The Infonomics IT Governance Letter
October 2005

Information, news and views on Corporate Governance of Information and Communications Technology

Welcome to the Infonomics IT Governance Letter

Australia's worst-ever IT Project Failure?

Last month, in our press review, we made brief reference to "A live case study" - the move to production of the Imports Module of Australian Customs massive re-engineering program. Hardly anybody in business today could be unaware of what happened next. Ports choked on unprocessed cargo, and the year's peak load of pre-Christmas imports was hopelessly delayed. Having studied the press discussions of this project over the past two years, we can only describe it as a monumental and catastrophic failure in corporate governance of IT. For our extended discussion, please read on.

Getting IT right

While Customs took the lions share of the press headlines this month. We can learn much from these examples, but the lessons will only be truly effective when organisations ensure that they are as effective in governing their IT assets as they are in governing their financial assets. See this month's headlines for the range of discussions we have this month.

Minimise the risk of internal fraud and compliance failure

On 24 November, our foundation sponsor Advent One joins with IDC to deliver a two hour briefing on this important topic, and to formally launch IntellinX onto the Australian market. This month, Advent One have provided us with an interesting case study, describing how a bank in Israel used IntellinX to satisfy stringent security requirements closely related to the requirements of the US Sarbanes-Oxley Act and the Basel 2 Accord. To participate in the briefing, in Melbourne, please contact Greg McAllister or Bob Bassat on 03 9626-2474 or by email.

Read On...

Feedback suggests that the web-based format is the one our readers like, so we'll stick with it. We've made a few minor changes to layout this month - breaking the press coverage up into a series of topics. We hope it makes them easier for you to read.

To read The IT Governance Letter, select the pieces you want to read from the menu at left. Or just click on the "next" button at the bottom of each page to read from start to finish. We don't expect that you will read the entire letter in a single sitting. Each topic is self contained, so you may find it worthwhile to read a bit now, and come back later. Whichever way you choose to use it - we hope you enjoy it.

And if you'd like to tell us what you think, please click on the feedback button, which is in the panel at left.

If you prefer to print and take away, we've also prepared this portable, printer-friendly version. Please be aware that, for the time being, we don't have the means of putting active hyperlinks into the PDF, so if something says "click", we mean in the web-based version.

Mark Toomey

14th November 2005.

Headlines - November 2005

Australia's worst-ever IT Project Failure?

On October 12th, one day after the October IT Governance Letter was published, Australia experienced an IT project failure of potentially catastrophic proportions. The Australian Customs Service introduced the Imports Module of the Integrated Cargo System, bringing to a climax its multi-year program of re-engineering the way imports and experts are handled.

Within a few days, Australia's sea and air cargo terminals were choked with unprocessed imports. But it took two weeks for the disaster to be acknowledged to the extent that Customs allowed importers to revert to the old system indefinitely.

The damage caused by this project will be immense, and perhaps incalculable. Already, the federal government has moved to change management of Australian Customs, with the appointment announced on November 10 of Tax Commissioner Michael Carmody to the top post. But the real consequences are not in the public service. Delays in import deliveries have hurt importers, transport firms, customs agents, retailers, manufacturers and probably many others. They have carried extra costs, they have lost sales, and in some cases, the damage may be terminal.

How could such a catastrophe have developed? We spent all our spare time over the last month pondering this question. We worked through our news archives, and found mountains of material covering the Customs Cargo Management Re-engineering Project spanning two years. As we put the pieces together in sequence, it became obvious to us that the October Imports Debacle was as predictable as the crowd at the Melbourne Cup.

So we wrote a story about it. For those who like to have it on a page - we're sorry. There is a single sentence version, which reads: ***"If you don't ensure that ALL the conditions for success are satisfied, your project will fail and no amount of spin will change that reality!"*** It's ten pages, packaged conveniently in a PDF, and, according to our reviewers, it's "a compelling read". One said: "Wow - I was aware of each article, but seeing them all together in one paper is stunning".

Infonomics believes that catastrophes such as this should be avoided by effective corporate governance of IT. The news gives us some insight to the potential omissions in governance. Only a formal investigation will reveal the extent of governance failure. We hope that the investigation starts soon, is fully transparent, and that we are involved.

Do your IT projects have any of the characteristics of the Customs project? Should you check? Why not ask us how you can find out quickly?

Do you have something to say about Customs, or about IT Governance in general? Tell us, and we will publish your views in the next IT Governance Letter, due for release on December 12th.

To read the full discussion of this project, you will need to load the separate 10 page PDF available online.

Advent One introduces IntellinX – Software that detects unauthorised and fraudulent data access.

Leaders in business and the public sector are increasingly concerned by their organization's inability to respond to simple requests. Some examples:

On leakage of sensitive information or on a privacy issue:

- *Exactly what information was accessed, by Whom, When, Why and how often? Can we prove it?*

On loss of a member of staff to a major competitor:

- *By lunchtime, I need to know all the customer master records accessed or printed by X in the last six months. What was X doing with these records - authorised entries, browsing, printing or even deleting?*

Fast and accurate responses to these questions are important in a competitive world. They are also critical in handling the media and in adherence to privacy issues as well as an array of government and business regulations.

Following its overseas success, the IntellinX solution to these concerns is being introduced in Australia and New Zealand by Advent One Pty Ltd.

