

# IT GOVERNANCE ROUNDTABLE:

## IT GOVERNANCE FRAMEWORKS

# IT GOVERNANCE ROUNDTABLE: IT GOVERNANCE FRAMEWORKS

## **IT Governance Institute®**

The IT Governance Institute (ITGI™) ([www.itgi.org](http://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 Frameworks* (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 judgment to the specific control circumstances presented by the particular systems or information technology environment.

## **Disclosure**

© 2008 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 authorization of ITGI. Reproduction of selections of this publication for internal and noncommercial 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](mailto:info@itgi.org)  
Web site: [www.itgi.org](http://www.itgi.org)

## Acknowledgments

### Participants

Paul Williams, Principal, Paul Williams Consulting, and IT Governance Adviser to Protiviti, UK  
The Honorable Robert T. Howard, Assistant Secretary for Information and Technology, US Department of Veterans Affairs, USA  
Pauline Jorgensen, Head of IT Security and Business Control, British Airways, UK  
Halina Tabacek, Senior Director of IT Business Planning and Management, Sun Microsystems, Inc., USA  
A vice president, risk management, for a financial services firm, USA

### ITGI Board of Trustees

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, 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 Peña 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, FHKIoD, 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, CGEIT, IBM, USA  
Lucio Molina Focazzio, CISA, Colombia  
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada  
Michael Schirnbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria  
Robert E. Stroud, CA Inc., USA  
John Thorp, CMC, I.S.P., 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  
Information Systems Security Association

## **Acknowledgments *cont.***

Institut de la Gouvernance des Systèmes d'Information  
Institute of Management Accountants Inc.  
ISACA  
ITGI Japan  
Socitm Performance Management Group  
Solvay Business School  
University of Antwerp Management School  
Aldion Consulting Pte. Ltd.  
Analytix Holdings Pty. Ltd.  
B Wise B.V.  
CA  
Consult2Comply  
Hewlett-Packard  
IBM  
ITpreneurs Nederlands B.V.  
LogLogic Inc.  
Phoenix Business and Systems Process Inc.  
Project Rx Inc.  
Symantec Corporation  
TruArx Inc.  
Wolcott Group LLC  
World Pass IT Solutions

In November 2007, I was fortunate to have the opportunity to meet with four esteemed colleagues to discuss various issues relating to IT governance—generally and in their enterprises and among their customers. I was joined by:

- The Honorable Robert T. Howard, Assistant Secretary for Information and Technology, US Department of Veterans Affairs, USA
- Pauline Jorgensen, Head of IT Security and Business Control, British Airways, UK
- Halina Tabacek, Senior Director of IT Business Planning and Management, Sun Microsystems, Inc., USA
- A vice president, risk management, for a financial services firm, USA, who wishes to remain anonymous

Since I was the moderator for the discussion, I was able to set the 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 exchange ideas because we were attending an ISACA conference on governance and compliance—two apt subjects, given the focus of our conversation. Sensing that having these experts in one place at one time was an opportunity too good to let slip, the IT Governance Institute (ITGI), ISACA's research affiliate, arranged our gathering. ITGI is extremely grateful to ISACA for hosting both the conference and the roundtable discussion on which this document is based. We also appreciate the willingness of our participants to give us time in their busy schedules and to engage freely, openly and candidly on a topic that is of concern to many enterprises around the world.



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

## What does IT governance mean to your organization?

**Halina Tabacek (HT):** We have been working to define IT governance for a number of years. The definition has changed over time. Its origins were in control and measurement but it has moved and progressed into more front-end planning, putting the processes in place. It is more preventive, rather than taking action afterwards. It is the framework to do business, make decisions and monitor progress.

**Robert Howard (RH):** I completely agree; that really is what governance is. It also provides the framework, mechanisms and methodology for involving the people, from those you support to those who provide support, and the boards that meet and deliberate so that people feel they have a say. When someone says ‘governance,’ a lot of people think about how they will fit into the process. Governance is about controlling things, better management of what is going on, and a more responsible look at where we are putting our efforts.

**Vice President (VP):** I tend to think about it from our point of view and that is: alignment with business needs, delivering consistency, sustainability and accountability for all our IT processes.

