The Infonomics *Letter*
Plain Language about Corporate Governance of Information Technology
May 2009 Edition

Fundamental Concepts

Debate about the distinction between "IT Governance" and "IT Management" is building. For years now, we have seen the IT industry using the words interchangeably, or trying to distinguish between higher and lower levels of management by referring to the higher level as "governance". We have seen the "governance" term attached to data, to xml, to green computing, to cloud computing, to outsourcing, to process, and probably to the kitchen sink.

Calling something governance without any further explanation does nothing except create confusion. And it not only confuses IT folk – it confuses managers, executives and directors of firms – because for each of these communities, the word has subtly different meanings.

And now, in the midst of the global financial crisis, with corporate governance very much in the spotlight, there is a redoubling of the focus on governance of IT: what is it; what does it mean; who does it; and how does it happen?

Of course, readers of The Infonomics Letter are well aware that ISO/IEC 38500 provides a clear definition of both terms – but having them written somewhere and having them used properly are two quite different issues.

The problem of distinguishing between governance and management goes beyond simply defining the terms. It requires that we build an understanding of how governance and management mesh together to provide effective overall control and oversight of an organisation, with respect to how it uses IT.

This challenge has been assigned, in the international standards arena, to the newly created workgroup that we announced in The Infonomics Letter, Special Edition of 20 November 2008, and was one of the primary points for discussion at the inaugural meeting of the workgroup in London in May 2009.

Having done considerable thinking about the matter as part of writing my forthcoming book, I had the opportunity to contribute my thoughts to an extensive discussion on the subject during the meeting. While by no means a statement of the final view of the WG, the paper was well received, and so I have decided to open it up for further discussion by presenting it as the main body of this edition of The Infonomics Letter. Your thoughts, as always, are greatly appreciated.

Kind regards,
Mark Toomey
26 May 2009.

A Framework for Governance and Management of IT

ISO/IEC 38500 is frequently listed as one of the available frameworks for governance of IT – along with CobiT, ITIL, ISO 20000 and ISO 27000. While it is good to see that the standard is recognised as a relevant tool, it is incorrect to classify it in this way. Why? Basically, ISO/IEC 38500 is purely about governance of IT – all the rest are focused on the management disciplines that must work well for IT use to be efficient, effective and acceptable.

The main reason that we see ISO/IEC 38500 being compared to the frameworks and standards is that there continues to be considerable lack of clear understanding about the difference, and relationship, between governance and management.

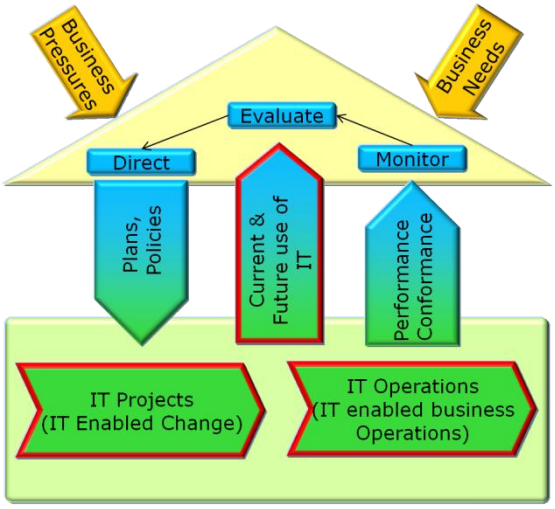
It is noteworthy that this confusion seems unique to the IT arena. We do not see in most literature discussions of "HR Governance", "Finance Governance", "Asset Governance" or "Risk Governance". Why? These generally older and well established disciplines have seamless linkages between the management systems and the overarching governance arrangements. In these disciplines, there are well established practices through which the governing body's intentions and requirements are communicated to management, and through which management provides necessary information to the governing body so that it can discharge its responsibilities. It is well understood that management acts within the governing body's delegated authority, but nobody insists that their delegated authority means they are doing "governance". Yet at the same time, the managers do have a clear understanding of their management systems, and how their base level activities are aggregated to provide information and evidence to those who are ultimately accountable for the organisation's performance. In effect, these aspects of corporate governance can be viewed as systems that overarch, provide direction to, and monitor the performance of the organisation in respect of that particular asset class or governance domain. The exact depth at which the transition between the pure governance tasks and the pure management tasks is somewhat variable, depending on the nature of the organisation, but in well-run organisations, it is quite clear as to where the boundaries lie.

