



IT GOVERNANCE
ROUNDTABLE:
IT GOVERNANCE TRENDS

IT GOVERNANCE ROUNDTABLE: IT GOVERNANCE TRENDS

IT Governance Institute®

The IT Governance Institute (ITGI™) (www.itgi.org) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI developed *Control Objectives for Information and related Technology* (COBIT®), now in its fourth edition, and Val IT™, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer

ITGI (the 'Owner') and the author have designed and created this publication, titled *IT Governance Roundtable: IT Governance Trends* (the 'Work'), primarily as an educational resource for control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

© 2007 IT Governance Institute. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ITGI. Reproduction of selections of this publication for internal and non-commercial or academic use only is permitted and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

IT Governance Institute

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

Acknowledgements

Participants

Paul Williams, Consultant, Paul Williams Consulting, UK
Jan van Puffelen, Principal Architect, Unisys, The Netherlands
Luc Chauvin, Senior CIO, Flemish Government, Belgium
Daniel Evrard, Partner, PricewaterhouseCoopers, Belgium

ITGI is extremely grateful to Unisys for hosting both the European Summit on IT Governance and the roundtable on which this document is based. The institute considers it an honour and a privilege to have had the opportunity to join with Unisys, PricewaterhouseCoopers Belgium and CIONet in sponsoring the summit.

ITGI Board of Trustees

Lynn Lawton, CISA, FCA, FIIA, PIIA, FBCS CITP, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, FHKCS, FH KIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph. D., CISA, CISM, CPA, KPMG, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

ITGI Affiliates and Sponsors

ISACA Chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum

Acknowledgements *cont.*

Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
B Wise B.V.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

On 3 September 2007, I had the unique opportunity to sit around the table with three esteemed colleagues and discuss the state of IT governance—generally and in their enterprises and those they serve. I was joined by:

- Jan van Puffelen—a principal architect with Unisys (The Netherlands) who works on delivering passive to proactive IT governance to customers
- Luc Chauvin—a senior chief information officer (CIO) with the Flemish government, which currently serves 13,000 civil servants but has a goal to double its customer base
- Daniel Evrard—a partner with PricewaterhouseCoopers (Belgium)

I explained to this august group that I had two primary goals for our one-hour discussion: (1) to produce at least one, possibly two, articles based on our conversation, and (2) to learn more about the real-life situations professionals are facing with regard to IT governance and see if we could identify ways to improve what is currently being done to address those situations.

We had this opportunity to gather in a room because we were all attending the European Summit on IT Governance, hosted by Unisys at its beautiful facility in St. Paul de Vence, France, and cosponsored by PwC Belgium, CIONet, and the IT Governance Institute (ITGI). The event was attended by approximately 35 representatives of the C-suite, predominantly from the European offices of multinational companies. The summit focused on the principles, processes and practices for value management; the leadership role of the CIO; and the cultural changes required by enterprise to achieve better business-IT alignment.

ITGI is extremely grateful to Unisys for hosting both the summit and the roundtable on which this document is based. We also appreciate the candor and enthusiasm with which Jan van Puffelen, Luc Chauvin and Daniel Evrard engaged in the discussion.



Paul Williams
Chair, ISACA/ITGI Strategic Advisory Group
Past ISACA/ITGI International President

How are people/companies defining the term 'IT governance' in your areas?

Paul Williams (PW): Of course, there are many different definitions of IT governance. I find that when I'm in the US, there is a very heavy compliance angle, and of course, compliance is a very important part of IT governance. Meanwhile, in Europe, specifically the UK, IT governance is more value- and performance-based, with compliance, whilst still important, taking less of a center-stage position.

Luc Chauvin (LC): It's interesting because I was in a meeting on the subject not long ago and we spent about half an hour trying to define IT governance. We made a distinction between IT governance and IT management, which we believe tends to focus on ITIL¹ and CMMI.² When we talk about IT governance we are talking about value creation for the business. Are we doing the right things? Are we spending our limited resources—be they money or people—on the things that will provide the best services to the citizens? Everything that has to do with what to do and how best to use our resources we call IT governance.

Jan van Puffelen (JvP): I agree with that definition. There are two problems with IT governance. First, explanation and buy-in needs to come from the CIO level and above. Anytime I've seen it introduced at a lower level, it fails. Perhaps it can work, but I haven't seen it. Lower levels tend to oppose or passively reject IT governance because they don't want what they initially see as tighter controls over their operations. That's a very strong force. IT governance only works, in my experience, if the CFO or someone of board level slaps his fist on the table and says, 'We *are* going to do this'! The second problem is making clear to the lower levels what the positive aspects of IT governance are. Our group has developed an IT governance game to try to get this message across. The game is played with key players of the organisation and it illustrates why IT governance is so powerful and positive.