**Paul Williams (PW):** One of the things within ITGI we have tried to do recently is change the emphasis from IT governance to enterprise governance of IT because we found that, within a lot of organizations, it can often mean the governance of the information technology itself rather than IT’s ability to provide support to and enable the business. That is one of the reasons that our certification is called Certified in the Governance of Enterprise IT™ (CGEIT™), to bring out the enterprise emphasis.

## How did your organization embark on the IT governance journey? What was the catalyst?

**HT:** The catalyst was an inquiry from the board of directors about what methods IT was using for governance. The inquiry contained a reference to *Control Objectives for Information and related Technology* (COBIT®) and no one within the organization at this time was familiar with COBIT. An external board member, who was on the audit committee, was well-versed in the COBIT framework. The CIO embarked on COBIT research to understand what COBIT is and subsequently created a mandate to incorporate its use. It took some time for us to understand what it means to follow COBIT.

**RH:** For us it was the Congressional committee—what they saw going on within the Department of Veterans Affairs (VA), the inability to explain where money was going within the IT arena, and visits to VA hospitals that had a wide variety of ways of operating. A lot of the pressure to reorganize came from Capitol Hill, from the oversight committees, primarily from the House of Representatives side. The House Veterans Affairs Committee has a subcommittee for oversight. Initially, a lot was centered on money and what was going on because of an inability to explain what was going on with the projects and why they never seemed to come to closure. A lot of employees, though, were familiar with COBIT and ITIL.<sup>1</sup>

**Pauline Jorgensen (PJ):** Governance needs to be widened to cover the whole organization, not just IT. There can be a tendency to focus on IT and forget about the governance of the rest because it’s easier to focus on IT.

**PW:** It is good to see the drive being initiated and sponsored at the board level. Ideally, the initiative should not start within IT. It needs to be properly sponsored by the business and be accountable to the business.

---

<sup>1</sup> IT Infrastructure Library

**VP:** The need for governance comes from the way the company is organized. We are a hybrid organization—we are both centralized and decentralized. Our technical platforms are running as almost separate entities, but report up to a central technology group, so there is a need to make sure everyone is speaking the common language, especially to all our technology groups providing centralized oversight. We have a need to deal with all the internal and external audits, as well as our lines of business, and having all the technology groups looking at things differently created significant problems.

### **Did you find the COBIT framework helpful? Were there any issues in adopting COBIT? What are your impressions of COBIT as your framework for governance?**

**PJ:** It is particularly useful that COBIT provides a common language that everyone can understand. The stimulus to use COBIT within our organization came from various places, not just in IT. The current version of COBIT is considerably better than the previous one. It has helped us benchmark and assisted with common understanding, and it has been useful in explaining issues to people who do not work in IT all the time.

**PW:** Have you found that your audit people use it as well?

**PJ:** Yes, external and internal audit.

**PW:** So, again, it provides a common language right across the board.

**VP:** With the newest release of COBIT, there is a higher level of awareness; we are going through, trying to look at it as putting it into the whole central governance model. There is more consistency around everyone speaking the same language. With COBIT® 4.1, there is more significant work that we can more easily adopt. I do like the efforts ITGI has made toward creating a COBIT evangelist. We have had someone who has given us some education on it, but it needs to be a regular, more consistent awareness, from our point of view.

**RH:** It does help explain things to senior officials with a sensible framework; it just seems to make sense. Checklists are enormously helpful. We did not need to put into place or explain the whole methodology, the whole business or controls—just the use of checklists in some of our compliance activities that draw on COBIT to some degree.

**PW:** What specifically kicked off the use of COBIT? Where did the initiative to use it come from? Was it internal or external?

**RH:** External and internal heat. When a decision was made to go forward with the reorganization (this took a year or so), it was because of pressure from Congress, some analysis conducted by Gartner that pointed out the benefits that would come from centralization, and security issues. The decision to reorganize (that is, centralize) was coupled with hiring a company to come in and help—in our case, IBM. IBM brought the knowledge of COBIT, but we had a few who were already knowledgeable and had a good understanding of COBIT's processes and methodologies. Most of the expertise came from IBM; they brought in specialists in this area. We tried to immerse ourselves as much as we could. We use a mixture of ITIL and COBIT.

**PW:** One of the questions I am often asked by people who probably don't quite understand is 'Should I use COBIT or ITIL?' My response is that you should use a combination of these things. Does that apply to you as well?

