



IT GOVERNANCE
ROUNDTABLE:
VALUE DELIVERY

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

IT Governance Institute®

The IT Governance Institute (ITGI™) (www.itgi.org) is a nonprofit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the nonprofit membership association ISACA in 1998 to help executives and IT professionals ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly allocated, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfill their IT governance responsibilities and help IT professionals deliver value-adding services.

Disclaimer

ITGI has designed and created this publication, titled *IT Governance Roundtable: Value Delivery* (the ‘Work’), primarily as an educational resource for executives and IT professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any 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, executives and IT professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology (IT) environment.

Reservation of Rights

© 2009 ITGI. 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 and use of all portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, 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

Acknowledgments

Participants

Brian Barnier, IT Governance and Risk, IBM, USA
Jennifer Alfafara, CISA, Consultant, Resources Global Professionals, USA
Urs Fischer, CISA, CIA, CPA (Swiss), Vice President and Head of IT Governance and Risk Management, Swiss Life, Switzerland
Steve Schlarman, CISM, CISSP, IT GRC Product Manager, Archer Technologies, USA
Paul Williams, CITP, FCA, MBCS, IT Governance Advisor, Protiviti UK, UK

ITGI Board of Trustees

Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, 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 (retired), 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

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 EURL, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
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 Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium

ITGI Affiliates and Sponsors

American Institute of 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
Institut de la Gouvernance des Systemes d'Information
Institute of Management Accountants Inc.
ISACA
ISACA chapters
ITGI Japan
Norwich University
Socitm Performance Management Group

Acknowledgments *cont.*

Solvay Brussels School of Economics and Management
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
B Wise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

In October 2008, I had the unique opportunity to participate in a roundtable discussion with the following esteemed colleagues:

- Jennifer Alfafara, CISA, Consultant, Resources Global Professionals, USA
- Urs Fischer, CISA, CIA, CPA (Swiss), Vice President and Head of IT Governance and Risk Management, Swiss Life, Switzerland
- Steve Schlarman, CISM, CISSP, IT GRC Product Manager, Archer Technologies, USA
- Paul Williams, CITP, FCA, MBCS, IT Governance Advisor, Protiviti UK, UK

As moderator for the discussion, I chose to focus on one of the key issues around IT governance: ensuring that IT investments provide the value they should. To use the IT Governance Institute's view of the world, we concentrated on the value delivery focus area of IT governance.

We had this too-rare opportunity because we were attending an ISACA conference for IT governance, risk and compliance professionals on the topic of measuring value, managing risk and assuring compliance. With so many experts in one place at one time, inviting them to sit around the table to discuss governance was a sure win.

We are grateful to ISACA for hosting the conference at which this roundtable took place. And I thank the participants for taking time out of their busy schedules to share their thoughts in such an open and candid manner.

Brian Barnier
IT Governance and Risk, IBM, USA

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

Brian Barnier (BB): We're going to discuss delivery of value. While there are a variety of perspectives on that topic, it might be helpful to tie those perspectives together by asking for your experience. Think of a time when you performed a diagnosis and the result was that value had **not** been delivered well. What were the steps you took to enhance value delivery?

Paul Williams (PW): In my experience, most organizations do not know whether they are getting value. But, what is value? Value means different things to different organizations. If you're a for-profit organization, value usually is measured as shareholder return. You're looking at generating good returns for investors in your enterprise. You're looking for good economic return, which is all about profit on a sustainable basis, and you're looking at increasing the value of your investment over time through dividends and increases in the stock price. We can look at how IT might contribute or detract from that. It's different, of course, in the government, public and not-for-profit sectors where it's not shareholder return that is the bottom line. It's really all about providing the best services to your constituents, whether they be tax payers or recipients of a charity, and the emphasis will be on delivering the best services at the lowest possible cost.

First of all, you have to define what value means to your organization. There's no one-size-fits-all definition. In my experience, very few organizations really measure or even attempt to measure the value of what they get from what they're spending on IT. It's a bit of a black hole. They spend money and keep their fingers crossed that something useful is going to come out of it at the end of the day. Determining whether you're getting value from any kind of expenditure is not easy, which is why most organizations don't even try to do it. To me, it all starts off with a robust business case—making sure, up front, that you're very clear as to what it is you're trying to do, why you're trying to do it, what it will cost and what the return will be over whatever period of time you set. Unless you know what value you expect to get from an investment, it's very difficult to determine later whether you achieved that objective. Business cases typically are not very well put together. They often start off with the thought that they have to prove that they're going to get a particular value in order to get this particular project approved. It isn't sensible to start with the answer and work back toward the question.

