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

July 2011 Edition

Mixed Emotions

Hello and welcome to The Infonomics Letter.

Last month, I mentioned the release of the COBIT 5 Exposure Draft. A brief scan had indicated some definite influence from ISO 38500. That, coupled with recognition of ISO 38500 in the COBIT 5 plans announced in 2010 had left me hopeful that COBIT 5 would provide a real breakthrough in practical guidance on how organisations might establish a comprehensive and effective system for governance and management of IT.

This month, having ground through *COBIT 5: The Framework Exposure Draft*, I am disappointed.

My concern is that COBIT 5 still does not align to the definition of governance provided in ISO 38500. If anything, it goes further down the wrong path of entrenching management activities under the heading "Governance". I've tried to express my concerns in a coherent manner in Shattered Dream.

Offsetting the disappointment is the continuing growth of market interest in ISO 38500. Building on this year's already highly successful forays into the Middle East, Latin America and Malaysia, we are now able to announce seven new events across Europe. In addition to being a reseller of *Waltzing with the Elephant*, IT Governance Limited will promote the ISO 38500 Foundation class. Two new partners for Infonomics are also promoting opportunities for their clients and the broader market to learn about the ISO 38500 approach to governance of IT:

- PMOworks is promoting a series of four events in European cities including its home of Dublin. The company specialises in developing, implementing and supporting PMO operations, helping organizations improve business processes and reduce project risk and overall costs.
- Falk Janotta Unternehmensmanagement is based in Wurzburg, Germany. The company provides a wide range of services to assist organisations achieve success in their use of IT. Company Principal Falk Janotta participated in one of the first Europe classes on ISO 38500, and is now facilitating access to knowledge about the standard for his diverse and expansive network.

See Infonomics Education Program for further detail.

Would you like to obtain some independent advice on your concerns or efforts around governance of IT? Do you have a strategy, a project or some other situation where you are not fully comfortable? Perhaps the Infonomics Access Service will be of assistance to you.

Mark Toomey
31 July 2011

Shattered Dream

Why is it that those who provide thought leadership to the IT community persist in confusing the concepts of governance and management?

Never before has this question been so urgently in need of resolution than right now, as COBIT 5 emerges from its chrysalis to become the new guiding light for 95,000 members of ISACA and numerous other acolytes who follow the guidance of that organisation.

Expectation

For much of its life, COBIT 4.1 has been described as a framework for governance of IT – yet its guidance has been focused purely on the management activities of the organisation. The *COBIT 5 Design Paper Exposure Draft* of 2010 said "COBIT 5 will clarify the distinction between governance and management with a revised process model that distinguishes between these domains while also showing how they relate to each other". The Design Paper went further: "A new focus on governance activities that are at the level of the board and executives will be organised in three new domains aligned with ISO38500: Evaluate, Direct and Monitor". The Design Paper was therefore, the basis for high hopes.

Reality

Now, having read, and re-read *COBIT 5: The Framework Exposure Draft*, I can only say that the hopes have been shattered. Certainly COBIT 5 does contain elements that are classified as "Governance" and other elements that are classified as "Management", but the definitions and distinctions provided are far from aligned with ISO 38500 and are still seriously divergent from contemporary understanding of Corporate Governance.

I'm not alone in my disappointment: Alan Calder, who heads up the UK's IT Governance Limited, said on his blog: "I didn't see anything which specifically addressed the board-level issues which are (I think) so well dealt with in ISO/IEC 38500".

Governance vs Management (1)

Much of the concern that has been articulated in the past about the notion of "IT Governance" is that it has seemed to embrace a vastly different set of activities to those normally understood as being required for other aspects of "Corporate Governance". On the one hand, guidance such as that provided by the ISACA affiliated IT Governance Institute has seemed to assign management level tasks to the board of directors. On the other hand, a wide array of

literature tells IT personnel that they are responsible for "IT Governance".

In the early efforts to communicate AS 8015, the progenitor of ISO 38500, Dr Ed Lewis, who chaired the Standards Australia committee responsible for the standard, explained that "govern" comes from a Greek word "kubernan", which he said means "to steer". At that time, the explanation seemed sound. Governance is about steering – the governing body steers management to ensure that the goals of the organisation are attained with acceptable risk. The principles in ISO 38500 could be seen as the spokes and hub of the steering wheel – the levers through which the governing body would maintain the required direction and promote appropriate behaviour as management went about the business of making decisions regarding the use of IT. Indeed the steering wheel concept even found its way in to *"Waltzing with the Elephant".*

COBIT 5 uses the same derivation from the Greek word "kubernan". At the foot of page 13 in *COBIT 5: The Framework* we see: "'Governance' derives from the Greek verb meaning 'to steer'". The explanation continues: "A governance system refers to all the means and mechanisms that enable multiple stakeholders in an enterprise to have an organised say in evaluating conditions and options; setting direction; and monitoring compliance, performance and progress against plans, to satisfy specific enterprise objectives. Means and mechanisms include frameworks, principles, policies, sponsorship, structures and decision mechanisms, roles and responsibilities, processes and practices, to set direction and monitor compliance and performance aligned with the overall objectives. In most enterprises, this is the responsibility of the board of directors under the leadership of the chief executive officer (CEO) and chairman".