- IntellinX provides extraordinary auditing and control capabilities for your systems without the risk and cost of programming changes.
- IntellinX is delivered on an appliance. It is non-invasive and does not require any changes in your applications, nor does it interfere with your existing systems and procedures.
- IntellinX can be immediately productive – literally "tomorrow".
- IntellinX cannot be bypassed. It can be likened to a camera recording every passage through a doorway.
- IntellinX records every transaction and when required will produce court admissible evidence for both recent and historical transactions.
- IntellinX allows internal auditors to visually replay all end-user's activity - screen by screen, keystroke by keystroke as if looking over the end-user's shoulder.
- IntellinX business rules detect user behavior patterns triggering instant alerts on exceptions allowing the internal auditor to zoom-in on specific suspects.

IntellinX will not directly stop inappropriate or fraudulent behavior, but:

- Advertising IntellinX presence makes it a significant deterrent.
- Intellinx alerts can trigger security procedures that can promptly terminate suspicious activities.

IntellinX is unique and patent applications have been made.

Following a short interview to confirm its relevance to your organization, IntellinX can be supplied to you for fuller evaluation on a no-obligation proof of concept basis.

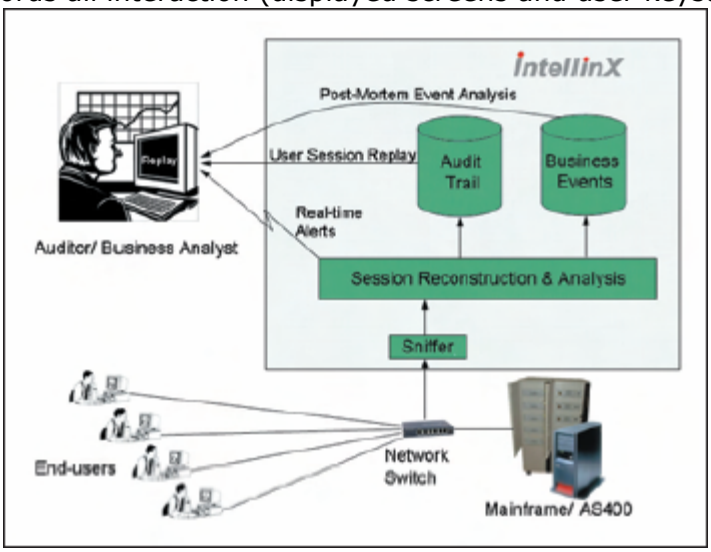
For further information please contact Bob Bassat on 03 9626-2474 or rbassat@adventone.com or visit our website at www.adventone.com.au

Stringent Compliance - an IntellinX Case Study

Following a large-scale embezzlement that eventually collapsed one of the country's small banks, Israel's Supervisor of Banks enacted Regulation 357 based in part on the Basel 2 Accord and somewhat similar to the US Sarbanes-Oxley Act. In effect from July 1st, 2004, the new regulation requires banks to, among other things, maintain a full audit trail based on computerized recordings (logs) of access, transactions and queries performed in their information systems. The logs should include the identity of the person accessing the systems, the place, time and particulars of the transaction, such as the account number accessed and the type of access (i.e. read, update, delete). The records management systems should also warn designated parties within the organization of unauthorized external activities as well as exceptional activities of the various types of users, as defined by the bank management.

Founded in 1902, Bank Leumi is Israel's leading international financial group with about 250 branches in 19 countries, over 1.7 million customers, and assets under management in excess of $100 billion. In the beginning of 2004, when the Bank of Israel published the new regulation, Bank Leumi's Head of Operations assigned a highly experienced group of managers to a task force that would coordinate the compliance project throughout the bank. One of the main challenges the team identified was creating a full audit trail of the bank's mission critical legacy applications running on the central IBM mainframe. Unlike network devices and infrastructure systems, there are typically no tools for analysing user activities at the application level, especially when the applications are developed or customized in-house. In the case of Bank Leumi, most of its applications had no embedded logging facility, so creating a log of all actions performed by all end-users required modifications to many programs in dozens of applications. The team estimated that it would require about 100 programmer-months to accomplish this task. Furthermore, additional programming resources would be needed in order to keep the logging facility up-to-date during the natural course of maintenance throughout the lifetime of these applications.

In order to meet the compliance deadline and to save resources, the Bank Leumi task force looked for an off-the-shelf software solution with logging and alerting capabilities that support the new regulation without requiring changes to the legacy applications. The only solution the team found was IntellinX, a new patent-pending technology which records all interaction (displayed screens and user keystrokes) between all end-users and legacy applications in real-time. It features zero-footprint non-invasive sniffing of network transmissions from which the original screens and user keystrokes are reconstructed. The content of the recorded screens is analysed in real time, automatically recognizing screen titles, captions and values, and user field keystrokes. The data is analysed using pre-defined rules that identify suspicious user acts or behaviour patterns, triggering instant alerts to designated personnel. These alerts allow an auditor to immediately zoom in on specific suspects and replay all their actions. The recorded sessions are stored by the system, allowing for new rules to be applied after-the-fact.