One of the things that most organizations are very immature at is measuring value—measuring the benefits that they actually get from any particular investment. The emphasis too often is on delivering a technical solution that works. Everyone then breathes a sigh of relief and moves on to the next project. But, in terms of any kind of metrics to determine the value that actually came from that venture, it's always very imprecise and most organizations don't even try to do it. Value is something that organizations have only recently started to consider.

Steven Schlarman (SS): I think that you can look at the definition of value and find that it is as nebulous in organizations as is the definition of risk. Just as you understand the risks that you're looking to manage, mitigate or accept or transfer, you have to define that same type of understanding from a value perspective.

It just occurred to me that you could have key value indicators just as you could have key risk indicators (KRIs). You could define the value that you're looking for, and then look at how you are going to achieve that value. An IT organization may almost be similar to a not-for-profit or government organization because a lot of the value in an IT organization is in how well they are providing the services to the business that are then driving the benefits from a shareholder perspective (e.g., revenue). When you're sitting in the IT organization, you have a direct value that you want to look for and you determine how to create shareholder value, which may be through reduction of costs or better management of the IT infrastructure in general. But then you also have the qualitative values: How well are we satisfying the business requirements? Does the business feel comfortable coming to us with a business problem or a business issue? Does the business have confidence in the IT department to analyze the problem, appropriately build a solution and deliver it on time and on budget so that the business can then bring the value to the shareholder?

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

BB: Let's take this down a level. Urs was talking prior to this roundtable about key risk indicators (KRIs) and key performance indicators (KPIs) and getting to that level of establishing value. And Jennifer made a comment prior to this roundtable about her new boss who had come in and said, "I don't know what you do."

Jennifer Alfafara (JA): I think that's typical. In California, we have a movie industry and some large companies, but the majority of the enterprises are smaller public companies and they have compliance issues. When they take on projects, they take them on in a different way—they view their IT in a different way than do the large corporations. Their IT departments often don't even have source code, but, nonetheless, they are charged with delivering something. What I've seen in these smaller companies is that they talk about delivering value and staying on course with their corporate needs and they say, "OK, what do we need to do this? Let's go out and buy software." They get together a selection committee and choose the software. They get it loaded onto the machine, but they can never get it implemented because they don't understand that there will be pain during that period of time and that's part of the whole process.

There's pain up front; you have to change your business processes to do these sorts of things. You have to measure results—this is where the metrics part of it comes in. You don't wait until you're at the end of the project to determine whether you're successful. You have to establish benchmarks and take measurements at those points and ask where you need to change course. I read a statistic that indicated that there are probably almost as many companies that fail at these types of things and lose faith in their IT departments, thinking they failed because of the IT department. There's just a gap between what leadership expects the IT department to deliver and what they can actually deliver and what they want to deliver.

Urs Fischer (UF): I want to come back to what Paul said. He was talking about the business case. He said you do the business case and then it's done. If you can provide a positive business case, you can do the project. I think that's the main problem. In the business case you have a break-even point, perhaps in two or three years. But no one will control it or know if you have ever reached this break-even point. So it gets back, again, not even to measurements but to control. For example, the commitment is one thing—with a business case, in my opinion, you commit yourself—but controlling whether you reached your commitment has to be done by another person. For example, you can use financial controlling to verify that the break-even point of the business case has been reached with the project. I don't care who does it. But you have to do it to get a new culture in your organization so that business cases are not just some illusionary thing.

PW: You're absolutely right, Urs, and that is one of the great failings with business cases. I believe you do need a comprehensive, robust business case to kick things off. But if that's where it stops, then you're not going to achieve much. Somebody, somewhere has to be accountable for delivering value. I think the "A" word—accountability—is one of the most important words in the vocabulary these days. In my view, it needs to be a business executive at board level. It has to be a business person who has to be accountable for the delivery of value because it's the business that delivers value. It's not IT in itself that delivers value. But I would also question what you're saying about the break-even point. Yes, break-even point is very important but it is only going back to where you started. You've spent the money and now you have that money back. But that's nothing in terms of delivering value. If you're only working toward the break-even point, you may as well not have bothered in the first place. So you have to go beyond that point and be able to prove that you are delivering enhanced value over time. And that's not easy to do, but somebody has to be accountable for that and you actually have to learn the lessons of where it works and where it doesn't work.

UF: You are correct. That is what I meant when I said break-even. At least somebody has to control when you reached this point where you start to earn money.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

BB: One of the things you all have is experience. For example, Urs, you talked about your KRIs and KPIs, and Jennifer, you talked about your new boss. What are the specific things that the two of you can share, just from those comments? Jennifer, what did you do then, so anyone reading this publication can see how they can do a better job with that elusive “alignment” thing? What do I put in the business case? What grabs their attention? And, Urs, you might want to comment on the things you’ve put in cases to get budget, money and activities at your firm, at least to give guidance to other people—things that they should be doing if they want to put up solid, defensible cases.