**Group:** Yes.

**PW:** Have you found that they integrate pretty well?

**RH:** ITIL is the library of best practices and it changes all the time. COBIT is not necessarily that way; it is focused on a list of controls used to tighten things down, as in ‘these are the things you need to worry about.’ They are different.

**PJ:** They do not conflict.

## Do you use the mappings that ITGI provides between COBIT and various other standards and frameworks?

**PJ:** Actually, we mapped to the various standards ourselves, before the mappings were completed.

**PW:** The culture behind COBIT is that it does integrate properly with the other standards and we recognize that it is not the answer to everything. If you use the right combination, you will end up with something workable and usable.

**PJ:** It is relevant for people setting controls, not necessarily to people using them. It is not necessary to describe it as COBIT.

**PW:** Yes, COBIT should be totally transparent.

**PJ:** You need to know what the control is and why it is important.

**RH:** Setting up the processes is very important. We put special teams together to undergo a period of deep study. We now have groups of government people who are very familiar with the processes and we didn’t have that a year ago. They are really good and are helping others to implement some of these processes.

**HT:** Two things haven’t been mentioned yet. One is a checklist—the inventory of processes that should be in place in an organization, against which the organization can then map what it has in place. In the past, very little was documented at our organization, so COBIT helped in terms of getting to a point of documenting processes, which then led to consistency across the organization. Now, everything is documented. The other aspect we found useful was the maturity levels—being able to do an assessment. We’ve done only a peripheral assessment, so we know we are relatively low on the maturity scale, but it is still very helpful having those definitions there to guide where we want to go and being able to do that somewhat judiciously. In some places it’s more important to be higher on the maturity scale than others, so that has been very valuable.

## Are COBIT’s maturity models useful for the rest of you?

**PJ:** We do use the generic COBIT maturity models. We set a target according to what the risk is, work out where we are and work on what we need to do to bridge the gaps. The only thing I would say is that sometimes the definitions make it a bit difficult to differentiate between two levels. Sometimes for one area you find you meet certain elements of multiple levels of maturity, but not others. You have some of this one and some of that one, so where do you put yourself?

**PW:** One of the key things for people to recognize is that they do not need to be on level five on everything. A lot of organizations, when they start off, think that COBIT is too prescriptive and they have to do everything that goes along with it, and you just can’t do that. It is a matter of recognizing the processes, of looking at where you are currently and where you want to be. An organization can be anywhere on the individual scales, depending on its risk and the type of business it is in.

**VP:** The framework has been helpful, from our point of view, because it guides self-assessment. It helps provide consistency when you have to self-assess because it gives you certain criteria.

**PW:** I think ‘COBIT evangelist’ is a great term. I think that every organization could benefit from actually having one. One of the concerns that is raised within large organizations is that it is difficult to find people who have real in-depth knowledge of COBIT. Although there is a fairly low-level certification program for learning COBIT—the COBIT Foundation Course—increasingly there are people who are setting themselves up as COBIT consultants. But true COBIT expertise is still relatively immature in many places, so there can be difficulties in actually getting people who really do understand it. In your organization, for instance, did you use external consultants or was that something that you developed from the inside out?

**PJ:** We had a COBIT evangelist already in place in our security department—one of the IT people.

**PW:** That’s good, because we tend to find that evangelists usually come from the audit side because that’s where COBIT started 15 years ago.

### **When you endeavored to engage the business in IT governance, what were the challenges and how did you overcome them?**

**RH:** People were upset that we were taking their localized IT people away. That’s the struggle we went through. There was great resistance to doing that until finally the Secretary said, ‘Sorry, this is the way we are going to do business’. Internally, we spent a lot of effort on it. The business was not interested; they were interested only in hanging on to as many people as possible. We put teams together to make sure we had the appropriate expertise and also put a group together to arbitrate. Some IT people did stay on the business side, but we mandated some interesting criteria. We reclassified the IT career field. People who remained in that career field have a role in defining business requirements. That helped a lot to identify who got transferred and who didn’t. We don’t define business requirements, we just help flush out IT requirements, and that seems to be working well.