At this point, most professional, experienced company directors will stop and say: "No, this is not governance! First and foremost, the board of directors is not subject to the leadership of the CEO – rather the CEO is subject to the leadership of the board. As for stakeholders, they manifestly do not set direction, though they may influence it. Further, the activities described sound very much like what the board would be expecting executive management to be doing on its behalf".

A many-faceted problem

Unfortunately, this flawed perception of governance is the foundation on which COBIT 5 is clearly built. The process model for governance and management presented in chapter 6 of the framework describes governance and management as two separate domains, in which governance has three practices (evaluate, direct and monitor) and management has four responsibility areas (plan, build, run and monitor). The reference model then goes on to identify five high level processes in "governance" which each involve the "evaluate, direct and monitor" practices, while the "management" side breaks down the plan, build, run and monitor areas into 12, 8, 8 and 3 processes respectively.

The model describing the "COBIT 5 Governance and Management Processes" presented in figure 20 of the framework at first looks very promising – it juxtaposes the governance tasks of evaluating, directing and monitoring (the organisation's use of IT) against a readily understandable set of management tasks for planning, building, running and monitoring (the organisation's use of IT). However, when considered in the light of the following text and more detailed process reference model the treatment of the concepts begins to diverge substantially. The governance tasks are used to frame the next level of detail in the five governance processes, while the management tasks are used to divide the overall set of management processes into four management domains, each of which contains a number of processes. This is quite confusing, and limits the concept of "evaluate, direct and monitor" to the internal structure of some high level processes, which is not what is intended by ISO 38500 at all.

The more detailed *COBIT 5: Process Reference Guide* sets out details of the 36 processes for governance and management of IT. In the governance set, each process is decomposed into three components – one for each "governance practice", namely: evaluating; directing and monitoring. As far as it goes, the expression of the practices is consistent with the approach described in ISO 38500. However, ISO 38500 regards these as the top level – the tasks of evaluating, directing and monitoring pertain to the totality of the organisation's use of IT, and not just to five processes that are seemingly intended to define a small set of ongoing executive management level activities.

One might ask many more questions about the way the text and models communicate the relationship between governance and management. For example, the Framework's earlier explanation of governance is very clear that governance involves setting direction, yet the process reference model contains no process in the governance space for setting direction, and in fact places the task of defining strategy (APO2) clearly and firmly in the space of management.

The root of the problem (1)

A recent, very timely and serendipitous encounter with an academic researcher looking into the role of the board in relation to information security provided what may be the key to the problem of governance and management being confused. He noted that early work on "IT Governance" analysed the origins of the word "govern" to provide a conceptual platform for the subsequent work. However, he also noted that there are several alternatives in the analysis of

origin for the word, and depending on which option is chosen, several different outcomes are possible. Choosing the wrong option would cause the wrong selection of activities to be presented under the title of "Governance".

As mentioned above, most literature on governance of IT, and the explicit statements in COBIT 5, position governance as being derived from the Greek word 'kubernan: to steer'. However, a little straight-forward research reveals other possibilities. For example, Oxford Dictionaries Online presents the origin of "govern" thus: Middle English: from Old French *governer*; from Latin *gubernare* 'to steer, rule', from Greek *kubernan* 'to steer'. Dictionary.com presents three options: 1 – to rule over by right of authority; 2 – to exercise a directing or restraining influence over; 3 – to hold in check; control. The English Word Information site at http://wordinfo.info is similar, if slightly more expansive in its explanation.

These references make it clear that in explaining the concept of "governance", a valid alternative to the notion of "steering" is the notion of "ruling". In a naval context, the Captain of a ship might be regarded as being responsible for organising and managing all the resources required to steer and navigate the ship to its destination, but the Admiral has the privilege of determining what the destination is, and checking that the captain is doing a satisfactory job of getting there.

Taking this to its conclusion, it becomes clear that the notion of govern that is consistent with modern corporate governance practice is the one of ruling – setting the overall objectives of the organisation, defining the required behaviour and performance, and checking to ensure that these requirements are met. There is no reason why this interpretation should not also apply to the specific domain of IT: Governance of IT deals with setting the organisation's overall objectives for the use of IT, defining the required behaviour in relation to use of IT, and checking to ensure that the required objectives and behaviour are being met.