JA: In a previous life, I was an IT director at a small manufacturing firm in Orange County, California. The company had been sold and we had a new president. I was to report directly to the president. The day he arrived, he walked into my office, stuck out his hand and said, “Hi, I’m Clay. Who are you?” I said, “I’m Jennifer and I’m your IT director.” He said, “I don’t know anything about IT.” I was starting to think about the end of my career! Then, he said to me, “But what I do know is that if everyone is happy, then everything is going OK. So if you have a problem you think might make someone unhappy, please make sure I know about it first.” And that was an easy enough thing to do. When I went back to my office to think about it, I thought about what I can do to make sure that I get all the things I’d like and then also make sure that everybody else stays happy. A lot of it was purely that communication and looking at it as an opportunity to go further from where I was.

Before that, we were a company that had huge margins. I didn’t have a budget. If wanted to buy something, I would buy it. And they didn’t know why I was buying it. They trusted me. That’s not the case any longer because there is accountability for all the toys you buy and all the software you implement. The key was that I needed to understand the current and future direction of the company. This is the thing that bridges the gap. I needed to sit in on the meetings and understand that my plans went along with your plans. And that wasn’t happening. What I realized, and it’s true of a lot of the companies I see, is that IT is purely in a support mode. It is in reactive mode and driven by their help desks. It has no direction.

And this is true of the smaller company where there is no strategic plan. They just get a budget every year that they live with from one year to the next. If companies are going to make money in gaining efficiencies, I think IT and the business need to get a little more “married” and work through this new concept we’re calling “governance” (which actually is not a new concept). I think it’s being realized more now because there is governance software, and thus governance plans. Out in California, it’s almost unheard of. But they’re familiar with the term. I think that’s true of these smaller companies. Wherever I go, where they’re thinking about implementing something like Sarbanes-Oxley, and you talk to them about those areas of management and planning and how their IT relates to the greater world, they consider IT just a support group—they look at IT like the telephone company. “IT has nothing to do with how well we do.” But, it does, and they don’t realize it. So that’s where our challenge is. Maybe we’re primitive and behind the times. I think that smaller enterprises tend to follow what the large organizations are doing. If somebody can prove success through an approach, and they have the tools, then they take advantage of that situation.

BB: Urs, you talked several times about KPIs. What are some specific things you can guide people in doing? What looks like a good indicator to you—or a good measure, if you want to make it broader?

UF: That’s the main problem—I’m still looking for it! You have to develop KPIs for your own company. We haven’t done it yet because we are looking around at what others are doing. If you look at big companies, big insurance companies, they do not yet have a mature system of KRIs or KPIs. One of my peers said, “Oh, I just react when something happens, that’s my KPI.” Fact is, at the moment, there isn’t a lot around.

But you asked me what you can do concerning value. I go back to this thing with the business cases. In our case, projects were started with a business case. Then you had to scope changes because there were a lot of additional wishes. The business case always stayed the same. If you would have looked at it and amended it, you would have realized that

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

you no longer had a positive business case. If we now have a scope change, we also need to change the business case. In addition, financial controlling does past project reviews to verify the business case has been fulfilled. And, as Paul said, we need to have accountability. It's the business, rather than IT, because the business has the requirements and the requirements provide the business case in the end. That's what we did and we improved the success of projects.

BB: You talked about something that was important in the business cases. You talked about calculating a net present value and a payback, and looking at the risk involved, the return and the project management risk, but there's also the requirement risk and the delivery risk. How would you counsel people to look at both the risk and the return elements in their business cases in order to have more effective cases? How would you involve the risk piece more in the business case?

UF: In the business case, you look at the current risk rather than at the value of delivery (although value of delivery also is a risk—whether you deliver or not). For each of our projects, the project manager would write down his or her risks, such as project management risks involving scope and being on time and on budget. So we ended up with the same descriptions for most of the projects as, for example, lack of resources. But lack of resources is a management issue; that's not a risk. If you don't manage your project efficiently and effectively, then you have a problem with resources. So it's not a risk, it's a management responsibility.

JA: Unless the conditions change, such as an acquisition.

UF: OK, yes. But at the beginning, each project has the same thing—a fight for resources. So it's a prioritization issue and not a risk issue. We recognized that the projects described some similar risks, so we thought about having a risk matrix that the project owners need to fill out so that the projects that involved risks could be compared to each other. We had some projects that suddenly showed up as red (using a traffic light ranking)—up to then they were always green—and we had to stop those projects. We had others that were red just because the project manager wanted to cover his or her behind so that if something went wrong, he could say, "I always said there was a problem." So we came back to having a matrix that the project manager has to fill out by answering structured questions—call it a structured interview approach for risk. This matrix has to be updated every month and, in the monthly project reporting, they have to report on changes to these risks.