Daniel Evrard (DE): To me it is all about a structured framework for IT governance. People become confused over where the boundary is between IT governance and IT management practices. IT governance helps the enterprise meet objectives, keep direction, achieve compliance, and understand roles and responsibilities. It's a link between strategy and IT management.

PW: I think it's interesting that you are talking about doing the right things. I quite agree. As John Thorp's 'Four Ares' model³ states: Are we doing the right things? Are we doing them the right way? Are we doing them well? Are we getting the value? It has always seemed to me that the 'are we doing things the right way' side is very much in the arena of COBIT⁴ and ITIL. Doing the right things and getting value from them—that's IT governance, and that's where we were coming from in putting together the Val IT framework.⁵ We thought companies were beginning to focus on those two areas but didn't quite have the right tools for doing it. Doing the right things is where it all starts. I also think it's interesting you have said this needs to be led by the CIO. I wonder where business management fits in. There should be a direct alignment between business management and IT—a move toward business governance of IT, as opposed to IT governance of IT, so there's a direct link between what happens in IT and what happens in the business.

JvP: I agree that there should be this connection—but at the board level, if you are going to have one champion, it should be the CIO or the CFO.

¹ IT Infrastructure Library

² Capability Maturity Model Integration

³ Based on the 'Four Ares' as described by John Thorp in his book *The Information Paradox*, written jointly with Fujitsu, first published in 1998 and revised in 2003

⁴ IT Governance Institute, *Control Objectives for Information and related Technology*, USA, 1996-2007, www.itgi.org

⁵ IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework*, USA, 2006, www.itgi.org

IT GOVERNANCE ROUNDTABLE: IT GOVERNANCE TRENDS

LC: The fundamental problem, as I see it, is that we are lost on IT governance because we have no business governance. So the first question is: how is IT perceived and positioned within the whole circle of managing requirements? In our case, IT is on the board. But IT is perceived as supporting the business, so it is very difficult to start talking about business cases, about benefits vs. costs, about prioritisation of things you want to do. Actually, the only way you can do that is by linking it directly to the business. So, I agree that IT governance has to be supported by the ‘top guys’; if you don’t have them, you are lost. We are currently working on many new IT governance models using advisory boards, working groups and think tanks—all the right things—but the ministries are not involved. So, from that point of view, we will probably have a very small probability of implementing a strong governance model.

PW: That’s not just a public sector issue, it’s something I come across in the commercial sector all the time. Governance will happen in the right way only if you have proper engagement at the board of directors and the top of the business, and that really means having IT represented at that highest level. There is certainly a big disconnect if you don’t have the CIO on the board, or if he or she is reporting to someone on the board who doesn’t have the same breadth of understanding of what IT is all about. That lack of engagement between IT and the most senior levels of the business is still a big issue in a lot of places. I write quite a number of articles, particularly for a UK publication called *ComputerWeekly*, and about a year ago I wrote an article about CIOs and the board—that if the CIO wasn’t actually a board member, then the board member responsible should have enough IT expertise to ensure that there is a meaningful discussion of IT at the board level. In fact, I said I thought that the CIO *should* be on the board; particularly for enterprises that are highly IT-dependent, they are missing out on a great deal if they don’t have that person on the board. From that article, I got so many and such varied responses. Most were saying, ‘Yes, you’re absolutely right’, but others said, ‘The CIO is never going to be on the board, IT is just a support thing, get over it!’ Is this an issue you are dealing with?

DE: The culture of the company is also key, as is the strategy. In large, decentralised organisations, it is more difficult to get access to the board. Further, if the corporate culture is more ‘federal’, where business has more autonomy in running its activities, it is even harder to get a common vision and decision-making model on IT. And IT is not the only one—marketing, HR, others also have difficulty reaching the senior ranks.

JvP: If a CIO is not a member of the board, then I would not consider that person a CIO. He is an IT director, or something like that.

PW: Yes, the names can sometimes get in the way. I suppose we are talking about the person who is in primary charge of IT. Is that person on the executive team sitting on the board or is he one or two steps removed and is therefore reporting through someone?

JvP: Often, a CIO who is not on the board will report through the CFO and, therefore, the buck stops there (with the CFO) and the CFO is ultimately responsible for IT at the board level. The problem is that the CFO usually has no feeling for IT. He is concerned only with what projects cost—and, of course, it is a great expense.

PW: Yes, that is quite typical, with CIOs reporting to CFOs, probably because accounting departments are often where IT got its start in a company. If you talk to those CFOs, many will admit that their understanding of IT is very limited; so, since they are not the right person for the job, IT ultimately does not always get effective board representation.