The team recommended evaluation of IntellinX during a short Proof-of- Concept. The product, installed in the bank's test environment in a few hours, immediately started recording user activity in that environment. As IntellinX runs on a separate server and there is no need to install any software or hardware on the host system or the clients, there was no performance impact on the host, clients or network, and no risk to normal IT operations. The Proof-of-Concept provided the full audit trail

required by the Bank of Israel regulation. Since this audit trail consists of very sensitive data, various security aspects were evaluated. The solution providers adhered to the bank's strict security requirements, including encryption and digital signature of the recorded data so it can, if needed, be admissible in court.

As the results of the Proof-of-Concept were very positive, Bank Leumi decided to move quickly, purchasing the product and deploying it in its production environment. Compliance was achieved by July 1st, 2004, with 24X7 recording of all mainframe end-users. Initially, the product was used out-of-the-box, allowing replay of specific user sessions and queries such as "Which users accessed which specific customer's account within a specific time range?". Subsequently, the internal auditing unit will define business rules to track suspicious user behaviour, triggering instant alerts. Defining new business rules is an ongoing process as the new rules can be applied to the data previously recorded in order to identify any irregularities that have already occurred.

For obvious reasons, Bank Leumi cannot disclose the exact rules it utilizes for fraud detection. Nevertheless, the following are examples of rules commonly applied in banking scenarios:

- Example 1 - While bank tellers normally access customer account details by entering the account number, rarely is the search done by customer name. IntellinX can detect in real-time a teller who frequently or continuously searches for account details by customer name at a rate of 3 times higher than the average rate.
- Example 2 - Accounts belonging to celebrities or bank managers are typically handled in the same way as the accounts of regular customers (non-celebrities), rather than assigned to specific clerk. When a specific user continuously or excessively accesses these special accounts, IntellinX can send an instant email alert to the designated auditor, advising of suspicious activity or malicious intent to exploit confidential customer information.
- Example 3 - Bank clerks are authorized to add beneficiaries to or change customer addresses in customer accounts. In the case where a user frequently performs these actions or if the new address or beneficiary is the same for different customers, IntellinX can send immediate SMS to the designated auditor. In addition, since the system stores all changes made by the user in a separate auditing database, an auditor can later verify if these were previously approved by the customer or are part of a fraud.

While the above-mentioned rules can detect fraudulent attempts, the fact that all user actions are recorded may further deter users from committing fraud.

After running the IntellinX recording for several months and creating a full audit trail of some 10,000 end-users, Bank Leumi has reported that there is no impact on the performance of its host, clients or network and that the recorded data, because of its extremely condensed format, occupies less than one standard PC disk. Mr. Head of Operations further states, "We are very pleased with IntellinX as a non-invasive solution for compliance and fraud detection. We are very satisfied with the support we receive from the developers and are expanding the use of IntellinX as the main logging solution for various types of client/server applications."

To enquire about attending the official Australian Launch of IntellinX, with an IDC briefing on "Minimising the risk of internal fraud and compliance failure", contact Greg McAllister or Bob Bassat on 03 9626-2474 or by email.

Self-assessment result

A broad spectrum of results from a diverse and open audience

On October 25th, 2005, twenty seven customers and guests of Corporate Information Systems Pty Ltd (CIS) attended a breakfast briefing, at which Infonomics Principal Mark Toomey discussed the intent of the Australian Standard for Corporate Governance of ICT (AS8015).

During the session, Mark asked participants to briefly assess the IT Governance performance of their own organisations, using 12 high level indicators of good governance performance. The indicators reflect behaviour and performance. The test assertions are:

G1 Governance system:	You have a system for governance of ICT.
G2 Management compliance:	Everybody understands and complies.
G3 Effective protection:	It protects you from ICT failures in operations and projects.
G4 Inform & engage:	It keeps management and directors properly informed of ICT status.
G5 Dependence understood:	Ongoing business dependence on ICT is well understood.
G6 Continuity & sustainability:	ICT adequately protects business continuity and sustainability.
G7 Business alignment:	ICT capability matches business needs and forward plans.
G8 Resource allocation:	ICT resource allocation matches the needs of the organisation.
G9 Business innovation:	Use of ICT balances business innovation against risk.
G10 Investment value:	ICT investments deliver results as per a formal business case.
G11 Deployment capability:	Demonstrated capability to deploy ICT initiatives matches aspiration.
G12 Acceptable risk:	The business risk of serious ICT failure is understood and managed.

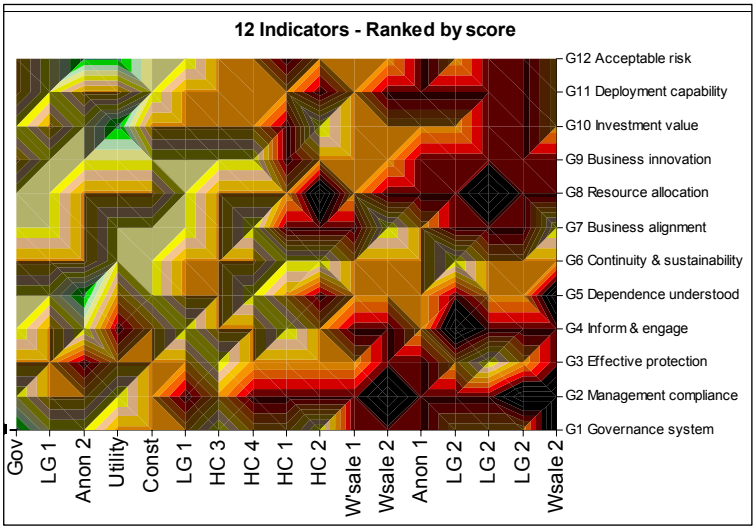
The indicators were ranked on a simple scale that translates into colours on the charts:

4 - ■ "Absolutely!" (Very well). 3 - ■ "Yes…" (Reasonably well) 2 - ■ "Sort of" (A little)
1 - ■ "No" (Definitely not) 0 - ■ "huh?" (The organisation generally does not understand this concept)

The 17 complete responses give some insight into IT Governance effectiveness in 11 diverse organisations. Organisations providing input included local government (LG), a state government department (Gov), a construction firm (Const), health care (HC) providers, wholesale/distribution companies and an infrastructure utility company. Two responses did not identify their sources.