PW: You have to bear in mind, what is the project manager's responsibility? The project manager's responsibility is, to the best of his or her ability, to ensure that the technical solution is delivered on time and on budget. It usually has nothing explicitly to do with value. The project manager generally doesn't even consider the "V" word—value doesn't come into it. That's where you need the business accountability that we have all mentioned.

I have two specific recommendations that I always make. Accountability is always number one. If there is a significant business change program or project, there has to be absolute, unambiguous accountability from a business board member for the delivery of value for that particular initiative. The project manager and others help to move toward it, but it's the business leader who has to have that accountability. The other recommendation that I regularly make is that we have to forget this idea of project management offices (PMOs). A lot of big organizations have PMOs, which are providing all of the project management expertise, but in my view, the emphasis of the PMO needs to change to being a value management office—a VMO. So it's not just looking at delivery of a technical solution that "kind of works," but it's actually, over time, making sure that it also delivers on value. Unless you have the processes to ensure over time that value is being delivered from the money that you're spending, the whole business case becomes useless. You know you can put whatever you like in a business case because you're never going to be accountable and no one's going to know whether you delivered value from it. But once you start getting into the routine of having proper benefits management processes in place, then you complete that loop. You learn from it and people know that they will be held accountable. But it's not there in most organizations right now.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

BB: Let's have one final word on that topic and then we'll switch to another topic. You mentioned the "V" word for value and the "A" word for accountability. The point I made earlier is that, without the accountability, there's no way it will get done. "Without the A, there's no way" is a catchphrase we've used recently. That accountability is real, meaningful accountability, not somebody who has an A in the matrix but doesn't have it associated with their personal metrics and their measures.

Now, the next topic in consolidating the earlier comments is centered around trying to put together the topics of crossing silos and convergence. Steve, you made several comments on convergence and performance. Let's touch on specific actions to address convergence in compliance and performance metrics, convergence in one-touch and single-touch systems to reduce controls that Steve mentioned and convergence in crossing the different silos, whether they are risk silos or other organizational silos that governance has been designed to bring together.

SS: As I said earlier, I hear the term "convergence" a lot. It's typically from organizations that have multiple activities going on, where they are measuring controls or perhaps also measuring performance. But, they're doing it for different purposes. You have a SOX team that is focused on financial controls. You have a PCI team that's looking at the credit card processing. Possibly, you have some business partners who are coming in and looking for some kind of attestation around controls of management of systems or whatever the organization is providing those business partners. And certain common control owners who are being asked the same questions by different groups at different times and it's just eating away at their time and their patience. So it's a concept of converging these measurements into something that hits all the points. We can do it once, but then turn the lens, if you will, to the different topics.

Let me look at my control environment as it pertains to Sarbanes-Oxley and the financial systems. And let me look at those same results in the context of the credit card processing systems. I've asked control owners out at the business just one time and I'm able to make those connections. Part of that convergence is the establishment of a control framework that is a superset of the requirements that pull together the different control activities the organization should be putting in place. Then there's this connection out to the requirements, whether it's a regulatory requirement, a business requirement or a service level agreement between the business and IT. It's having those reference points looking at internal practices, such as when you're measuring controls and following that linkage back to put the results of any kind of controls assessment or monitoring or reporting in the context of those different lenses.

There are a couple topics that pop out of that concept of convergence. We're looking to break through some of the silos. That means that some of those entities that are focused on SOX and PCI may have to start changing their processes so that everyone is converging on what may be an assessment methodology or a risk assessment methodology. They're looking for commonalities among those different activities so you have some personal interest in those groups. They have to be open to breaking down some barriers and converging on some things. I may not be able to do everything I used to do when I owned this one little silo. Now I have to play nice with the other children in the sandbox.

It also goes back to a broader governance issue and being able to articulate requirements in a reference architecture or something you can use to itemize different requirements and to map those internal practices that need to be put together and centralized in policies and standards—a centralized framework that has the policies, standards, control activities the organization should be following and putting in an infrastructure that meets multiple requirements. The enterprise should be creating a set of best practices and principles and then communicating those principles out to the organization.

JA: And they can adopt it and it's a common ground, so everyone is communicating at the same level with certain expectations that have been preset.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

SS: Especially when you get to compliance—you always ask the question, “Compliance against what?” You have to state a goal and indicate whether you’re going to measure the outcome. What I’ve seen in some organizations is that they will rush toward an assessment methodology. Perhaps they even begin assessing business units or systems, etc. But they have yet to raise the bar on setting requirements to meet the level of activity that they’re doing from an assessment perspective. You have to push those activities at the same time. That goes along with breaking down the barriers, the silos. People have to adopt common methodologies.