Thus, this paper proposes an initial framework for understanding the concepts of, and distinction between the disciplines of governance and management of information technology, that is similar in nature to the governance and management of the

other classes of asset about which an organisation's governing body would normally be concerned.

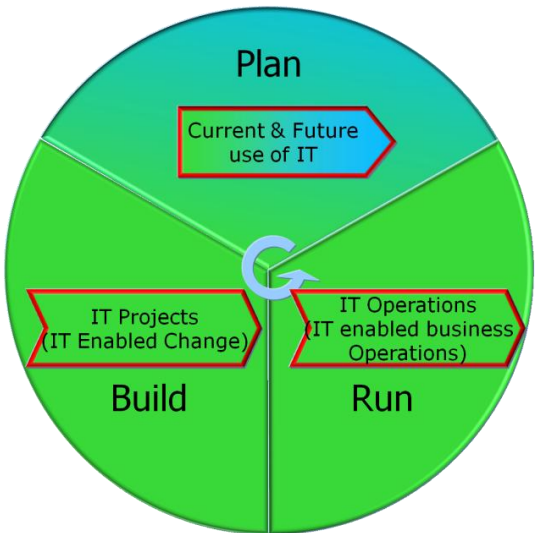
(Corporate) Governance of IT is the system by which an organisation's current and future use of IT is directed and controlled (ISO/IEC 38500). Governance of IT principally deals with the plans for use of IT (in both strategic and operational contexts), the initiatives that create the future use, and the operational activities that constitute the current use.

The model for governance of IT presented in ISO/IEC 38500 positions three key governance tasks – evaluate, direct and monitor, as the key to providing direction to and monitoring performance of managements role in conduct of the organisation's planning, implementation and operational use of IT.



ISO/IEC 38500 Model for Governance of IT*

It can be readily understood then that the focus for governance of IT maps directly to the most basic model for business – Plan-Build-Run. It must be recognised that while this model is sometimes used by IT specialists to explain aspects of the IT cycle, it is also widely understood by business leaders and educators as the basic management cycle of business – and that is the context in which it is used here.



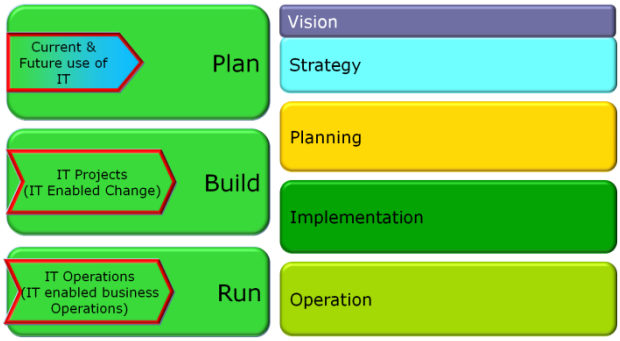
ISO/IEC 38500 in the business management cycle

* ISO/IEC 38500 Corporate Governance of Information Technology is copyright of ISO/IEC

The key assertion in this paper is that the system for governance of IT oversees, controls and receives information from a suite of interconnected management systems uniquely configured to serve the needs of the organisation. The management systems implement the governing body's delegated authority through well-defined policies, processes, role assignments and supporting tools, to provide effective and seamless control over and transparent visibility of the organisation's use of IT. In effect, the management systems provide the "machinery of governance", in that they are controlled by, and give effect to the policies determined by the governing body, and provide the necessary visibility to enable the governing body to fulfil its duties in monitoring conformance and performance with respect to the organisation's use of IT. The precise definition of the points of engagement are quite variable, depending on the nature of the organisation, but in general the purpose of the points of engagement are for the obtaining of direction from the governing body (such as overall corporate direction, behaviour and policy), submission of matters for approval to the governing body (or those acting on its behalf by means of its delegated authority), and provision of feedback and evidence to the governing body as required by its corporate rules.