A Key Performance Indicator shows persistent weakness!

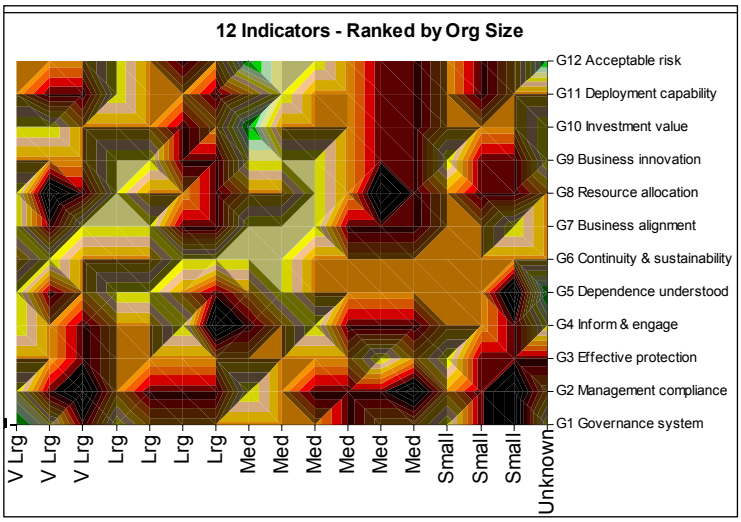
Recent research by world-renowned Australian Academic Peter Weill confirms a link between the extent of management awareness of and compliance with the organisation's system of IT Governance, the organisation's success with the use of ICT, and bottom line business performance. History shows that many IT initiatives are technically successful, but fail to deliver business outcomes. A majority of clearly identified ICT project failures are attributed to problems with business engagement and strategic alignment.



The responses map at left ranks performance from best (left) to worst (right). Its design provides a 3 dimensional profile where lower scores appear as peaks and ridges, while strong scores appear as valleys. The common themes of ICT project failure clearly stand out. As in a recent similar survey conducted among 60 IT Auditors, most attendees at this session ranked management compliance (G2) as being weak. It is quite noteworthy that this weakness also corresponds strongly with poor scores allocated

on other topics, such as deployment capability (G11), business alignment (G7) and resource allocation (G8). Other areas which indicate broad issues include lack of confidence in protection of business continuity and sustainability (G6), and a lack of confidence that IT investments always deliver value – a result that matches findings in KPMG's biennial Global IT Project Management Survey, released in September 2005.

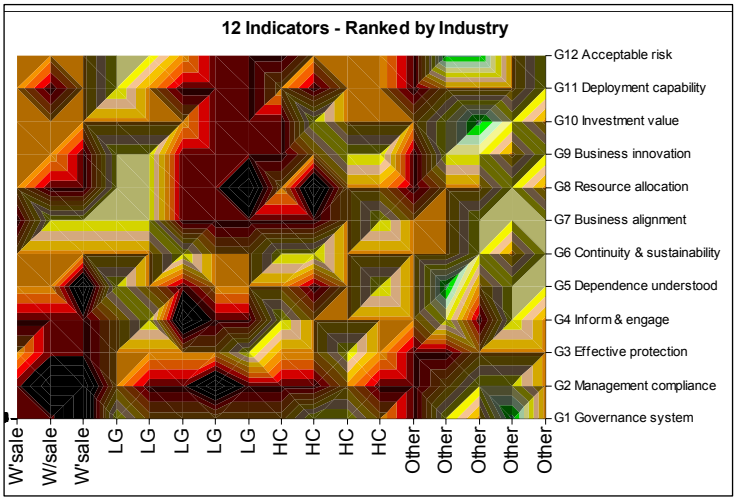
Size makes little difference



Small organisations have few managers, and the managers are generally across most of what's happening, and informal governance should be successful. But, small organisations often experience limitations in areas other than day to day operations. Note the weak scores around dependence (G5), continuity (G6) and deployment (G11) for small and medium organisations.

Diverse scores across the rest of the sample, indicate that organisation size probably has little to do with IT Governance performance. Notice how some organisations appear to have uneven performance – good in some areas, not so good in others – while others exhibit uniformly poor performance. See also that weakness in informing and engaging of managers in the IT Governance process (G4) tends to be most closely associated with organisations that have generally poor ratings across all the indicators.

Neither Industry, reporting lines, package use nor method of sourcing IT show themes.



In this chart the data is clustered according to the industry from which the response emanated. Each individual response is plotted, and there is no levelling to reflect that several people may have responded in respect of a single organisation. Similar plots were developed (but are not presented due to space restrictions) for IT reporting lines, the use of packages vs custom solutions for the main IT systems, and insourcing vs outsourcing.

