an interesting space. We have been trying to educate people for ages now about turning mobile phones off in meetings, and not expecting instant responses to emails. The trouble is that what is acceptable in one context or place is not acceptable in another. Boards, like any other organisation, need to recognise the temptation and establish their own protocols and etiquette.

There are cases where instant messaging between individuals in a meeting is extremely effective, and others where it is highly disruptive. The outcome depends on the context and the behaviour of the individuals.

What guidance is available to organisations as they consider adopting new consumer-oriented technology in the boardroom?

The guidance in ISO 38500 is very relevant and powerful. Boards should directly, or through delegation to management:

- Evaluate their boardroom and related processes, and the opportunities and risks presented by emerging and evolving technologies;
- Direct adoption of relevant enabling technology and practices in support of the board's effectiveness and efficiency;
- Monitor and refine the effectiveness of technology used in the boardroom and in support of their governance duties.

In support of these actions, the board should apply the six principles for good governance of IT to their own situation. For example:

- Responsibility: Ensure that there is clarity regarding who is responsible for what in respect of planning, implementing and using technology enabled systems for the boardroom, and ensure that all personnel involved, including the directors themselves, are fully aware of their responsibilities regarding use of technology in the boardroom context.
- Strategy: Ensure that all plans for development of the board's capability take into account the opportunities presented by new technology, and ensure that all plans for new technology in the boardroom are well aligned to the intended mode of operation of the board.
- Acquisition: Ensure that all expenditure on new and existing technology for the board is appropriate, taking into account the opportunities and the risks, the capability of the company and its personnel, the company's investment priorities and its capacity to implement change, especially in the boardroom.
- Performance: Ensure that there are clear and appropriate performance criteria for IT-enabled boardroom activities as well as for manual activities and ensure that these criteria are met. The criteria should address a wide array of measures for the overall system of governance, with a reliable baseline and efficient routine measurement techniques that enable problems to be identified and resolved before they become debilitating.
- Conformance: This is of course a major boardroom issue. Ensure that the obligations of the governing body overall as well as those of individual directors and officers are thoroughly understood and that their interests are neither unduly compromised nor over-zealously protected through adoption of technology in the boardroom. Ensure that the board establishes and enforces its own protocols regarding use of technology, and that it provides leadership by example to the organisation in this regard.
- Human Behaviour: Recognise that, in the boardroom as in any other context, there will be individuals who are champions and enthusiasts for technology and others who will be challenged and sceptical about its value. Ensure that

decisions regarding use of technology are moderated so that they balance these forces. Ensure that the appropriate steps are taken to ensure that when change occurs, it is with strong agreement on the intended purpose and outcomes, with relevant support and control to ensure that the change is a success from the individual and collective points of view.

Boards adopting new technology have a golden opportunity to experience the techniques that are used to adopt new technology at the lower levels of their organisations. They should pay close attention, and assess whether or not the techniques are adequate. Some may be very surprised!

[top]

Infonomics Education Program

In the last Infonomics Letter, I announced that Europe is now positioning itself for a major program of learning about ISO 38500.

Unfortunately, the economy in Europe is not in the best of health. As a result, two of the proposed six events have been withdrawn. However, registrations for the other events are sufficient and they will be going ahead. I again invite all in Europe to consider joining us for one of these events.

Three one-day workshops on Business Governance of IT and ISO 38500, organised by PMOWorks, are in:

- Dublin 26 September
- Amsterdam 28 September
- Madrid 30 September

There will be one ISO 38500 Foundation Class conducted in conjunction with IT Governance Limited:

- London 3-4 October

For details, see the Events Schedule.

Suggestions and requests for education events are always welcome – send them to mail@infonomics.com.au.

[top]

Thanks for the Help

Much of the work that underpins international standards is done by volunteers, working through their respective national standards bodies. When one becomes involved in international standards, the activity can become very expensive. For some volunteers, this is not a problem, as they are employees of major companies which willingly absorb the costs and continue to pay salaries, knowing that they derive benefit from the work in the long term. But for some volunteers, such as myself, there is no benevolent employer, and the cost of participating in standards work is a substantial hit on our personal bottom line. It's a double whammy too, as we not only have to cover our out of pocket costs for participating, but we also forego revenue while we are working on standards issues.

The Australian government provides a scheme to subsidise people who have to travel to work on international standards. The scheme is administered on the government's behalf by Standards Australia. Like all government schemes, this one has rules that sometimes lead to unsatisfactory outcomes and in this case, the unsatisfactory outcome was that I was, at very late notice, denied any financial support for the journey to London for a critically important meeting next week (19 – 22 September).

With no cash in kitty, it was necessary to urgently find alternative sources of funds. An email to over 1000 Australian contacts and subscribers to The Infonomics Letter produced the desired result.

The Australian Computer Society pre-purchased services for a professional development program that will be conducted in 2012.

The Alinement Network pre-purchased services for editing three future editions of the Alinement magazine.

Dr Patrick McConnell is a Visiting Fellow at the Macquarie University Applied Finance Centre. During October, he will be delivering three short courses on Strategic Risk Management. With his new copy of *Waltzing with the Elephant*, he will be able to provide a more comprehensive mention of issues in governance of IT.

Fifteen other people have acquired eighteen brand new copies of Waltzing with the Elephant and The Director's IT Compass.

To all those who helped, and the numerous others who offered moral support, I extend my sincere thanks. And once again, I ask that everybody backs up this support by completing the short survey on future development of guidance and standards for governance of IT.

[top]