JA: Yes, and they should probably tweak their own processes in order to adopt the methodology that’s been established for the organization as a whole. There isn’t a guideline that’s being established by this entity that doesn’t need to be preset. To get people involved, tweak the guideline to fit and then adopt the guideline.

SS: I’ll provide a practical, focused example. I worked with an extremely large, multinational organization—it was in about 160 countries. One of the struggles in the IT department was that they had no common configuration baselines for technologies. If they were building a server in one country, it was totally different from the server in another country. They knew they had the expertise within the company to come up with configuration baselines for technologies, so they invested in establishing a common framework around configuration management. They built groups, identified the gurus in the company, established committees, went through the pain of all the arguments of what it means to be a secure Unix platform. That took a considerable amount of investment. They broke down a lot of silos among the different countries, the different operating units. What they ended up with was a committee of individuals who were from different locations and business units who had come together to converge on creating a baseline for these technologies. There was an investment made to get to that point, but then the value kicked in because they had the best of their people defining the configuration baselines. So the value is not only the reduction of costs of the individual countries and operating units trying to research security controls around these technologies. They reduced cost that way, but then they started getting consistency. They rolled it into an audit methodology. Now they were not only implementing these configuration baselines, but they were also auditing against them. That’s a very small subset when you’re talking about trying to break down silos. At the end of the day, they had an extremely comprehensive and broad view of what it took to secure a technology. This was security-focused with multiple people involved in the process. They had a lot more consistency. Maintenance was a lot easier. When they lost one of their key people, they didn’t lose all that knowledge. The key Unix guy in Brazil may have moved on, but there was a whole committee behind him that helped to make sure that the knowledge didn’t walk out the door with him.

BB: We’ve talked about two kinds of convergence: one is reducing the number of control touches and the other is crossing the silos. There are a couple of other flavors when people use the word “convergence” in conferences and articles, etc. Paul referred to one of them earlier when he was talking about how one looks at assurance. He looks at assurance from both the value and the compliance perspective. Urs made reference earlier to the way his organization is tying in both the traditional compliance-type metrics and the rating agency metrics. One of you may wish to illustrate how you have a single picture or, dare I use the word, “scorecard,” that allows a view of what that business is like. Please comment on tips or suggestions you have to help get to that converged picture of measurement.

PW: To get to where they actually have a dashboard or a scorecard (or whatever provides the information that they need to provide the assurance that they’re looking for) is an outcome from the input of many different people, at different levels within an organization, each of whom may require a different level of detail. I don’t know your particular product, but I’m sure that the end result is dashboards and lots of fancy things, which are terrific, but they need to be tailored to the needs of the user. Some of them are going to be at a very detailed, granular level, and others are going to be supplemented with drill-down capabilities if you want them. But you’re not going to get a CEO to plow through pages and pages of dashboard information. What the CEO wants is a high-level view of the reds, greens and ambers. The CEO wants to answer the question, “What do we need to worry about now and what don’t we need to worry about?” Part of the art of this whole convergence process is making sure that you are pulling together the right information in a timely and reliable form, focused for the user.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

One thing I'd also say is that none of this, in my view, is going to work if it's looked at purely with a tick-in-the-box mentality. It's not just that I have to do this because someone up there tells me I have to do it. It has to make good business sense as well. You have to move from a mentality of "I have to do these things" to "I want to do them" because it will give me better results for my organization and it makes good business sense. Making that transition is quite difficult. I still see far too much of that tick-in-the-box mentality—we're going to do this because, although it's a burden, someone told us we have to do it, so let's buckle down and do it.

JA: A lot of that, I think, is a result of not being able to participate in the original decision. Someone says, "We have this great new initiative. Here's this piece of paper that lists what's expected of you." The person who's involved—and I think it has to be from the bottom up in this case—needs to be involved in contributing to that plan. It needs to be "our" plan rather than "their" plan. You see that a lot more in larger companies as opposed to smaller companies, which is ironic. In the smaller company, the person hears it out in the hallway. With large organizations, you have IT departments with their own building, their own part of the campus, their own country, and they come over from Building One and hand you this piece of paper and say, "Go for it." I think that is how they say, "They're telling me to do this."