Across all of these views, the patterns remained quite scattered – with stronger and weaker performers in all categories. There is room for improvement in all situations. Lessons may be learned from better performers.

What is your situation?

The results of this mini-survey are consistent with prior surveys and broad industry understanding of IT Governance performance. Relatively few organisations can claim persistent long term success with ICT – and poor governance is a hallmark of failures. If you honestly assess your organisation with the 12 indicators, where will you rank? If you can't score a solid 36 of the possible 48 points, you may have an unacceptable risk, and you should consider a more formal assessment of your IT Governance performance.

The Best Governance?

What are the criteria for being good at IT Governance?

On 12 October 2005, news articles reported that Telstra had scored top marks for corporate governance in the Horwath 2005 Corporate Governance Report, which rates the corporate governance practices of Australia's top 250 companies by market capitalisation. Does this make sense? Haven't we been hearing recently that Telstra has made some major errors with investment in its infrastructure? Are these outcomes compatible with good corporate governance?

Horwath's methodology is based on examination of the organisation's annual report. It refers to best practice guidelines from diverse sources, and includes several Australian sources.

It is very interesting to note that a number of organisations in the top 25 of the Horwath rankings have experienced difficulty with IT of some type in recent times. For example, the Crane Group, which shares equal top ranking with Telstra, AMP and the Commonwealth Bank was the subject of several announcements arising from a difficult IT project.

We think that these results underpin the view that boards are frequently poorly equipped to objectively evaluate the IT situation for their organisations. And they are unable to determine, with any confidence, whether the management practices that have been adopted for the control of IT and IT enabled business change are effective.

How can boards become more effective in their assessment of IT? There are numerous options. Infonomics provides key services in this area, to build understanding, and to provide insight regarding the organisation's situation.

To encourage organisations to act promptly, and make sure that their IT activities will not put them in the same situation as Crane, or Fox Meyer Drug Company, or Australian Customs, Infonomics is continuing its promotional offer for engagements signed-up by November 30th.

IT Governance Assessments are cheaper than you might imagine

There are compelling messages that organisations must improve their top level governance of IT. The payback is intuitively obvious – reduced risk and improved business performance, with no adverse publicity – all of which contribute to higher profits and better share prices. The benefits are not hypothetical – there is solid academic research by leading researchers such as Peter Weill and Raymond Young that demonstrate conclusively – investment in good ICT Governance creates economic value.

Have most organisations already got good IT Governance? Many would like to think so, but the frequency of significant problems in both operations and projects says that few have it working well. Infonomics hands-on experience of organisations we have assessed indicates that there are substantial opportunities for improvement, and that the major improvements are not actually all that difficult to put in place.

Checking that your IT Governance is working need not be expensive. If you call in a major advisory firm, they might charge you a six digit sum to have a look and tell you what they should do next. A specialist like Infonomics will charge you much less, and tell you what YOU should do next. Our premier product – the AS8015 Alignment Diagnostic is unlikely to cost more than $50,000 for even major listed organisations.

To promote higher performance in Australian organisations, and success in the way that they use IT, Infonomics is reducing the prices by 10%, for work that is booked 10 October to 30 November 2005. These reduced prices are only available to readers of "The IT Governance Letter" and must be claimed when the engagement is booked.

- The **AS8015 Alignment Diagnostic** gives you an 84 point assessment of the performance and effectiveness of your IT Governance model, and informs your senior people about what is important. A typical IT Governance Assessment with input from 20 senior people and perusal

of key planning and control documents would normally cost $40,250. The special price is just $36,225.

- The **ICT Investment Business Case Assessment** helps you check that your proposed investments in ICT make sense. A typical ICT Investment Business Case Assessment with input from 12 senior people and perusal of key business case documents would normally cost $32,800. The special price is just $29,520.
- The **ICT Investment Project Assessment** helps you confirm that projects remain on track, with good prospects of delivering business value. A typical assessment takes input from 12 stakeholders, and peruses a wide range of project outputs. This service would typically cost $36,000. The special price is only $32,400.
- The day long **IT Governance seminar** helps your senior business and IT people develop shared understanding of what is important in making sure that the use of ICT supports the business and delivers value with appropriate levels of risk. Past participants have applauded the way the seminar takes the mystery out of IT for business managers, and gives them a new framework for their engagement in the IT process. Normally $8,800, the seminar is now offered for just $7,920, for up to 15 participants.

To qualify for our special offer, participating organisations will need to provide a firm order by close of business on 30 November 2005, with the engagement to be completed by 30 June 2006. This offer is open to all readers of "The Infonomics IT Governance Letter", including those who are reading forwarded copies. Final pricing is dependent on the exact dimensions of the engagement, and will be calculated using our pricing schedule which is available on request.

For the Board

IT governance has become critical to enterprise success: CPA Australia

The profile of IT as an important corporate governance issue continues to grow. Hard on the heels of the KPMG Global IT Project Management Survey comes a publication from CPA Australia, entitled "IT Governance: A Practical Guide for Company Directors and Business Executives". For information and ordering, please refer to the press release on the CPA Website

Principal author of the CPA Guide is Chris Gillies - one of Australia's leading practicing company directors with strong hands-on IT experience. She is backed up by a leading academic and Gartner researcher, Dr Marianne Broadbent. Chris Gillies is a long term friend of Infonomics, and has been instrumental in the establishment of IT and business change governance at board level for organisations such as Centrelink and Bendigo Bank. The very practical 59 page guide is peppered with illustrations based on real world experience, and contains numerous straight-forward checklists that directors and executives can use to see whether they have adequate coverage in their IT Governance.