JvP: This is not statistically tested, but I would say that 30 percent of businesses have no direct representation of the CIO on the board. The old joke is that IT projects *cost* money, whilst business projects *earn* money. Things are now very different. IT projects do not exist anymore; there are only business projects with a smaller or larger IT component. That implies that the business has to be involved in IT; otherwise, you cannot have a joint project. It also means that the goal is no longer lower costs, but higher profits. We may not be entirely there yet, but the change is happening.

DE: Regarding the issue of having someone sitting on the board, the way we solved it in some circumstances was to have a steering committee, with representatives of the different business units who are literate in IT and able to represent and defend IT in their line of service and business unit. The steering committee will report to the board. We are now setting up the strategy, prioritization and internal direction—and doing it with the business people.

PW: I think that can work well but, in my view, there still needs to be someone sitting on the board who is sufficiently knowledgeable about IT and the business to really drive it. Some of the steering committees I have seen are ineffective because they haven't got the right leadership—the leaders are just not as engaged as they should be. I recently did a consulting engagement with a London bank and part of my report was that the steering committee was not effective because it didn't have the right leadership. As I was presenting that portion of my preliminary report to the board member responsible for IT, he responded, 'Yes, it does have appropriate leadership—it's me. I am the chair and I am a board member'. I said, 'Yes, I know you're the chair. But I've had a look at the minutes for the last year and a half, and it appears you have not actually shown up to chair a single meeting'. It all deteriorates from there—when leadership is not engaged, people gradually start sending their deputies, and sooner or later it devolves into a sort of user group, which is a very different thing entirely.

Why do so many big business-related IT projects go wrong? What role does governance, or lack thereof, play in the failures?

JvP: Part of the problem is IT management and part is IT governance; it is difficult to tell which proportion of the failure belongs to which. If IT management is the cause, IT governance should take notice and perhaps kill projects in the early stages before more damage is done.

DE: Over last years, IT spending ambitions have been reduced after Y2K, the Euro conversion and the e-bubble. Projects are now expected to deliver return at very short term, and sometimes they lack the ambition and the means to achieve visible business benefits. Programmes are not laid into a longer (five-year) perspective, hence the 'big picture' is lost and individual projects may diverge. Governance and IT value management clearly have a role to play there, by giving accountability and responsibility to the right decision levels in the organisation. This would also reduce the dependency on individuals in the organisation, especially when key decision makers change.

PW: That's clearly a problem with the public sector, but there are parallels in the private sector as well. One can see it particularly when business sponsorship of a project changes; priorities tend to change as well. Also, there is a reluctance to cancel projects and shift resources when they are failing. Once they get started, they just tend to keep on going. Of course, that's a governance issue, too—a lack of oversight over the entire project portfolio. Times and needs change, and sometimes a project that started out with great promise no longer is quite so necessary, but no one takes responsibility to pull the plug.

JvP: I remember seeing a 2004 survey that indicated that one of the most important critical success factors for IT governance was life cycle management—being aware of what your projects are doing, how they are performing, what they are costing and what they are earning. Often that information is just not there.

What positive signs do you see that IT governance is getting better?

JvP: Awareness is increasing, but IT governance is a complex subject. We need to teach executive management.

DE: Regulations are imposing more requirements, forcing companies—not just US companies—to do more things. Boards, stakeholders and customers are seeking more transparency. These are the things that are moving us toward more structured governance. Thanks to compliance requirements, boards and management have been made more aware of governance needs. Now, some think about transforming these compliance projects into efficiency projects, i.e., using governance to make business and IT leaner or more efficient.

JvP: Organisations have to do something about transparency. Sarbanes-Oxley, Basel II, you name it—all these have to do with conformance, with compliance to laws and regulations.

PW: But that's still very heavily focused on 'are we doing things the right way' rather than doing the right things.

JvP: But it's a source of information. People need to study it a bit more, and focus more on performance rather than just conformance. But regulations like Sarbanes-Oxley make it possible to discuss these issues.

LC: The Flemish government is currently undergoing major restructuring and reorganisation. We are really trying to focus on business planning, stipulating exactly what our objectives are, what our deliverables are and what we expect our return to be. In writing up these plans, it becomes very clear how pervasive IT is. The business may not have recognised it before, but virtually every plan calls for or depends on IT. Of course, the big surprise part of that is the money side: 'We are spending too much on IT; we are not spending it on the right things'. In truth, our budget is low. At least the process of writing these plans makes everyone think about costs; it is a tremendous opportunity to push IT governance. We need to teach it—and I would start with the lower-level IT people.