The root of the problem (2)

Corporate Governance models vary around the world. International corporate governance expert Robert Tricker explains in *Corporate Governance - principles, policies and practices* a number of variations in corporate governance models. For example, in Britain and Australia, governance is usually the task of a board comprising several non-executive directors and one (or perhaps more) executive directors who are also part of the management structure of the organisation, with one of the non-executive directors also taking the role of chair. In the United States, the prevailing model seems to be one in which the board has a substantial proportion of executive directors, with the CEO often also taking the role of chair.

In many parts of Europe, however, there are often two-tiered board structures, where there is a higher level supervisory board that is composed of entirely non-executive directors, and a management board composed entirely of executives who have day by day responsibility for the organisation.

The duties and obligations of the bodies responsible for governance of organisations are usually set out in law and regulation. In Europe, where two-tiered boards are common, there are specific obligations and accountabilities defined for the supervisory and management boards.

Discussion of governance matters can sometimes become confused when the models applying in different jurisdictions are not addressed with sufficient clarity. For example, a duty that is assigned to the board in Australia may also require governance attention in Europe – but the question arises – is this a duty of the supervisory board, or the management board? Going in the other direction, a duty that is assigned to a management board in Europe may be described as a board duty – but is it actually a task for the unitary board in Australia, or a duty that should be addressed by management, under the appropriate supervision of the unitary board?

In a two-tiered board context, the interpretation of the word "govern" might result in the supervisory board being expected to "rule", while the management board is expected to "steer". Given that the executive management team in a unitary board context is largely equivalent to the more formal management board in the two tier context, it is easy to see that guidance which might have been intended for the management board in Europe has been wrongly targeted at the (unitary) board of directors in other jurisdictions, when it should have been targeted at the executive management team. A corollary of such an error would be to then regard the work of the management board in the two tier system as "governance", and to use the same tag for the same tasks in a unitary system, even when these tasks are manifestly part of the duties of management.

Governance vs Management (2)

It seems fair to say that COBIT 5, despite clear intentions expressed in the design paper, is still quite confused about the distinction between governance and management. As we explain above, one possible reason for this is a flawed interpretation of the meaning of the word "govern". But COBIT 5 has another element that raises some concern.

After presenting its explanation of governance, COBIT 5 goes on to say: "Often differentiated from governance as the distinction between being 'committed' (governance) and 'involved' (management), management entails the judicious use of means (resources, people, processes, practices et al) to achieve an identified end. It is the means or

instrument by which the governance body achieves a result or objective. Management is responsible for execution within the direction set by the guiding body or unit. Management is about planning, building, organising and controlling operational activities to align with the direction set by the governance body".

The notion of distinguishing governance and management using the terms "committed" and "involved" seems little short of bizarre. How many managers would regard themselves as not being "committed"? How many diligent directors would see themselves as not "involved"? Even in a legal context, these terms are not appropriate – there are many situations where management personnel may be held just as accountable under the law as the directors.

At the very least, it would seem that a great deal more work is required before COBIT 5 can articulate the distinction between governance and management in a way that is clear, unambiguous, and applicable in all jurisdictions, around the world.

Of course, there is an easy alternative: COBIT 5 could simply adopt and enhance the definitions provided in ISO 38500. They are already quite clear and unambiguous. Or the words of Robert Tricker could be used to explain the situation: "Management runs the business; the board ensures that it is being run well and run in the right direction".

Governance & Management as a System

The notion of governance as a system is deeply embedded in the classical definitions for corporate governance, and is carried over into ISO 38500. However, corporate governance does not operate independently of the management systems in the organisation. The board's role in oversight of finance for example both depends on and involves input to the management activities pertaining to finance. Increasingly, the same thing happens in respect of human resources. Some industries involve numerous other points of interaction between the governance and management systems.

In all these cases, it can be readily observed that there is interdependence between the governance and management systems: governance guides management; management informs governance. As such, clarity of the way that governance operates is best supported by presenting governance as an overarching system that embraces and engages with the overall management system and its constituent parts.

In addition to the challenge created by defining "governance" activities that are more correctly the domain of the upper levels of management, the presentation of governance and management in COBIT 5 does not appear to provide sufficient engagement of the real governing body in oversight of the organisation's use of IT.

As they are described, the "governance" processes may be tasks that are delegated to management as enablers for properly engaging the governing body in oversight of the use of IT. Drilling right into the process reference model does show, for example, that the "management" process for defining strategy (APO02) does involve some engagement with the "governance" processes. However, the RACI model provides only that the governing body is "Informed" of the IT strategy. This may not be a sufficient level of engagement.