The guide is backed up by a CD with a single file that provides spare copies of the tables and checklists in the document, so reviews can be done over and over again.

Infonomics applauds the CPA initiative to further spread the word that IT Governance is a vital matter for executives and directors. The messages in the guide are entirely consistent with the messages in the Australian Standard.

For the CIO

Good IT Governance is Career Enhancing

Quite regularly, particularly in US based press, one reads of CIOs having poor career prospects and short tenure expectations. CIO's often struggle in their roles, not because they are incapable, but because the expectations under which they labour are unrealistic.

This problem stems, in our view, from the lack of real understanding of IT issues in broader management roles, and in the boardroom. What this leads to is an expectation that the head of IT, or the CIO, is responsible for every aspect of IT - including how the organisation uses it. Such expectation leads to business managers avoiding responsibility, and IT managers being held accountable for matters well outside their control.

How many well meaning CIOs have identified and championed strategic projects, right to the point of implementation, only to find that the business is not ready, and not intending to take advantage of the new capability. How often does a senior executive with little comprehension of IT complexity fall to the seductive charms of a solution vendor, committing the organisation to an IT based adventure that costs a fortune, disrupts all that is critical, and has only a vague chance of delivering anything useful?

Smart CIOs avoid these problems by acting to improve corporate governance of IT. They make sure that the executive and the board know just how fundamental IT is to the business, and how effectively it is being used. They ensure that the essential processes are in place, and working properly, to control all stages of planning, delivery and operation, so that there are no wasted opportunities, no roadblocks to business and no blind alleys that could in the future create disruption.

Many of the resources we have identified for executives and boards are also entirely relevant to CIOs. Our services help CIOs ensure that their roles are well understood, with proper and appropriate boundaries, and no unreasonable expectations.

Do CIOs matter?

In its report on SEARCC 2005, held recently in Sydney, Computerworld asked "Do CIOs matter?" The article repeats the view that CIO careers are often damaged by IT projects that fail to deliver expected return on investment, with the CIO having been too focused on technical issues and not giving enough attention to the non-technical. It suggests that in future, CIOs will need to be much broader in their outlook, with strong business leadership, financial analysis and operational execution skills.

Infonomics agrees that this is the future for CIOs. It raises an important management and governance issue: Are we developing CIO skills appropriately?

In another article in Computerworld on 12 October, Australian Computer Society President Kumar Parakala said that CIOs still have a long way to go in becoming recognised as business leaders. The article again reinforces the view that CIOs need to be boardroom savvy, able to position the entire portfolio of IT activity in the context of business need and priority.

Growing CIO Skills

A CIO Magazine article "The Road to CIO: How to Prepare yourself for the Top Spot" continues the theme and gives the aspiring CIO five steps to becoming more business oriented. We particularly like point 5 - "Find a mentor". Often, a limiting factor for people who have risen tot the top of the IT tree is the fact that they have precious little exposure to the business and boardroom culture and language. It's pointless to exit somebody who understands your systems and technology intimately, simply because they have not had an opportunity to learn in a wider context. In many cases, a good mentor, and perhaps a coach, can add breadth to an individual who already has more than enough depth.

Taking this a little bit further, we sometimes encounter the self-defeating argument that "we can't take the CIO into the executive meetings and boardroom because we can't understand him or her". Well, if we never put the CIO in that situation, he or she will never learn, and will never gain the insight they need to adjust the way they communicate.

Innovation

Ongoing developments in information and communication technology create opportunities for organisations to change the way they operate, or to offer new services and products. Sometimes the

innovation can be so profound that it changes the rules for a marketplace, giving the innovator a major advantage over the competition.

It's not the purpose of the IT Governance Letter to expound all the opportunities for innovation. What we are interested in is whether or not organisations have the appropriate disciplines in place to identify and take measured advantage of appropriate opportunities to innovate. This is a matter for all boards, which should be setting the organisation's posture in terms of the risk it is prepared to take in seizing on advanced technology, or staying long term with established, and perhaps redundant technology.

In a timely warning, Computerworld (October 10th) warns that business needs to take responsibility for technology investments, to ensure that resources are not wasted on ill conceived IT projects.

To illustrate the extent of possibilities, The Australian Financial Review on 4th November reports on a new online conveyancing pilot, that could reduce the cost of a typical house purchase. This is a clear example of an industry approach, driven by the major banks, to employ technology to fundamentally redefine how the conveyancing process operates.

Success Stories

Not all IT investments go bad. In fact, some organisations have a remarkably consistent track record of getting IT exactly right. Nor surprisingly, most of them recognise this as a strategic advantage, and keep it quiet. But there are always a few good stories and it helps when they are told, to balance the depression we might feel when confronted by unending tales of disaster.

Where are they?

As always, we look through our daily news feeds and the hard copy papers, seeking out stories that give us lessons on effective IT Governance. Perhaps it's because of the overwhelming focus that this month has had on what's gone wrong at Customs - but we can't see anything in our clippings that ranks as a definitive good news success stories.