To understand the nature of a comprehensive system for governance of IT requires a progressive breakdown of the management cycle to which ISO/IEC 38500 is mapped. The first stage of breakdown identifies four primary management systems:

- Strategy development – to define the intended use of IT integrally with, and in the context of the organisation's business vision and strategy. It is sometimes beneficial to view strategy development at two levels – establishing the vision to which the organisation aspires, and defining how that vision is to be attained;



ISO/IEC 38500 primary management systems

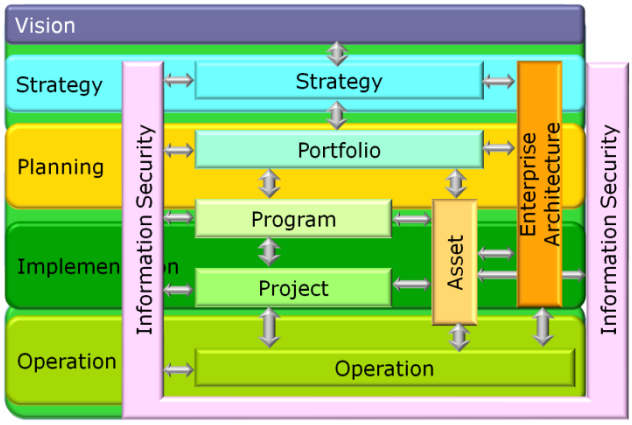
- Planning – to prioritise and allocate the resources to deliver and operate the IT-enabled business systems as required by the organisation's strategy;
- Implementation – deployment and management of allocated resources to deliver the new and

updated business systems required by the organisation's strategy;
- Operation – ongoing conduct of IT-enabled business activities to realise the organisation's established strategic and operational objectives.

It is not essential that these four primary management systems are thought of as being solely focused on IT. Indeed, as IT is pervasive throughout most organizations, it is likely that taking the narrow IT-only perspective on these systems would lead to mismanagement – because IT is merely an enabler to the bigger picture and neither an end, nor a solution in its own right. A more effective approach is to recognise that IT is intrinsic to these management systems and at that level, not given independent focus.

For many organisations, the extent, complexity and risk associated with use of IT as a key enabler of business requires that these four primary management systems be decomposed into a suite of core disciplines. While there can be many ways of breaking the management systems into more discrete units, there has been a good deal of consistency in identification of the next level of management systems. John Thorp, author of The Information Paradox, provides a suitable model which identifies seven disciplines:
- Strategy
- Enterprise Architecture
- Portfolio
- Program
- Project
- Asset
- Operation

In addition, we can effectively wrap Thorp's model with the nowadays essential discipline of Information Security, which is no longer confined to operational matters, but which necessarily considered in all of the disciplines referenced in Thorp's model.



The Extended Thorp Model

Note that while Thorp's model was construed in the context of better managing the use of IT in organizations, it is by no means limited to the IT context, and indeed cannot be isolated to IT alone. To do so would be to deny the reality that IT is an enabler of the business system, which also comprises people, process and structure, as defined by Harold Leavitt in 1965. The significant challenge in many organisations that seek improved governance of IT is in organising these disciplines so that they properly engage on the four key elements of the business system, rather than trying to deal with IT as an independent concept. In this context, the role of Enterprise Architecture comes to the fore – as a well-developed enterprise architecture capability will be addressing the overall design of the organisation, and specifically dealing with the four key dimensions of the business systems.

At this point, it appropriate to note that the disciplines identified in the Extended Thorp Model have all been the focus for development of management frameworks and standards. The existence of directly related standards, which include ITIL, the ISO/IEC 20000 family, the ISO/IEC 27000 family, TOGAF, Prince2, PMBOK and many more, gives confidence that the management disciplines identified in the model are appropriate. It also highlights the inappropriateness of the assertions that sometimes arise that any one of these standards is a complete answer to the needs of organisations in respect of governance and management of IT. (Note, CobiT is also a relevant framework in this context, though its scope is wider and it requires more detailed knowledge of CobiT to clearly identify the way that it underpins the validity of the disciplines identified in the Extended Thorp Model).

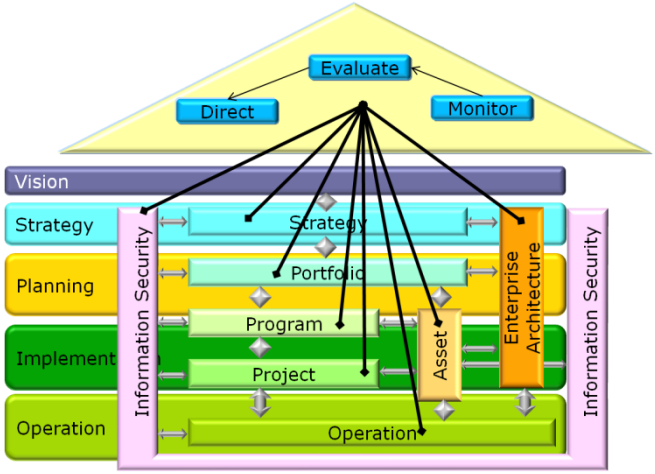
Within the Extended Thorp model, it is feasible if required to further decompose these eight primary disciplines into Key Practices. Identification of the key practices is a task that will require some effort to survey available practice models and link them to the disciplines, acknowledging also that there may be additional key practices that are not presently defined within available practice models. However, for the purpose of illustration, the ISO/IEC 20000 standards clearly identify such management practices as Configuration Management and Incident Management.