SS: Unfortunately, not all of the business value is easy to articulate. I worked on a SOX project for a billion-dollar company with about 300 people in the IT department. We were going through the general SOX activities, using COBIT as our approach (change control is one of the key things in COBIT), and we made the case for change control because, in this 300-person IT department, change control was someone yelling over the cubicle to the next guy, "Hey, I'm going to do this, just so you know." And the other guy would say, "OK." We were trying to propose that you need to have a more rigorous control process. Lucky for us, they not only had a distribution center shut down for two days because of an unauthorized change, but nobody knew when it was going in. One programmer shut down the distribution center for two days; another programmer made a change that threw off the inventory values because he received a request from an end user. So we had some things to say: "This was not just a tick-in-the-box. You guys have shut down a distribution center. You threw off monthly inventory. These are dollars you're throwing out the window." In those cases, you feel lucky because you can turn that tick-in-the-box into specific risks.

In other cases, it's a lot more subtle. I talked about the big company with the configuration baseline. That was a much subtler sell because we had to articulate the following: "Did you know that administrators in all of these countries are trying to track down vulnerabilities and monitor these technologies? And they don't always have the right information. There is a lot of time and money being used in a nonproductive manner when you can instead centralize that approach."

JA: That's in ideal situations, but I've seen companies where it's their intention to let entities run autonomously. When you have that autonomy and then Sarbanes-Oxley hits, you have a nightmare. I think there's been enough water under the bridge now that they're a little more receptive to the suggestion of adopting a common approach to doing things. But, up until that was needed, I think a lot of these companies were saying, "Oh, yeah, we're just a line in the financial report and we do what we want and throw money over the wall."

UF: Regarding the tick-box approach, as I experienced, we had some projects coming from the business based on regulatory legislation and IT had to participate in these projects. The projects normally were managed by external consultants. They told us what we had to do. But we decided that we wanted to do more because we felt, in the end, that we wanted to have something more come out of it than just a checklist. We said, "No, we do more. We want to have controlled processes." It's a management objective to have controlled processes through internal controls. My management objective is not only to fulfill that in the end. The external auditor says, "Yes, financial reporting is OK." That's one issue. That's for the CFO. But for me, as an IT manager, I have additional objectives. So I agree with Paul. We should go away from this tick-in-the-box mentality because then we just have on blinders.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

BB: Let's wrap up this section with two observations. One is a practical example. I was called into a financial institution and the question that was posed to me was, "We have a business continuity plan and a disaster recovery plan. The business continuity plan shows all green. The disaster recovery plan is green, yellow and red. How can this be, if the business continuity plan has as one of its dependencies the disaster recovery plan?" It turns out the answer was that the business continuity plan was based on a regulatory compliance checklist. The disaster recovery people, bless their hearts, were actually trying to make the systems run. So they were returning yellows and reds because they had problems of an operational nature. In our discussion here, one of the catchphrases we used was, "real threats to real operations," not just compliance. That gets lost in a lot of nonindustrial companies. But when you're in an industrial firm or a healthcare firm, you have to look at operations because you're delivering real services and real things as outputs. Those outputs are more natural and tangible than transactions that go across computers.

BB: That takes us to our last topic. We've started to blend in with Paul's comments around, "How can we use governance and risk as part of process improvement?"—i.e., business process improvement within the organization. There are a lot of people out there who are afraid of governance because it sounds like another "feed the monster" overhead exercise, another set of committee meetings that are going to waste resources—more busywork for people to do, more reasons for people to take away my resources and inspect what I'm doing. But there is also an entire body of literature that is decades old—I'm thinking primarily of the quality-focused literature that says quality is free, as in the Phillip Crosby book that says if you're doing a good job with managing these processes, if you reduce rework and waste of time and energy, you should be able to recover the cost you're putting into good assurance.

Let's conclude by touching on some of the topics. Steve mentioned that governance pulls the different kingdoms together. Urs talked about process improvement issues associated with risk and risk governance. Jennifer talked about acquisition integration. Along the way, we can touch on end-to-end views of business activity. Jennifer's examples would be nice because they are smaller-company views that are more tangible. Urs has talked about other forms of issues and dependencies that can be commented on: How does this actually add value, so someone reading this discussion doesn't say, "Oh, boy, I'm going to walk in and ask for a bunch of money to do process work." How can I show that this is something that will make us more efficient and improve our business process?

I'll start this off with one story of a risk manager who was very good at managing risk but found out that, to do it effectively, he had to understand the processes that were going on in the business. With a lot of the processes it wasn't possible to manage risk if you didn't know that the risk existed. So he did a lot of business process reengineering. By the time he was done (in about a year), he ended up being named head of process reengineering as well as risk management.