Sure there are a few cases where IT costs have been cut, and IT has been sed to shave at the margins of business cost. But we seem to have missed out on any big good news items.

Perhaps our readers would be good enough to let us know of significant success stories, where organisations have used IT to make a real difference.

Trouble Spots

Of course, Customs has presented us with the major trouble spot for the month. But it's not the only story in the past month where IT has been associated with problems.

Some time ago, Insurance Australia Group introduced a new approach to obtaining quotes for smash repairs, with repairers no longer inspecting the damaged vehicle, but working from digital photographs. The scheme has been controversial, with operators saying that it will reduce quality and compromise safety. Now, according to The Age on November 9th, the NSW Government is looking into the scheme, through an independent investigator.

There is a linkage between this story and the one at Customs. In both cases, IT is being used as an enabler for a transformation of the way an entire industry operates. The challenge in such transformation is less likely to be the complexity of the technology, as it is the complexity of achieving an industry wide agreement that the changes are necessary, appropriate and acceptable. The continuing objections from the smash repair industry suggests that in this case, agreement has not been reached.

Some other, more or less mundane examples of trouble with the use of IT are:

- The Age reported on November 9th that National Australia Bank will refund $21.6 m to overcharged customers, because of incorrectly applied penalty interest rates. The article doesn't make it clear whether or not this was an IT related problem, but our experience is that such situations often occur when rules built into software are forgotten, or improperly managed by business users and managers. There are continuing risks for business that the extent of automation in IT systems results in the business being deskilled, and subsequently surprised by unexpected outcomes from systems operating exactly as designed.
- Significant embarrassment for Westpac bank reported in The Australian on November 3rd, as an email "escaped" prematurely, bringing forward the announcement of the bank's results by two days. As numerous cases have shown of late, the instantaneous nature of electronic communication can be problematic. It may be time for organisations to think seriously about how they categorise and control the flow of information through electronic portals, not merely as a protection against spam and viruses, but for legal and competitive reasons, and to ensure that they maintain appropriate standards of quality in their dealings with external parties.
- Again on the email topic, Telstra announced (Computerworld, 19 October) that it cannot store customer email indefinitely, and would commence deleting messages more than 120 days old. One wonders how this might affect individuals and small business operators who do not have the technical savvy to save their emails for long term retention.
- We've heard a great deal of late about how Australia's national communications infrastructure is not doing so well. In The Australian Financial Review of November 4th, we find a further discussion that says Australia is missing out on opportunities for business because our broadband infrastructure is too slow and too expensive. It compares Telstra services with Deutsche Telekom offerings of similar price, and reveals that German customers enjoy eight times the bandwidth, and suffer no download limits.

Compliance

New legislative and regulatory requirements are driving a heavy workload of compliance for many organisations. And for many, the sources of compliance pressure are no longer just local. In particular, we keep hearing that the US Sarbanes-Oxley Act creates requirements for organisations that trade in the US, even if they are not domiciled in that country.

So it's not surprising that there is a good deal of discussion of compliance issues in today's press. There are numerous areas where top level executives and boards need to pay attention, even if it's only to be sure that all of the compliance requirements have been identified, and dealt with.

Computerworld raises an issue for many firms with older systems, in "Mainframe users struggle with new compliance measures". The focus of the article is a technical challenge in meeting new rules for keeping credit card transaction data secret using encryption tools. It serves to remind us that changing business conditions eventually mean that software does "wear out" and needs to be replaced with new, better structured and more flexible solutions. Organisations need to consider whether their compliance load is a driver for replacement of systems rather than continued maintenance.

In "Compliance spend a missed opportunity" on October 19th, The Age refers to a KPMG survey that shows organisations are not capitalising on opportunities driven by new compliance requirements. Instead of addressing compliance from a business perspective, and taking the opportunity to overhaul practices, organisations are focusing on adjusting just the IT systems. This approach is at odds with the reports in last month's IT Governance Letter, which reported a US survey that shows business benefits accruing to organisations that take a business improvement view of compliance.

The Age also noted that compliance work tends to be fragmented, meaning that the higher levels of management and the board have difficulty forming a view of how much compliance work is happening, how much is yet to be done, and whether there might be business opportunity inherent in the compliance process.

Legal Matters

It's unlikely that Infonomics will ever step into the field of offering legal advice. But we do have concerns that the increasing penetration of IT into the core of business raises legal risk, if there is not proper consideration of the legal aspects of IT use in projects and operation.

Software Licensing

One matter of considerable importance is a subtle change in copyright legislation that has come about in conjunction with the US Free Trade Agreement. Previously, a copyright breach was classified as a civil matter. Suddenly, it's become a criminal matter. That means, among other things, that using software without a proper license may leave individuals and organisations open to criminal proceedings. The Business Software Association of Australia (BSAA) is waging a strong campaign for compliance, and has plenty of relevant information on its web site.

What's important for organisations is that they have the processes to ensure, and demonstrate, that they have the proper licenses for all software in use by the organisation.

Record Keeping

We've mentioned email elsewhere in this month's letter, and in past editions. But the topic simply won't go away. Emails are crucial business records, and organisations that don't retain them properly are at significant risk. But, as CIO Magazine explains in "Juris E-Prudence" it's also possible to store too much information with an email. This substantial article is a "must read" for all who are concerned that their organisation keeps proper legal records.