**PJ:** We have not had that problem since we have always had a centralized IT department, so we never had to go through that. Engaging the business has nothing to do with discussing things like COBIT. It has more to do with explaining what the risks are, why they are risks and how we can mitigate them. We try to shield the rest of the organization from more of the technical aspects of what goes on underneath.

**VP:** I agree. We use the governance framework and give them an enterprise view of the risk management facet—where we are as far as everything is rated. The business representatives can take a look at the dashboard to see where we stand right now, but they would not necessarily know it was COBIT.

**HT:** We had quite a few challenges with that, partly because the culture of our company is very entrepreneurial. Any introduction of process is often seen as inhibiting creativity, as well as adding bureaucracy that hinders getting the work done quickly. From the business there was a lot of resistance. We had to take COBIT out of the picture and focus on the processes; Sarbanes-Oxley helped since we were required to put controls in place. There was reluctant acceptance of the fact that we needed to do that, but the preference would be not to. There is a much higher tolerance of risk, but being an engineering company that is faced with having to innovate constantly, what’s foremost is moving quickly, so the process is not always accepted. There was high acceptance in that the CIO reports to the CFO, so from the financial and audit perspectives we had tremendous support. This relationship helped bridge the gap with the other business organizations.

**PW:** So Sarbanes-Oxley was a major incentive to embark on this effort.

**VP:** Sarbanes-Oxley is always a factor. We try to make sure we have a strong program to help identify potential issues before the external and internal auditors do. Sarbanes and other regulations have had a big impact on my firm.

**PW:** One of the concerns I have always had about IT governance and regulations is that regulations encourage a very understandable emphasis on controls and compliance, but do not address the other part of governance—value attainment and building the value of business.

### What have you done to address the value side of IT governance?

**RH:** We spent great effort on tightening controls. Now we must figure out a way to provide better service. That's going to be hard. Staffing problems were discovered and, in some cases, we clearly do not have the people we should have, so we have to figure that out from a contract side. Project management is an issue, a really big problem. We have clearly discovered why the VA has not been able to deliver a product. It has less to do with money and more to do with the expertise to pull off the projects—not to say we don't need money, we need both! We discovered that there were difficulties with people being able to manage programs and bring them to fruition, and you're dependent on that project management ability to be able to present something to the customer that has quality. The Electronic Health Record was developed internally by coordination between physicians and IT people. There was a lot of creativity involved in the project from within, and the leadership of the Health Administration in the VA encouraged innovation and decentralization. In fact, although we are centralized, most of us would prefer to be decentralized. That's fine if you can keep some standards in place, which is where we failed. The idea of delivering a quality product and figuring out how to do that better is a major problem for us a right now. We've tightened our controls with COBIT, now how do we actually do it and enhance delivery?

**PJ:** There is a huge focus on business benefit—measuring the benefit through the life of the project—and quite a strong audit focus on that to justify future investments. The other main focus has been cycle time. How do you get it done quicker? We need to continue to be more and more responsive to deliver benefits more quickly.

**HT:** Particularly because IT generally does not support our engineering community, which is core to the business, there is a view of IT that we tend to be more of the 'plumbing.' Because IT is the plumbing, there is a tendency to ask why expenditures are so high for something that is, for the most part, not very visible. Value is a little bit of justification and awareness, to communicate what is provided within that plumbing and the consequences of not having or maintaining that.

**PW:** I can see that the emphasis is probably more on how do we control or reduce cost, rather than how do we actually prove we are getting definable value from expenditures.

**HT:** More recently, there is a realization that there is value in having information. Things are starting to change and there is recognition that IT systems provide access to information, which then supports the organization within the business functions. We need to make sure that the partnership continues to exist to ensure what we are delivering within IT is addressing the business-side needs.

**PJ:** That's a key point you just brought up: you don't deliver value just from IT.

**PW:** It can be one of the most difficult things for a business to define. I see lots of organizations struggling to define exactly how they get value from IT. But, you don't. It's the business that gets the value. You have to look at it in a more properly integrated way and it can be a big challenge.

**VP:** It is a pretty good challenge. We constantly look at continuous process improvement. We say we deliver exactly 'X' number of dollars from certain activities and there are certain initiatives that we can show that, from replatforming major systems or the innovation of a banking system. There are ways to actually put the savings behind it. Otherwise, we know we are delivering value because we get good feedback from the lines of business. It's also a challenge to really demonstrate that. Right now, we have been doing well to be aligned with the business objectives, but what's the best way to show you are demonstrating the value? It's an ongoing challenge for us.