PW: When it comes to processes, you don't start with the IT processes. You start with asking: What are the business drivers? What are the things that make this organization successful? You have to start at what drives the revenue, the profitability. Then you have to drill down from there to the business processes that make that happen, then the IT processes beneath that level that enable the business processes. So you don't start off looking at program change control; you start looking at your processes for getting new customers or retaining existing customers, fulfilling your sales, etc. Then you really work backward from there. It has to be, in my view, totally business-led. If you start digging into the detail of business IT processes, you might need to get into that detail. But if you start at the business end, you'll know why you're getting into the details!

JA: I think the caution is that you don't intentionally silo because, when you look at different business processes, they may be overlapping.

PW: You're absolutely right. You have to be very careful with that. But I still think that you have to start off by asking, "What are the business drivers?"

JA: It's always nice when the horse comes before the cart.

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

UF: That is the case. You have to look at your business-critical processes. Then you say to IT, “Which IT processes support the business critical processes?” That’s another way of managing risk.

I had quite a dispute again this year with our auditors. They wanted to see a risk inventory. I told them that I don’t have a risk inventory. I do risk management in a qualitative way, not in a quantitative way. For me, a risk inventory involves having quantitative information like probability and impact—and I don’t have anything like that. I always have a business-critical process. I have the IT processes that support the business-critical processes. And I raise the maturity (efficiency and effectiveness) of these processes. That’s my risk management because, when I have the critical processes in IT under control, I automatically reduce my risks. I had quite a dispute with our auditors because they wanted to see figures and I told them I cannot provide figures because I don’t have the statistical basis to generate the figures. To start to do risk management, it would be my advice to do it in this way—first, look at your processes. I agree with my auditors; in the end, you need a risk inventory—you cannot be without it. But why not base this inventory on the maturity of your processes? That may be a practical, pragmatic way for some companies just to start.

BB: The people who are doing a risk inventory and trying to do calculations on parts of a process are doing themselves a huge disservice because they don’t know what the end-to-end process looks like. We’re now getting regulators who are starting to realize that although a firm can state that a recovery point objective on a mid-range server is X hours, that tells the regulator nothing about recovering the end-to-end process. We should make sure our readers are clear that such piece-part evaluations of risk say nothing about the end-to-end process and don’t help locate weak links. Steve mentioned the tools and automation benefits to help make that visible.

SS: I have an anecdote that I think goes to Paul’s point about understanding the business. I worked on a project with a multinational company with lots of different business units, different sizes. The project was establishing an information security framework for the multinational organization and then expectations of control activities for the different business units. Part of the engagement involved conducting site visits. We went to some of the smaller business units. One of the business units that I visited was manufacturing.

One side of the building contained the raw materials as they came in—in this case, potatoes. The other side of the building held the end product, potato chips, as they went out in trucks. The business unit created the entire product in a single building. After we conducted the site visits and interviewed the CIOs about risks and so forth, we went back to those individuals who didn’t go on those site visits and we started working on which control activities were expected at those business units. A lot of times I’d say, “Look, guys, they have one building, potatoes coming in one side, potato chips going out the other side. An intrusion detection system is not one of the major risks that we need to be talking about because they don’t even think about risks from that perspective.” So I think it’s important to be grounded in what the business does, what the business needs and understand that you build the control activities around the end-to-end business process so you build the right control points rather than coming in with a list of controls.

JA: No two businesses are alike. Unfortunately, public accountants don’t look at it that way. This is what I’m experiencing. I had the same public accountant, two different clients, and they had the same audit approach. But one client doesn’t operate the same way as the other.

BB: Jennifer, would you please extend that further by commenting on acquisition issues related to performance improvements?

JA: With acquisition issues, I’m finding that we need to ask, “Do they even have time to look at performance improvement?” Before 1992, I worked for a company that started out as a lone entity that went public and then, all of a sudden, it went into this wild acquisition mode. They started buying companies all over the world. I was trying to bring these guys into the fold where I had no communication up to the new CEO and he didn’t understand the importance of having everyone in the same area. I consulted with other companies that had similar issues to see how they dealt with

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

this issue. The first thing they were most concerned about was the need to get everyone into the consolidation. The basic business processes become secondary. I'm fascinated with how they handled this from a Sarbanes point of view because, in dealing with J-SOX, one of the parent companies had over 200 entities worldwide and I was working at just one of those entities. In considering the demand on that small company to do things the same way as the sister organization that is 15 times bigger, you have to question whether that is appropriate. Is it going to cost these guys the same as what it costs those guys to meet that level of compliance? It's unfair; it hurts the smaller company.

I'm seeing things on a global basis. In the United States, if it's all US, it's a whole different thing. To me, it has been confusing; however, I think it's getting better. I'm seeing how planning an organization at the entity-level controls is becoming important now, whereas that part of COBIT wasn't really important before—it was a minor thing.