Of course, we must recognise that COBIT 5 also makes it clear that the reference model is just that – a reference model rather than a specification, and many organisations will vary from the model, for good reasons.

Notwithstanding, it would seem that there is a need for considerable further work to develop and properly articulate the true systematic nature of governance and the way that governance and management of IT operate as a system.

Governance & Management Explained

Governance and Management are both defined concepts in ISO 38500. The definitions in the standard are further developed and explained in chapter 3 of *Waltzing with the Elephant*. The free introductory download of *Waltzing with the Elephant* includes chapter 3 and should be a useful resource for those who wish to establish a clearer understanding of how the two concepts are distinct, but interdependent.

Whither the ISO 38500 Principles?

ISO 38500 defines six principles for effective governance of IT. These principles are a fundamental part of the guidance in the standard, but, curiously, they do are not referenced at all in COBIT 5. However, there are frequent uses of terms that suggest some awareness of the principles and their effect throughout the COBIT 5 material. This may be because the terms would be relatively common, or it may be because COBIT 5 attempts to address the principles through process – not unexpected since the fairly obvious orientation of COBIT 5 remains to the establishment of a process model for governance and management of IT. What COBIT 5 appears to miss in this regard is the fact that principles which guide overall behaviour can result in a very high level of performance without requiring a great deal of rigour and overhead in formal processes. This should not be seen as advocating process anarchy – but rather highlighting that organisations should only define as much process as is needed, and should use other means to complement process in their pursuit of effective and efficient governance and management of IT.

Other observations on COBIT 5

COBIT 5 is an immense piece of work. The exposure draft of the framework runs to 86 pages; the reference model is 224 pages. But it's not just immense – it's also complex. It will take practitioners a long time to come to terms with it. It will urgently need additional guides for managers and other stakeholders who need to understand how it works and what it means, without getting into the detail.

The challenge in getting to grips with COBIT 5 is exacerbated by its current presentation. For reasons that a probably known only to the publisher, the documents make extensive use of very small fonts, to the extent that anybody working with it in printed form will need both a very recent eye-test with correct prescription spectacles AND a magnifying glass. Moreover, its use of colour, while highly desirable in the interests of clear communication, does result in significant contrast problems when the material is printed on a non-colour printer.

Like its precursors, COBIT 5 retains a "Big Corporate" feel. The majority of the language used is that of large organisations. Again, while the material provided does clearly say that the adoption process should develop a system for governance and management that suits the target organisation, it is likely that there will be many smaller organisations that become overburdened with bureaucracy because they, or the consultants that help them, depend too heavily on the process reference model rather than thinking through the specific circumstances that apply to each unique organisation.

COBIT 5 also appears to remain strongly aligned to the notion of an internal IT function that controls IT separately from the business and has the potential to become a "tail wagging the dog". A significant indicator of this is that COBIT 5 appears to retain the notion that IT strategy is developed separately from business strategy, while not providing any guidance on the increasingly important practice of defining the use of IT integrally with the business strategy. The extent to which modern business strategy is both driven by advances in the capability of IT and highly dependent on the availability of IT means that such integration is now critically important. Similarly, experience of contemporary major business transformation enabled by IT is that the IT elements cannot be managed separately from the other, frequently substantial work to design and implement the business change for which the IT is a key enabler.

Accordingly, the framework for governance and management of IT must nowadays provide for much deeper engagement and integration between business planning and implementation activities than was previously the case.

[top]

Infonomics Education Program

Echoing the high levels of interest in the Middle East and Latin America, Europe is now positioning itself for a major program of learning about ISO 38500.

The working group responsible for ISO 38500 meets in London from September 19 to 22. Immediately after that, I will be conducting a series of four events to present the ISO 38500 approach to governance of IT to business and IT leaders. These events are organised by PMOWorks, and will be held in:

- London 23 September
- Dublin 26 September
- Amsterdam 28 September
- Madrid 30 September

For details, see the Events Schedule or the Brochure.

We're also doing two Foundation Classes:

- London 3-4 October
- Würzburg, Bavaria 6-7 October

For details, see the Events Schedule.

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

[top]

Infonomics Access Service

What do you do when you need some insight or new perspective on how your organisation currently makes decisions about its use of IT? How do you begin investigating a situation where you are just not quite comfortable about what you are seeing or hearing? What questions do you ask when you have just received a report on a project that seems just too good to be true, or is unfathomably complex and full of babble?

The Infonomics Access Service is coming shortly. It provides business and IT leaders across the globe an opportunity to have a conversation with me, Mark Toomey, about any aspect of your organisation's current and future use of IT.

Keep an eye out for further details.

[top]