PW: I agree to a certain extent but I wouldn't suggest having a course on IT governance because, to my mind, IT governance is a means to an end, not the end itself. What we're trying to achieve is getting the right value for the money we're spending on IT, improving shareholder return in the private sector and, in the public sector, improving the level of service provided. We shouldn't focus so much on the process—governance—but what you want the governance for. If you say you're offering a course in IT governance, the natural reaction for many people will be 'That's not for me; that's for the IT department'. For example, I was speaking at a conference on IT governance a few weeks ago—a very well attended conference of about 150 people—and I said that I would know people were taking IT governance seriously when at least half of the attendees at such a conference were business people. In this case, probably 145 of the 150 were IT people. Obviously, IT people are important in this process, but, as we've all said, we have to get at the people who are in the business. We have to find better ways to articulate the IT governance message—that we're not improving IT governance for the sake of improving IT governance but because it make sense from a business/profitability/survival/service provision angle.

LC: Perhaps we are calling it the wrong thing. Maybe we shouldn't call it 'IT governance'.

JvP: It's business governance.

PW: Exactly. It's business governance of IT. I think the more we refer to it in that way, the more we can engage the people we want to engage.

ISACA and ITGI offer COBIT, Val IT and other materials for free. Other organisations offer different products. Are there other things the solution providers could be doing to help improve the IT governance process?

JvP: Self-study courses.

LC: One of the problems we have is that boards don't often want to invite an IT person to meetings for fear the IT person will recognise how limited the understanding of IT is on the board. And the board isn't helped in its understanding when people come in and talk to them in IT terms. They need to be addressed in business terms: what IT is doing for the company. So, what would be helpful would be small booklets that explain, in almost storytelling terms and business language, the alignment between business and IT. The books should be aimed at top management and should not talk about IT governance or steering committees or priorities or CMMI or any of those terms. It should just talk about what IT governance can do to benefit the business.

PW: That's a good idea, but it's difficult to find the right level—simple, but not patronising. Also, everyone has different levels of understanding, so where you pitch it is a particular challenge. But, you're right, we have to find the right language, the right format, the right method for actually getting to these people. I'd like to hear more about the game concept mentioned earlier.

JvP: The game is played with key members of the organisation, clustered into groups, and the object is to see what happens in businesses with and without IT governance. It has been effective at creating awareness at lower levels. We use it as part of a management meeting; it can be an effective management tool. It takes only a few hours to complete. It's in the public domain, through the NAF⁶ web site; it's available only in Dutch right now.

What are key messages you would have for people embarking on the IT governance journey?

JvP: It is a complex issue. Within our company, we identified seven critical success factors that must be in place for IT governance to be successful: a proper organisation, good procedures, business cases, portfolio management, standards and best practices (this is where I'd put COBIT), tools to support your IT governance efforts, and life cycle maintenance.

LC: I would try to convince them that this is not hype; it really can help improve your investments. I'd try to demystify IT governance and explain its end goal of improving the business.

PW: Actually, just embarking on the IT governance process will itself generate value to business. It may be an investment up front but it could be the best investment the organisation will ever make because IT is so pervasive throughout the company's activities. Gartner says that 20 percent of the money spent on IT is wasted; the trick, of course, is to know which 20 percent! If you have governance in place, you can cut that 20 percent down. You'll never get it down to zero, because there is risk in everything you do—so not everything will work out. But even if you get the 20 percent down to 10 percent or even 15 percent, the bottom-line savings to the company will be significant. An MIT⁷ study mentioned that there is a 25 percent better return on IT-enabled business investments when IT governance is in place. Even if it were only 5 percent, it would be well worth it. Many businesses put off implementing IT governance because they don't know where to begin and it's easier to continue business as usual. It's a journey. You have to start if you're ever going to get anywhere. For those of you who are consultants, do you find there is a lot of receptivity in your customers, or is it a hard sell? Do your customers ask for 'IT governance'?

⁶ Nederlands Architectuur Forum (Dutch Architecture Forum), a non-profit organisation consisting of universities, IT organisations and end user organizations; www.naf.nl

⁷ Massachusetts Institute of Technology, USA

IT GOVERNANCE ROUNDTABLE: IT GOVERNANCE TRENDS

LC: It depends on what you are calling 'IT governance'. It can range from IT practices to governance/risk/compliance practices. The words can sometimes be misused; sometimes vendors use these terms to get in the door, but that's not what they are actually selling. It also depends on the maturity level of the company. Some larger companies are farther along—they have the seven critical success factors listed earlier—and some smaller companies think IT governance is just for larger enterprises. For everyone, you have to bring them along by steps—set milestones and accomplish certain portions by certain points in time.