BB: All these issues we talk about regarding value, efficiency and performance, and what you get from risk management can go up in smoke when you're doing an integration. Urs talked about project management and evaluating projects. An acquisition and integration is the ultimate project. Next to a major business expansion, it's about as big as you can get.

JA: And it depends on how big the swallow is going to be. If I'm going to pick up on this little entity and all they're making is potato chips, it's not as complicated as if they have an order-driven manufacturing company where their accounting is extremely complex. I've seen the small companies try to swallow something like that.

BB: Plus, you have the factors of whether there is a new jurisdiction with rules you have to swallow. Are there new industry rules you have to address? Are there new supply chain conventions you have to follow? Then you get to the whole issue of heterogeneity of the IT infrastructure. If everyone is on IBM or Windows, then it's very smooth. You have skills issues and experience that you can bring together. But if it's a whole mishmash—and each acquired company was a mishmash in the first place—the complexity increases.

The point is that having a COBIT approach, having a Val IT approach, disciplined and in place, is something you can use to make that process much less painful if you've done that upfront. And this goes to your point about attending the business meetings, getting into those governance organizations that Paul mentioned.

JA: A lot of the time, in these smaller companies, the IT people aren't even invited to the table. I'm not sure if it's appropriate for the IT director or the CIO to say, "Hey, I'd like to sit in the room, too, when you guys are doing your strategic planning. We need to share this to see if we can get on board with it."

PW: IT can be at that table and not be told this is what you've got to do. But that could make a whole topic for one of these discussions because it is fascinating, often controversial, and very important.

BB: As we begin to wrap up, let's go around that table and hit on what you each would like to emphasize.

SS: A key point, I think, is that convergence is something that we all have to face. We have to break down some of those silos. The point that I evangelize the most around convergence is establishment of internal controls architecture, the framework, whatever you want to call it, that sets out the requirements and combines aspects of whatever these reference architectures are (ITIL, ISO, COBIT)—basically, translating those into policies, standards and controls and getting a common methodology around the definition of what a control is for the organization. Then, leveraging that for multiple compliance, risk or performance management activities.

UF: In my view, one of the most important things that we should pick up is to look for a balance between the cost of managing the risks vs. the benefit of reducing the risks. The second thing is that we have to get away from the tick boxes!

IT GOVERNANCE ROUNDTABLE: VALUE DELIVERY

PW: I would add a couple of things so we don't lose sight of them. The first one is the accountability thing. The "A" word is absolutely essential. If you don't have accountability, you don't get results. Accountability is uppermost in my mind. The other thing is to make sure that you root everything in the business. It's all very well to look at IT processes and IT risks, but at the end of the day, we have to remember why IT is there. It's there to support and enable the business. Unless we understand what the business drivers are, what it is that makes the business a success, then everything we do will only happen if it is a tick-in-the-box thing and we dismissed that as not being a sensible idea. Business understanding or business awareness is essential.

JA: From my small-world point of view, bringing IT to the table for some of the planning is important. IT is task-oriented. It is siloed and it has been siloed for a long time. Unless the business brings IT to the table or lets IT participate in future planning, governance is never going to work. Regarding the check-box mentality—companies will still have that "wizard behind the curtain" approach toward their IT department.

BB: I would like to mention, again, three points that I hit on. First, don't be frivolous. A governance effort that doesn't have that accountability, by definition, is frivolous. If you're not serious about it, it shouldn't be considered a real effort. You shouldn't try to say that we've now handled governance by putting in place a useless steering committee with people who are not really accountable. It has to be real governance that you're truly serious about doing. As part of that effort, and making it more mature, you want to emphasize the point about risk-aware governance—to pick up on Urs' earlier comments, both in the sense of having the risk and return information be part of the business cases, not just the return, and in the sense of risk to daily operations. Everyone tries to put out the revenue number that Paul mentioned and it is somewhat mythical. But including the risk stuff makes it real and allows you to differentiate in a conversation with the CFO which projects are more likely to succeed and pay off.

Urs' good points on the dependencies are very important, not only in and of themselves, but as maturity points. They are something very tangible that people can do who don't yet have a mountain of data and are still working their way toward automation before they get to those tools.

The last point is about the efficiency issue. To use all the points we've talked about so far, there are ways you can make governance efficient so it can drive value in a smooth way. That will make people feel not only that we're not consuming too many resources, but also that they're being treated fairly in the process and thus assure the various stakeholders that it's not going to take away all their resources and change their power positions. In some ways it may, but it has to be done with some modesty and integrity in order to make everyone buy in and believe that they truly are optimizing the result. That goes back, again, to Paul's accountability and the right metrics to tie that off. So that "accountability" word seems like something that has run through much of our conversation and a good word on which to close.