## Has ITGI's Val IT framework been helpful?

**HT:** There are elements of Val IT that we were already doing, even without the framework, which represents the entire value chain. The framework helps put it in perspective. Another key is a distinction that was made earlier: the fact that it is enterprise governance of IT not IT governance. There is currently a very large initiative to perform a major upgrade to our enterprise resource planning (ERP) system. It is very much a business-driven initiative, which is very fortunate and the right way to do it. All of the savings and return on investment are focused on the entire enterprise. It isn't strictly what we are going to save in IT by doing this because there is a tremendous investment being made in IT, but it's really how the business organization is going to benefit from the deployment of this IT infrastructure. Once the project is completed, it is going to be such a big component of our IT infrastructure that I think it is the tide turning for the foundation for us to look at it enterprise-wide.

**PW:** I think the key thing with Val IT is to start off with its ten principles, including measuring benefits across the life cycle, taking the full scope of activities including the business change cost, and so on. I think that is the logical place to start. Val IT is relatively new; it has been available only for about a year. It is very much aimed at covering the more subtle angle within governance, which is the value rather than just compliance and control, although they are all interlinked.

## How do you actually measure success?

**RH:** Feedback from business partners is key. We get a lot from IT and compliance people. There are also other measures, for example, decreases in security incidents and in stolen equipment. Another measure we are currently working on is establishing better collection mechanisms to include dashboards to view incidents and outages because those are typical indicators of how things are going.

**VP:** By having a regular feedback process. Our senior executive team meets every two weeks to take a look at the risk management point of view. We are now at the point that we get regular feedback. In addition to historical trends and things that we have been tracking and looking at, we also get into discussions of new issues that are developing and can say we should add these to things we should be tracking. We can show now, on a monthly basis, how we have been improving and what new things are developing, and get things on the radar at the appropriate level and go from there.

## Do you use dashboards and the balanced scorecard? How are they working out?

**HT:** We are just in the process of developing a balance scorecard for IT, so it is not something that has been widely rolled out yet. A small team of the CIO staff has been doing the hard work of pulling it together and then, periodically, we are keeping the rest of the senior IT leadership informed on progress. This way we don't have to involve 12 people spending their time in the meetings to develop the scorecard. It is certainly important to have their perspectives, so we are making sure to get their feedback. We hope to then use the balanced scorecard as a key measure. We also have a set of operational metrics—a dashboard—where we measure the service delivery aspects as opposed to the strategic initiatives. We've got the support.

**PJ:** Our measures are very public within the organization. They are on our intranet and there are regular reviews of the both the measures of operational performance and compliance, as well as the measure of change. You've got to target in terms of what you want to do differently and what you are doing to move toward that target. We make those targets and performance public within the organization as well.

**VP:** We currently use a mix of both a dashboard and the balanced scorecard. We usually have a couple of different risk committee meetings—meetings with senior executives every month and risk committees every two weeks. Senior management reviews the balanced scorecard regularly so that each individual group knows where it stands on the key performance indicators we define, not only as we go, but usually as we define our goals for the year. We map them to the scorecard so we know how we are doing relative to our goals.

### **What hints and tips can you provide to organizations beginning on the IT governance journey?**

**PJ:** Make sure you base it on risk. Do not try to be perfect at everything. Also, do not look just at your own risk, but at everyone else's as well.

**HT:** Leverage external organizations, whether it's something like ITGI or research firms like Gartner or Forrester. They can do benchmarking for you and bring those best practices in to give you a running start.

**RH:** In hindsight, based on what we went through, we should have gotten a very thorough assessment of existing conditions throughout the VA. You had better know what you are going to inherit. We didn't do that to the degree we should have. Now we are discovering what we have inherited and there are a lot of problems that have to be cleaned up.

**VP:** Having the right management support has been important. You have to know that the process can work and is going to help, but do not expect overnight results. You have to look further down the road and recognize this is going to be a challenge. It's really having the right support and the right mindset to get the undertaking going.

**PJ:** Build the change into the life cycle, but do not do it in isolation. Make sure you don't make things worse while you are busy fixing things to make them better!