At this stage, it is not necessary for us to exhaustively decompose the management systems. Rather, we can expect that the eight primary disciplines identified here can be reliably decomposed and that there will be ready agreement on the decomposed models. What is more important now is to understand how these disciplines and the key practices within them engage with the overall system for governance of IT.

In reality, the governing body's engagement with the management systems will be a matter for determination on a case by case basis by each organisation. However, there will be common characteristic in the engagement, and these are pointed at by ISO/IEC 38500. It should be fairly clear that the governing body's engagement is by way of

establishing top level policies including delegations of authority (often developed in conjunction with management), participation in development of, and approval of strategy, approval of major expenditure items and contracts, and monitoring of conformance and performance in respect of investment and operational activities. While the governing body may not directly engage with every discipline, and certainly not with all of the key practices, it is nonetheless important that the design of the system provides a level of integration that assures proper transmission of the governing body's policy and other requirements throughout the system, and also provides appropriate levels of visibility and transparency.

In large and complex organisations, the authorities and much of the detail of the system for governance of IT are likely to be delegated to executive, senior and middle management. This delegation is manifest in the specific design of the management systems.



Governance – Management Engagement

Thus, we can now visualise an evolved version of the ISO/IEC 38500 model for governance, where the three fundamental steps in the management cycle are now replaced by the eight key disciplines, mapped over the four primary management systems. In this way, we can now begin to develop a clearer understanding of how governance and management roles and tasks are related, and how they are both distinct and inter-dependent.

It can reasonably be said that the management systems or the disciplines within those management systems have a point, or points of engagement with the governance system. These points of engagement provide for:

- Preparation, adoption, communication and enforcement of policy relevant to the management system;
- Delegation of authority and escalation to higher authority as and when required;
- Provision of formal reports in respect of conformance and performance to meet the needs of diligent and efficient oversight by the overarching governing body and any intermediate bodies that it may appoint to act on its delegated authority.

The detailed design of these points of engagement are again a matter for determination on a case by case basis by the subject organisation, taking into account the overall design of its system for governance of IT and the delegated authorities that apply to it.

The ideas presented here are a beginning, not an end. They will be the subject of debate, hopefully on diverse forums, and involving people from all backgrounds, including corporate and government leaders, academics and IT specialists.

There will be specific work done in the ISO context, and it is to be hoped that a clear and workable model will emerge in the near future, so that the entire IT industry, and the organisations that depend on it, can at last have clear and unconfused conversations about governance and management of IT.

Speaking about Governance

As mentioned in the introduction, there are numerous debates that have emerged and run on the topics of governance, management and ISO/IEC 38500. If readers would care to let me know of hot debates that are running, I will set up a links page on www.infonomics.com.au to enable ready access to them.

Learning about ISO/IEC 38500

It promises to be a busy year on the speaking and education circuit. In April, I delivered the first if the ACS Education Across the Nation series in Hobart, Tasmania, with an enthusiastic audience including practicing company directors. Details of the program are on the Infonomics Site web site. April also saw the first delivery of the two-day Extended Masterclass in Kuala Lumpur.

May has been the month for standards meetings and Europe. A small, but quite senior audience participated in the BSI British Standards conference on governance of IT in London, UK on May 20, where Chris Ogden of Business Next joined me to present the Business Case for ISO/IEC 38500 and then a case study on its practical application.

Tomorrow I begin delivery of two heavily subscribed full day Masterclasses in Frankfurt, in conjunction with Serview – the Business IT Alignment Consultants.

August and September will include presentations on governance of IT at the itSMF Australia conference in Sydney in August, and the ISACA Oceania CACS conference in Canberra in September. See the Infonomics Site to see more details on forthcoming education events.