Workplace Surveillance

Use of technology to monitor what employees are doing in the workplace is coming under constant scrutiny, as the need to protect against inappropriate conduct butts up against the rights of individuals to privacy. The debate does not limit itself to the use of security cameras - it includes email filtering and monitoring tools, and the overt and incidental use of tracking devices. In "Call for National Workplace Surveillance Legislation", CIO Magazine explores an emerging move to common standards across Australia, which should give greater clarity to organisations regarding the appropriate controls for, and limits on the use of surveillance tools.

Digital Evidence - a New Milestone

Age journalist Nigel Carson wrote on October 25th about a precedent set in the Australian Federal Court. In "Digital fingerprint cracks the case", Carson reports how Judge Murray Wilcox relied on "digital evidence from forensic computer specialists", when finding that Kazaa (a file sharing system) was illegally authorising copyright infringement.

Theft of emails

On October 28th, in "Bosses face court over hacking", The Australian reported on charges laid against two executives after allegedly stolen from a competitor's email system. While perhaps the tip of an iceberg, this article opens up the question of just how easy it might be for sensitive information to be accessed inappropriately, and copied by people with unscrupulous intent. How long do unused screens remain active while unattended? What measures are used to control the use of ubiquitous finger-sized storage devices that can hold more data than most computers of just a few years ago?

Snippets

That's just about it for the November IT Governance Letter.

But just before we go, we thought we should share a couple of brief points:

Value in Obsolescence?

We all know that some organisations have kept old systems - hardware and software, running way beyond their "use by date". It's a practice that's been going on for years, and despite our best efforts to improve governance, it will continue.

What's amazing is the length that some organisations will go to to keep their clapped out systems running - and the money they will spend to do this. We've heard in the past of banks buying pallet loads of teller terminals from South America. Recently, we had a close-to-home experience. Somewhere along the way, the Infonomics storeroom had captured a perfectly good, but utterly useless IBM PS/2 computer. We had a cleanout and despatched said computer to the recyclers. A week later, we learned of a local organisation that has software that will only run on that model, and they had just paid $3,000 each for 12 of them. That's three times as much as a contemporary basic PC! Surely it's time for that organisation to bit the bullet, and rework the software so it's able to run on modern, cheap hardware.

Passwords Unsecured?

During the 1980's, I was working in the UK, and became a customer of one of the major UK banks. Their ATMs offered a facility for selecting your own PIN, and of course, I employed it. At the time, I was horrified to see that, having entered the secret new PIN, the ATM then asked me to confirm that it was what I had entered, by displaying it back to me - in nice big clear numerals that could be seen by anybody watching me. Of course, we all know now that the proper way to verify secret things like that is to enter them twice.

That applies to user selected passwords too, doesn't it?

And having entered a new password twice, isn't it fair to assume that we can remember what it is?

Some web sites seem to still use the practice of sending an email to registered users, to inform the user of the password that has been chosen. In one case we expereinced recently, the email gave me my user id and password, toghether in a single email.

Why worry you say? Well consider this:

- Emails are not secure. They can be intercepted en route, and copies are often retained at waypoints. Any number of people can, and possibly have read that email, and have access to my user id and password for that web site.
- Many people make extensive use of the internet, and so are registered on many web sites. It is very difficult to manage the establishment of unique user ids and passwords for so many sites - so a lot of people use a standard practice of using a standard name and password. That's fine, as long as the user id and password are going to remain secret.
- But as soon as one website operator releases the username and password together in an email, that user's access to all websites with that identifier becomes open season.

The lessons here are twofold.

- Don't trust website operators to keep your data confidential; and
- take great care to use unique, and truly secret passwords on all websites of importance, such as your bank!

Events

AS8015 Briefings

AS8015 is the Australian Standard for Corporate Governance of Information and Communication Technology. It was developed by a Standards Australia committee, and published in January 2005. AS8015 provides guidance for company directors and their public sector counterparts regarding why it is important for boards to govern the use of ICT in their organisations.

On December 5th, Mark Toomey will brief members of the Australian Computer Society IT Quality SIG, again expanding on the key messages of AS8015.

On November 24th, Mark will address the annual ITSSA Conference of Victorian TAFE IT Managers, in Moama. The topic - the lighter side of IT Governance - things that have gone wrong.

AS8015 In-depth Workshop

The workshop we offered last month didn't happen. There were not enough enquiries.

Forward Agenda - what do you want to know?

It does seem that Governance of IT is a topic of considerable interest, with large audiences at a variety of briefings. But, there weren't enough takers to make a close look at AS8015 viable.

So, we are asking you, our customers, to tell us what you want in terms of information, education and support for your IT Governance improvements. Please think about it for a moment, and hit the feedback button to send us a message about how you think we should be bringing the message forward.

Our sponsors

We are delighted to welcome back our first sponsor for the IT Governance Letter. Advent One designs and implements business and infrastructure solutions based on IBM software, infrastructure, services and financing options. Of particular interest is their new offering - IntellinX - Software that detects unauthorised and fraudulent data access.

Infonomics welcomes sponsorship enquiries. Our monthly IT Governance Letter is evolving in scope and form, and its circulation base. Our readers range from senior members of the company director community, through senior business and IT executives, consultants, project managers and business change agents.